

**BỘ GIÁO DỤC VÀ ĐÀO TẠO  
TRƯỜNG ĐẠI HỌC NGOẠI NGỮ - TIN HỌC  
THÀNH PHỐ HỒ CHÍ MINH  
KHOA CÔNG NGHỆ THÔNG TIN**

---



**MÔN HỌC: BẢO MẬT NGƯỜI DÙNG CUỐI  
ĐỀ TÀI:  
NHÓM 3**

**GIẢNG VIÊN HƯỚNG DẪN : Th.S Đỗ Phi Hưng**

**SINH VIÊN THỰC HIỆN : 22DH112390 - Đặng Lê Quang Ngọc  
22DH114543 Huỳnh Gia Hòa  
22DH113040 Nguyễn Lê Văn Quyền**

**TP. HỒ CHÍ MINH, THÁNG 8 NĂM 2025**

# MỤC LỤC

|  |    |
|--|----|
| <b>CHƯƠNG I. GIỚI THIỆU ĐỀ TÀI</b> .....                             | 9  |
| 1.    Giới thiệu chung.....  | 9  |
| 2.    Giới thiệu giải pháp IDS/IPS .....                             | 9  |
| <b>CHƯƠNG II. CƠ SỞ LÝ THUYẾT</b> .....                              | 9  |
| 1.    Tổng quan về an toàn thông tin .....                           | 9  |
| 1.1.    Khái niệm an toàn thông tin .....                            | 9  |
| 1.2.    Mục tiêu của an toàn thông tin – CIA Triad.....              | 10 |
| 1.3.    Vai trò của an toàn thông tin trong xã hội hiện đại .....    | 11 |
| 1.4.    Đối tượng và phạm vi áp dụng.....                            | 11 |
| 2.    Mối đe dọa và lỗ hổng bảo mật phổ biến .....                   | 11 |
| 2.1.    Khái niệm mối đe dọa và lỗ hổng .....                        | 11 |
| 2.2.    Các loại mối đe dọa phổ biến đối với người dùng cuối.....    | 11 |
| 2.3.    Lỗ hổng phổ biến bị khai thác .....                          | 14 |
| 2.4.    Tác động của mối đe dọa và lỗ hổng .....                     | 14 |
| 3.    Bảo mật thiết bị và dữ liệu cá nhân.....                       | 15 |
| 3.1.    Tầm quan trọng của bảo mật thiết bị và dữ liệu cá nhân ..... | 15 |
| 3.2.    Các biện pháp bảo vệ thiết bị cá nhân .....                  | 15 |
| 3.3.    Bảo vệ dữ liệu cá nhân.....                                  | 17 |
| 3.4.    Một số thói quen cần tránh .....                             | 17 |
| 4.    Bảo mật trong sử dụng mạng.....                                | 18 |
| 4.1.    Mạng và vai trò trong đời sống số .....                      | 18 |
| 4.2.    Nguy cơ khi sử dụng mạng không an toàn .....                 | 18 |
| 4.3.    Biện pháp bảo mật khi sử dụng mạng .....                     | 18 |
| 4.4.    Quản lý quyền truy cập trong tổ chức .....                   | 19 |
| 5.    Chính sách bảo mật và tuân thủ.....                            | 19 |
| 5.1.    Khái niệm chính sách bảo mật.....                            | 19 |
| 5.2.    Các loại chính sách bảo mật phổ biến.....                    | 19 |
| 5.3.    Tuân thủ pháp luật và tiêu chuẩn bảo mật.....                | 20 |
| 5.4.    Trách nhiệm của người dùng cuối trong việc tuân thủ.....     | 20 |
| 6.    Phản ứng và xử lý sự cố an toàn thông tin.....                 | 20 |
| 6.1.    Khái niệm sự cố an toàn thông tin.....                       | 20 |
| 6.2.    Các loại sự cố phổ biến .....                                | 21 |

|  |  |           |
|--|--|-----------|
| 6.3.                                       | Quy trình phản ứng sự cố.....                        | 21        |
| 6.4.                                       | Vai trò của người dùng cuối trong ứng phó sự cố..... | 21        |
| 6.5.                                       | Tác động khi không xử lý đúng cách .....             | 22        |
| 7.   | Xây dựng nhận thức và văn hóa bảo mật.....           | 22        |
| 7.1.                                       | Vai trò của nhận thức bảo mật.....                   | 22        |
| 7.2.                                       | Hành vi người dùng ảnh hưởng đến bảo mật.....        | 22        |
| 7.3.                                       | Các hình thức đào tạo và nâng cao nhận thức .....    | 22        |
| 7.4.                                       | Xây dựng văn hóa bảo mật .....                       | 23        |
| <b>CHƯƠNG III. XÂY DỰNG HỆ THỐNG .....</b> |  | <b>24</b> |
| 1.   | Bảng phân hoạch IP.....                              | 24        |
| 2.   | Sơ đồ mạng .....                                     | 25        |
| 3.   | Triển khai IDS .....                                 | 26        |
| 4.   | System Endpoint .....                                | 30        |
| 4.1.                                       | Kịch bản 1 .....                                     | 30        |
| 4.2.                                       | Kịch bản 2 .....                                     | 31        |
| <b>CHƯƠNG IV. KẾT LUẬN.....</b>            |  | <b>33</b> |

## DANH MỤC HÌNH ẢNH

|  |    |
|--|----|
| Hình 1: Các mối nguy cơ trong thế giới số .....  | 10 |
| Hình 2: Mô hình nền tảng bảo mật CIA Triad .....   | 10 |
| Hình 3: Các loại Malware .....   | 12 |
| Hình 4: Sơ đồ tấn công kỹ thuật xã hội (Social Engineering Attack Flow).....                               | 13 |
| Hình 5: Mô hình tấn công MitM (Man-in-the-Middle) .....  | 14 |
| Hình 6: Biểu đồ thể hiện thời gian để dò mật khẩu (brute-force) dựa trên độ phức tạp .....                 | 15 |
| Hình 7: Các phương pháp xác thực đa yếu tố .....   | 16 |
| Hình 8: Sao lưu và bảo mật dữ liệu .....   | 17 |
| Hình 9: Sơ đồ logic hệ thống mạng triển khai .....   | 25 |
| Hình 10: Bật interface để IDS monitor .....  | 26 |
| Hình 11: Thêm rule cho IDS .....   | 27 |
| Hình 12: IDS gửi được cảnh báo khi hacker tấn công .....   | 28 |
| Hình 13: Hacker truy cập được web host ở DMZ .....   | 29 |
| Hình 14: Các lệnh để tấn công web .....  | 30 |
| Hình 15: System endpoint ghi nhận được log audit của người dùng cố gắng truy cập bằng tài khoản admin..... | 31 |
| Hình 16: Tùy chỉnh file ossec.conf .....   | 32 |
| Hình 17: System endpoint ghi nhận được sự kiện folder monitor có file mới thêm vào.....                    | 33 |



## DANH MỤC BẢNG BIỂU

|   |    |
|---|----|
| Bảng 1: Bảng phân hoạch IP triển khai hệ thống..... | 24 |
|---|----|

# LỜI NÓI ĐẦU

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ trên toàn cầu, an toàn thông tin đã trở thành yếu tố sống còn đối với mọi tổ chức, doanh nghiệp và cả nền kinh tế – xã hội nói chung. Các hình thức tấn công mạng ngày càng tinh vi không chỉ nhắm vào hệ thống kỹ thuật mà còn khai thác điểm yếu từ con người – đặc biệt là người dùng cuối, những cá nhân trực tiếp tương tác với thiết bị, hệ thống và dữ liệu hằng ngày. Một thao tác bất cẩn, một mật khẩu yếu hay một liên kết độc hại được mở ra từ hộp thư điện tử đều có thể trở thành cánh cửa cho các cuộc tấn công có khả năng gây ra thiệt hại nghiêm trọng: từ đánh cắp thông tin, phá hoại hệ thống đến gián đoạn hoạt động kinh doanh và ảnh hưởng đến uy tín của tổ chức. Chính vì vậy, bảo mật ở cấp độ người dùng không còn là vấn đề cá nhân, mà là một mắt xích thiết yếu trong chiến lược bảo vệ toàn diện.

Môn học **“BẢO MẬT NGƯỜI DÙNG CUỐI”** được xây dựng nhằm cung cấp nền tảng kiến thức vững chắc về các mối đe dọa phổ biến và các nguyên tắc bảo vệ thông tin trong môi trường số. Thông qua việc tìm hiểu cách phòng tránh phần mềm độc hại, lừa đảo trực tuyến, kỹ thuật tấn công qua mạng xã hội, cũng như cách sử dụng an toàn các thiết bị, mật khẩu, hệ thống mạng và dịch vụ số, môn học góp phần hình thành nhận thức và chuẩn hóa hành vi sử dụng công nghệ trong môi trường tổ chức. Qua đó, các cơ quan, doanh nghiệp và cộng đồng có thể nâng cao khả năng phòng vệ nội bộ, giảm thiểu rủi ro từ yếu tố con người, và xây dựng một văn hóa an toàn thông tin bền vững, thích ứng với những thách thức ngày càng gia tăng của kỷ nguyên số.

# LỜI CẢM ƠN

Trước hết, nhóm thực hiện đề tài xin bày tỏ lòng biết ơn sâu sắc đến khoa Công nghệ Thông tin, cùng toàn thể quý thầy cô giảng viên đã tận tình giảng dạy, truyền đạt kiến thức, tạo điều kiện thuận lợi cho nhóm trong suốt quá trình học tập và thực hiện đề tài này.

Nhóm xin gửi lời cảm ơn chân thành đến Th.S Đỗ Phi Hưng, người đã trực tiếp hướng dẫn, định hướng và hỗ trợ nhóm trong suốt quá trình triển khai đề tài. Sự tận tâm, những nhận xét chuyên môn sâu sắc và những đóng góp quý báu của thầy/cô chính là kim chỉ nam giúp nhóm hoàn thiện đề tài một cách hiệu quả và thực tiễn nhất.

Bên cạnh đó, nhóm cũng xin gửi lời cảm ơn đến bạn bè đã hỗ trợ, góp ý và chia sẻ kinh nghiệm quý báu trong suốt quá trình thực hiện nghiên cứu.

Mặc dù đã nỗ lực hết sức trong việc tìm hiểu, xây dựng và triển khai đề tài, nhưng do giới hạn về thời gian và kinh nghiệm thực tiễn còn hạn chế, bài làm không tránh khỏi những thiếu sót. Nhóm rất mong nhận được những góp ý chân thành từ quý thầy cô và bạn đọc để có thể tiếp tục hoàn thiện hơn trong tương lai.

Một lần nữa, xin chân thành cảm ơn sự hỗ trợ, đồng hành đối với nhóm trong suốt quá trình thực hiện đề tài.



# CHƯƠNG I. GIỚI THIỆU ĐỀ TÀI

## 1. Giới thiệu chung

Trong thời đại số hiện nay, khi các cuộc tấn công mạng ngày càng tinh vi và có tổ chức, việc bảo vệ hệ thống thông tin không chỉ dừng lại ở các lớp tường lửa hay antivirus truyền thống mà còn đòi hỏi các giải pháp bảo mật toàn diện và chủ động. Một trong những trọng tâm trong chiến lược an toàn thông tin là đảm bảo an ninh tại các endpoint – nơi người dùng trực tiếp tương tác với hệ thống, cũng là mắt xích yếu nhất trong chuỗi bảo mật.

Endpoint, bao gồm các máy trạm, máy chủ, thiết bị di động,... là mục tiêu hàng đầu của các cuộc tấn công như: malware, ransomware, phishing hay truy cập trái phép. Việc xây dựng một hệ thống mạng bảo mật endpoint giúp giám sát, phát hiện, và phản ứng nhanh chóng với các mối đe dọa, từ đó nâng cao khả năng phòng thủ tổng thể của tổ chức.

Đề án này tập trung vào việc thiết kế và triển khai hệ thống mạng có khả năng bảo vệ endpoint, tích hợp các giải pháp như IDS/IPS, EDR, antivirus, logging và phân tích sự kiện để phát hiện và ngăn chặn tấn công trong thời gian thực.

## 2. Giới thiệu giải pháp IDS/IPS

IDS – Intrusion Detection System (Hệ thống phát hiện xâm nhập): IDS là hệ thống có chức năng giám sát lưu lượng mạng hoặc hoạt động hệ thống để phát hiện các hành vi đáng ngờ, từ đó cảnh báo cho quản trị viên. IDS không ngăn chặn mà chỉ phát hiện và cảnh báo. Có hai loại IDS chính:

- NIDS (Network-based IDS): Giám sát lưu lượng mạng (ví dụ: Snort, Suricata).
- HIDS (Host-based IDS): Giám sát hoạt động trên máy chủ hoặc máy trạm (ví dụ: OSSEC, Wazuh).

IPS – Intrusion Prevention System (Hệ thống ngăn chặn xâm nhập): IPS là hệ thống mở rộng từ IDS, có khả năng ngăn chặn các hành vi tấn công ngay khi phát hiện (ví dụ: block kết nối, dừng tiến trình). IPS thường được tích hợp vào firewall hoặc các thiết bị mạng trung gian (ví dụ: pfSense + Snort/Suricata).

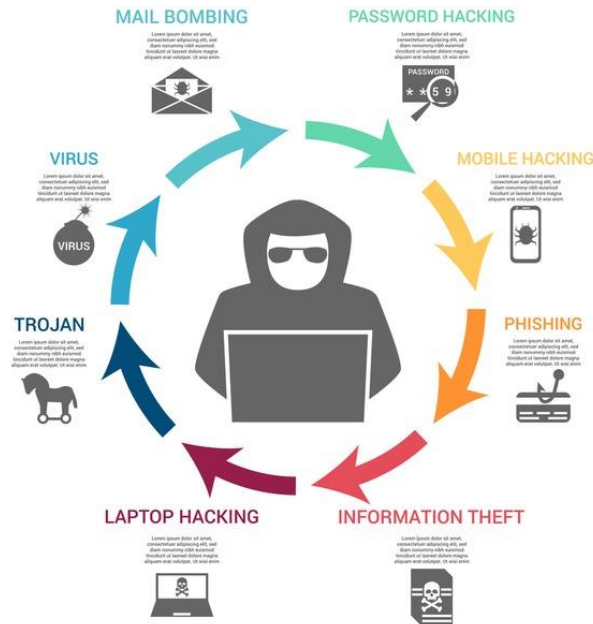
# CHƯƠNG II. CƠ SỞ LÝ THUYẾT

## 1. Tổng quan về an toàn thông tin

### 1.1. Khái niệm an toàn thông tin

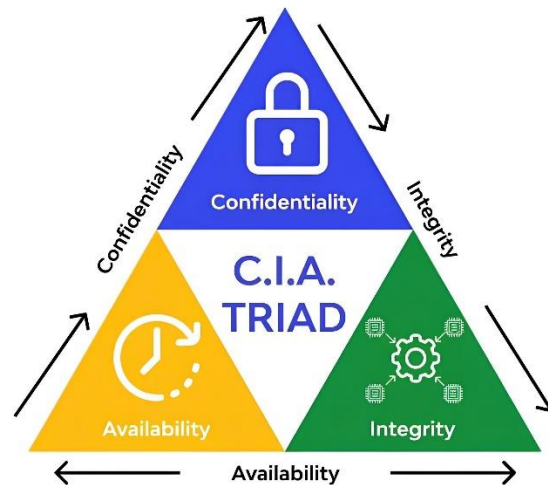
An toàn thông tin (Information Security) là quá trình bảo vệ thông tin khỏi các mối đe dọa nhằm đảm bảo tính bí mật, toàn vẹn và sẵn sàng của thông tin. Đây là một lĩnh vực liên quan đến các chính sách, quy trình, kỹ thuật và hành vi nhằm ngăn chặn truy cập trái phép, sử dụng sai mục đích, tiết lộ, phá hoại hoặc thay đổi dữ liệu.

Trong môi trường số hiện đại, thông tin không chỉ là tài sản có giá trị mà còn là yếu tố quyết định đến uy tín, vận hành và sự sống còn của tổ chức. Việc đảm bảo an toàn thông tin vì vậy không chỉ là vấn đề kỹ thuật mà còn là trách nhiệm chiến lược của cả cá nhân và tổ chức.



Hình 1: Các mối nguy cơ trong thế giới số

## 1.2. Mục tiêu của an toàn thông tin – CIA Triad



Hình 2: Mô hình nền tảng bảo mật CIA Triad

Ba mục tiêu cốt lõi tạo thành nền tảng của mọi chính sách và giải pháp an toàn thông tin được gọi là mô hình CIA, bao gồm:

- Confidentiality – Tính bảo mật: Thông tin chỉ được truy cập bởi những người, hệ thống hoặc quy trình được phép. Điều này đảm bảo dữ liệu không bị rò rỉ hoặc bị kẻ tấn công đánh cắp.
- Integrity – Tính toàn vẹn: Dữ liệu phải chính xác và không bị thay đổi bởi những tác nhân trái phép. Bất kỳ sự thay đổi nào trong dữ liệu đều phải được kiểm soát và ghi nhận rõ ràng.
- Availability – Tính sẵn sàng: Hệ thống và dữ liệu luôn phải sẵn sàng để người dùng hợp lệ truy cập khi cần thiết. Điều này đòi hỏi các biện pháp bảo vệ khỏi tấn công từ chối dịch vụ (DoS) và các sự cố kỹ thuật.

### 1.3. Vai trò của an toàn thông tin trong xã hội hiện đại

Trong thời đại mà dữ liệu trở thành “tài sản số” và phần lớn các hoạt động xã hội, kinh doanh, quản lý đều diễn ra qua môi trường điện tử, an toàn thông tin đóng vai trò sống còn. Bảo mật không còn là vấn đề riêng của bộ phận CNTT mà đã lan rộng tới từng cá nhân sử dụng công nghệ.

Một vi phạm an toàn thông tin có thể dẫn đến:

- Thiệt hại tài chính (đánh cắp tài khoản ngân hàng, tiền mã hóa...)
- Rò rỉ thông tin cá nhân, mất quyền riêng tư
- Mất uy tín của tổ chức, ảnh hưởng đến khách hàng và đối tác
- Nguy cơ pháp lý và vi phạm quy định luật pháp (ví dụ: vi phạm luật bảo vệ dữ liệu)

Không những vậy, các nguy cơ về an toàn thông tin còn đe dọa đến sự ổn định xã hội nếu nhằm vào hạ tầng trọng yếu như điện lực, giao thông, y tế hay truyền thông.

### 1.4. Đối tượng và phạm vi áp dụng

An toàn thông tin không giới hạn trong phạm vi hệ thống máy chủ hay dữ liệu doanh nghiệp. Nó bao gồm mọi khía cạnh từ người dùng cuối, phần mềm, phần cứng, mạng lưới, dịch vụ đám mây cho đến thiết bị IoT. Mỗi cá nhân khi sử dụng thiết bị số đều là một phần trong hệ sinh thái an toàn thông tin – và cũng là một điểm yếu tiềm tàng nếu không được trang bị đầy đủ kiến thức.

## 2. Môi đe dọa và lỗ hổng bảo mật phổ biến

### 2.1. Khái niệm môi đe dọa và lỗ hổng

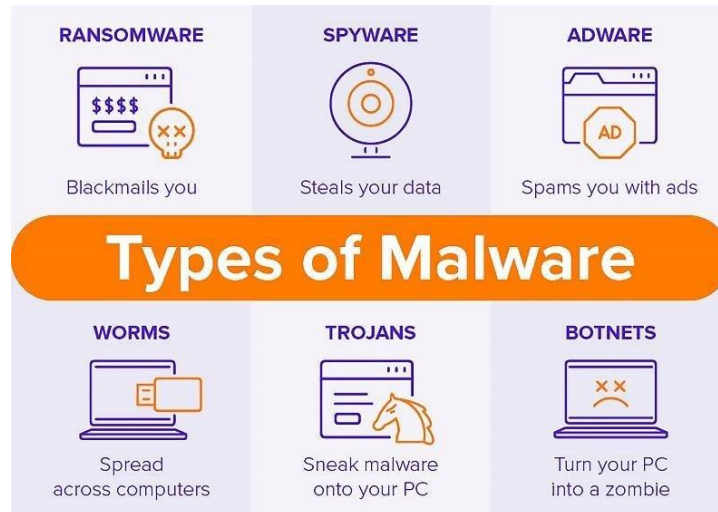
Trong lĩnh vực an toàn thông tin, môi đe dọa (threat) là bất kỳ yếu tố nào có thể gây ảnh hưởng xấu đến tài nguyên, dữ liệu hoặc hệ thống thông tin. Môi đe dọa có thể đến từ con người, phần mềm độc hại, sự cố tự nhiên, hoặc lỗi hệ thống.

Lỗ hổng (vulnerability) là điểm yếu trong hệ thống, phần mềm, quy trình, hoặc hành vi người dùng mà có thể bị môi đe dọa khai thác để gây ra thiệt hại.

Một cuộc tấn công thành công thường xảy ra khi môi đe dọa khai thác được một lỗ hổng chưa được bảo vệ đúng cách.

### 2.2. Các loại môi đe dọa phổ biến đối với người dùng cuối

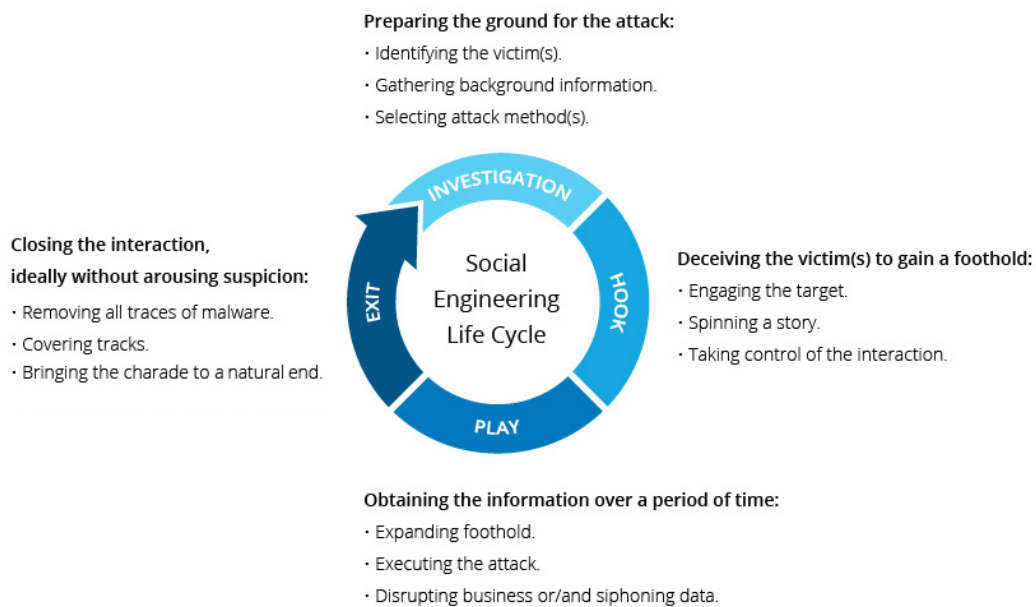
- a) Phần mềm độc hại (Malware)



*Hình 3: Các loại Malware*

Phần mềm độc hại là chương trình được thiết kế để gây hại, đánh cắp dữ liệu hoặc kiểm soát hệ thống người dùng. Một số dạng malware phổ biến gồm:

- Virus: Lây lan bằng cách chèn vào các tệp tin hợp pháp và kích hoạt khi tệp đó được mở.
  - Worm (Sâu): Lây lan qua mạng mà không cần tệp chủ. Có thể nhanh chóng làm nghẽn mạng và gây hư hại hệ thống.
  - Trojan Horse: Giả dạng phần mềm hợp pháp nhưng thực chất chứa mã độc.
  - Ransomware: Mã hóa dữ liệu người dùng và đòi tiền chuộc để giải mã.
  - Spyware/Keylogger: Theo dõi hành vi người dùng và đánh cắp thông tin cá nhân (như mật khẩu, số thẻ tín dụng).
- b) Tấn công kỹ thuật xã hội (Social Engineering)



*Hình 4: Sơ đồ tấn công kỹ thuật xã hội (Social Engineering Attack Flow)*

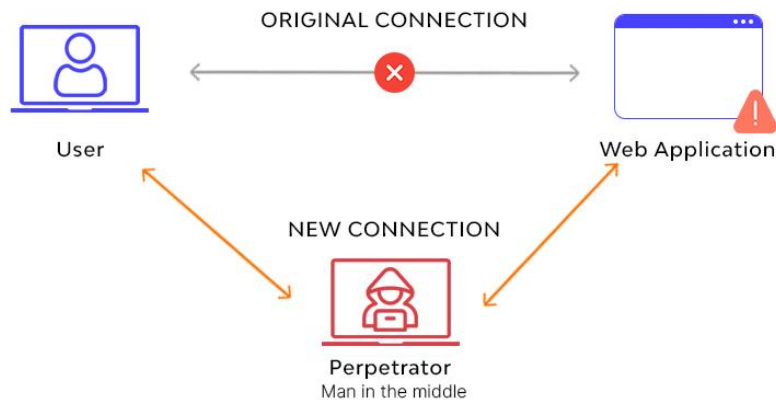
Đây là hình thức tấn công đánh vào yếu tố con người, lừa người dùng thực hiện hành động có lợi cho kẻ tấn công. Một số dạng phổ biến:

- Phishing: Giả mạo email/tin nhắn từ tổ chức uy tín để dụ người dùng nhấp vào liên kết độc hại hoặc cung cấp thông tin cá nhân.
- Spear Phishing: Tấn công có mục tiêu cụ thể, thường cá nhân hóa nội dung để tạo sự tin tưởng.
- Vishing (Voice Phishing): Giả mạo cuộc gọi điện thoại để lấy thông tin nhạy cảm.
- Pretexting: Tạo ra một "bối cảnh giả" (ví dụ, giả làm nhân viên kỹ thuật) để lấy lòng tin của nạn nhân.

c) Tấn công mạng (Network Attacks)

Các hình thức tấn công khai thác lỗ hổng trong giao tiếp mạng hoặc hệ thống:

- Man-in-the-Middle (MitM): Kẻ tấn công chen vào giữa người dùng và máy chủ để đọc, chỉnh sửa hoặc đánh cắp dữ liệu.



*Hình 5: Mô hình tấn công MitM (Man-in-the-Middle)*

- Tấn công từ chối dịch vụ (DoS/DDoS): Làm tê liệt hệ thống hoặc dịch vụ bằng cách gửi lượng truy cập quá tải.
- Brute Force Attack: Dò mật khẩu bằng cách thử hết tất cả các khả năng có thể, đặc biệt hiệu quả với mật khẩu yếu.
- Session Hijacking: Chiếm quyền điều khiển một phiên truy cập (session) của người dùng hợp lệ.

### 2.3. Lỗ hổng phổ biến bị khai thác

Không chỉ mỗi đe dọa bên ngoài, nhiều lỗ hổng nội tại có thể tạo điều kiện cho tấn công xảy ra:

- Mật khẩu yếu hoặc trùng lặp: Là một trong những lỗ hổng phổ biến nhất. Người dùng thường đặt mật khẩu dễ đoán hoặc sử dụng lại mật khẩu cho nhiều dịch vụ.
- Phần mềm lỗi thời: Các hệ điều hành, trình duyệt hoặc ứng dụng chưa cập nhật thường chứa các lỗ hổng chưa được vá.
- Thiếu xác thực đa yếu tố (MFA): Chỉ dùng một lớp bảo mật (như mật khẩu) là chưa đủ.
- Cấu hình sai: Hệ thống hoặc dịch vụ bị cấu hình sai (ví dụ: mở cổng mạng không cần thiết, tắt tường lửa) có thể bị khai thác.
- Thiếu nhận thức người dùng: Người dùng thiếu kiến thức bảo mật có thể trở thành điểm yếu lớn nhất trong hệ thống.

### 2.4. Tác động của mối đe dọa và lỗ hổng

Một khi mối đe dọa khai thác thành công lỗ hổng, hậu quả có thể rất nghiêm trọng:

- Rò rỉ hoặc mất mát dữ liệu cá nhân và nhạy cảm
- Mất quyền truy cập vào hệ thống, tài khoản, dịch vụ
- Gián đoạn hoạt động của tổ chức, gây tổn thất tài chính
- Ảnh hưởng đến uy tín và niềm tin từ khách hàng hoặc đối tác
- Có thể bị truy cứu trách nhiệm pháp lý nếu vi phạm luật bảo vệ dữ liệu

### 3. Bảo mật thiết bị và dữ liệu cá nhân


#### 3.1. Tầm quan trọng của bảo mật thiết bị và dữ liệu cá nhân

Trong môi trường số hiện nay, mỗi cá nhân đều sở hữu nhiều thiết bị công nghệ như máy tính, điện thoại thông minh, máy tính bảng, và đồng thời sử dụng nhiều dịch vụ lưu trữ, truyền tải và xử lý dữ liệu cá nhân. Các thiết bị này chính là "cửa ngõ" vào dữ liệu nhạy cảm như tài khoản ngân hàng, thông tin cá nhân, tài liệu công việc, hình ảnh riêng tư... Vì vậy, bảo mật thiết bị và dữ liệu cá nhân không chỉ nhằm bảo vệ quyền riêng tư của mỗi người, mà còn góp phần vào sự an toàn tổng thể của tổ chức và cộng đồng số.

#### 3.2. Các biện pháp bảo vệ thiết bị cá nhân

a) Sử dụng mật khẩu mạnh và bảo mật

| Time it takes a hacker to brute force your password in 2025 |              |                   |                             |                                      |   |
|---|--------------|-------------------|-----------------------------|--------------------------------------|---|
| Hardware: 12 x RTX 5090   Password hash: bcrypt (10)        |              |                   |                             |                                      |   |
| Number of Characters  | Numbers Only | Lowercase Letters | Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters | Numbers, Upper and Lowercase Letters, Symbols |
| 4   | Instantly    | Instantly         | Instantly                   | Instantly                            | Instantly                                     |
| 5   | Instantly    | Instantly         | 57 minutes                  | 2 hours                              | 4 hours                                       |
| 6   | Instantly    | 46 minutes        | 2 days                      | 6 days                               | 2 weeks                                       |
| 7   | Instantly    | 20 hours          | 4 months                    | 1 year                               | 2 years                                       |
| 8   | Instantly    | 3 weeks           | 15 years                    | 62 years                             | 164 years                                     |
| 9   | 2 hours      | 2 years           | 791 years                   | 3k years                             | 11k years                                     |
| 10  | 1 day        | 40 years          | 41k years                   | 238k years                           | 803k years                                    |
| 11  | 1 weeks      | 1k years          | 2m years                    | 14m years                            | 56m years                                     |
| 12  | 3 months     | 27k years         | 111m years                  | 917m years                           | 3bn years                                     |
| 13  | 3 years      | 705k years        | 5bn years                   | 56bn years                           | 275bn years                                   |
| 14  | 28 years     | 18m years         | 300bn years                 | 3tn years                            | 19tn years                                    |
| 15  | 284 years    | 477m years        | 15tn years                  | 218tn years                          | 1qd years                                     |
| 16  | 2k years     | 12bn years        | 812tn years                 | 13qd years                           | 94qd years                                    |
| 17  | 28k years    | 322bn years       | 42qd years                  | 840qd years                          | 6qn years                                     |
| 18  | 284k years   | 8tn years         | 2qn years                   | 52qn years                           | 463qn years                                   |

 **Hive Systems** [Read more and download at hivesystems.com/password](https://hivesystems.com/password)

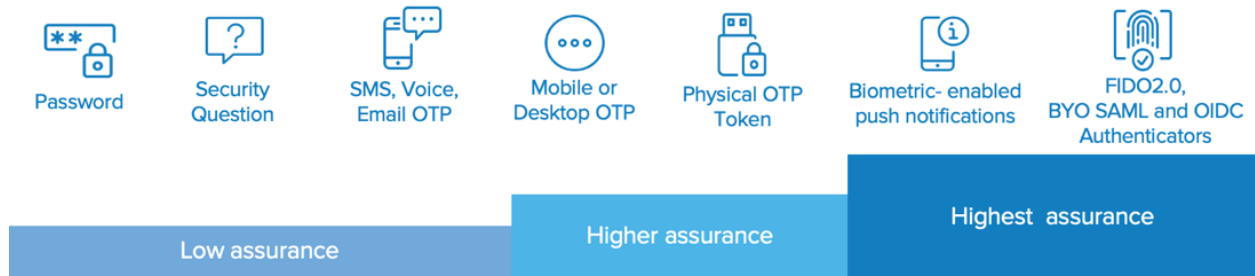
Hình 6: Biểu đồ thể hiện thời gian để dò mật khẩu (brute-force) dựa trên độ phức tạp

Việc đặt mật khẩu yếu hoặc dễ đoán (như “123456” hoặc “password”) là một trong những nguyên nhân phổ biến khiến người dùng bị xâm nhập. Mật khẩu mạnh nên:

- Có độ dài tối thiểu 12 ký tự
- Kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt
- Tránh dùng tên, ngày sinh hoặc thông tin cá nhân
- Không sử dụng lại cùng một mật khẩu cho nhiều tài khoản

Ngoài ra, nên sử dụng trình quản lý mật khẩu (password manager) để tạo và lưu trữ mật khẩu an toàn.

b) Kích hoạt xác thực đa yếu tố (Multi-Factor Authentication - MFA)



Hình 7: Các phương pháp xác thực đa yếu tố

MFA là lớp bảo mật bổ sung ngoài mật khẩu, yêu cầu thêm một yếu tố xác thực như mã OTP, vân tay, hoặc ứng dụng xác thực. Điều này làm giảm đáng kể nguy cơ bị truy cập trái phép ngay cả khi mật khẩu bị rò rỉ.

c) Cập nhật phần mềm thường xuyên

Hệ điều hành, ứng dụng, trình duyệt, và firmware cần được cập nhật định kỳ để vá các lỗ hổng bảo mật. Tin tặc thường khai thác các bản vá chưa được áp dụng để tấn công vào hệ thống người dùng.

d) Cài đặt phần mềm bảo mật

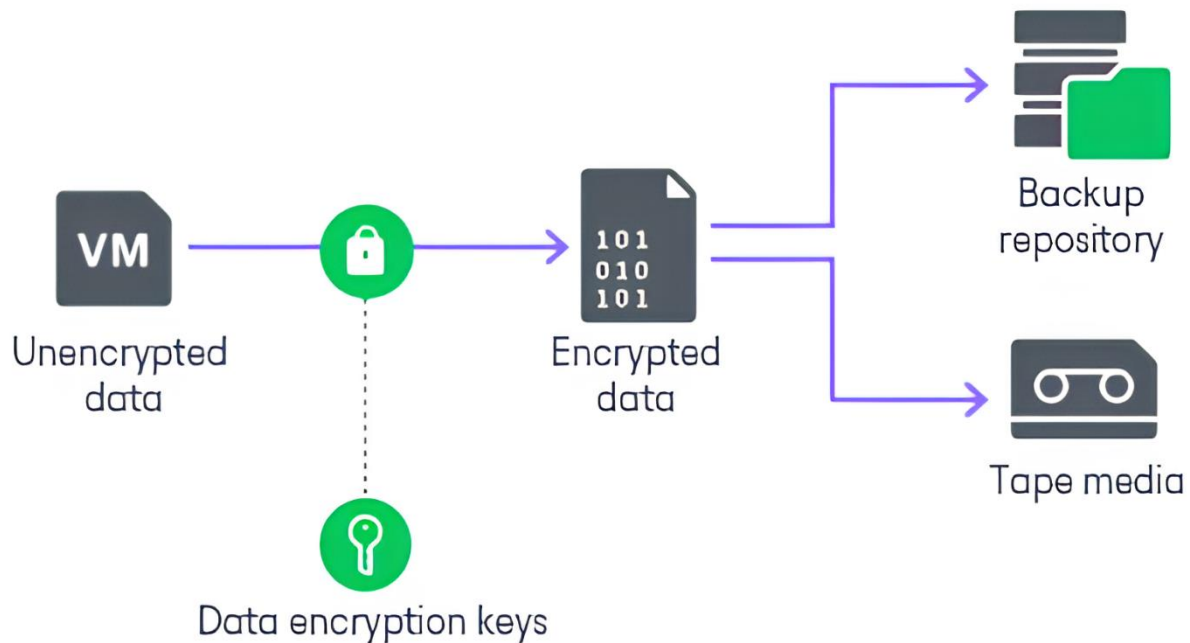
Sử dụng phần mềm diệt virus và tường lửa cá nhân giúp ngăn chặn phần mềm độc hại, cảnh báo trang web nguy hiểm, và bảo vệ thiết bị khỏi truy cập trái phép.

e) Khóa thiết bị khi không sử dụng

Thiết bị nên được khóa tự động sau một thời gian không hoạt động, đồng thời sử dụng mã PIN, mật khẩu, hoặc sinh trắc học (vân tay, khuôn mặt) để mở khóa.



### 3.3. Bảo vệ dữ liệu cá nhân



Hình 8: Sao lưu và bảo mật dữ liệu

#### a) Mã hóa dữ liệu

Mã hóa giúp dữ liệu trở nên vô nghĩa đối với người không có khóa giải mã. Việc mã hóa nên áp dụng cho cả dữ liệu đang lưu trữ (trên thiết bị, ổ cứng, USB...) và dữ liệu đang truyền (qua email, tin nhắn...).

#### b) Sao lưu định kỳ

Sao lưu dữ liệu quan trọng vào thiết bị khác hoặc dịch vụ lưu trữ đám mây giúp phục hồi dữ liệu khi thiết bị bị mất, hỏng, hoặc bị mã hóa bởi ransomware.

#### c) Hạn chế chia sẻ và cấp quyền truy cập

Chỉ nên chia sẻ dữ liệu khi thực sự cần thiết và kiểm soát quyền truy cập, đặc biệt trên các nền tảng đám mây như Google Drive, OneDrive. Tránh cấp quyền "Toàn quyền chỉnh sửa" cho mọi người.

#### d) Xóa an toàn dữ liệu khi bỏ thiết bị

Khi thanh lý, bán hoặc cho người khác mượn thiết bị, cần xóa dữ liệu một cách an toàn bằng cách đặt lại thiết bị về trạng thái gốc (factory reset) hoặc sử dụng phần mềm chuyên dụng để ghi đè dữ liệu.

### 3.4. Một số thói quen cần tránh

- Lưu mật khẩu trong trình duyệt mà không có mã bảo vệ

- Cài đặt phần mềm từ nguồn không rõ ràng
- Kết nối Wi-Fi công cộng không sử dụng VPN
- Gửi thông tin nhạy cảm qua email hoặc tin nhắn không mã hóa

## 4. Bảo mật trong sử dụng mạng

### 4.1. Mạng và vai trò trong đời sống số

Mạng máy tính và internet là nền tảng thiết yếu giúp người dùng kết nối, chia sẻ thông tin, làm việc từ xa, học tập và sử dụng các dịch vụ trực tuyến. Tuy nhiên, khi truy cập vào một mạng – đặc biệt là mạng công cộng hoặc mạng không bảo mật – người dùng có thể vô tình trở thành nạn nhân của các cuộc tấn công đánh cắp dữ liệu, giám sát hành vi, hoặc lây nhiễm phần mềm độc hại. Do đó, việc đảm bảo an toàn khi sử dụng mạng là yêu cầu quan trọng để bảo vệ thông tin cá nhân và tài nguyên số.

### 4.2. Nguy cơ khi sử dụng mạng không an toàn

Một số rủi ro phổ biến người dùng có thể gặp phải khi sử dụng mạng:

- Nghe lén (eavesdropping): Kẻ tấn công có thể theo dõi lưu lượng mạng không mã hóa để lấy thông tin đăng nhập, tài khoản, hoặc nội dung truyền tải.
- Tấn công Man-in-the-Middle (MitM): Kẻ tấn công chen vào giữa người dùng và máy chủ để đánh cắp, chỉnh sửa hoặc giả mạo dữ liệu.
- Giả mạo điểm truy cập (Rogue Access Point): Tạo một mạng Wi-Fi giả với tên gần giống Wi-Fi hợp pháp để lừa người dùng kết nối và đánh cắp thông tin.
- Phát tán phần mềm độc hại: Mạng không an toàn có thể là đường dẫn để cài mã độc vào thiết bị người dùng.

### 4.3. Biện pháp bảo mật khi sử dụng mạng

#### a) Sử dụng kết nối mã hóa (HTTPS)

Luôn ưu tiên truy cập các trang web có giao thức HTTPS (biểu tượng ổ khóa trên thanh địa chỉ). HTTPS mã hóa dữ liệu truyền đi, giúp bảo vệ thông tin cá nhân khỏi bị nghe lén hoặc đánh cắp.

#### b) Sử dụng mạng riêng ảo (VPN)

VPN (Virtual Private Network) tạo một đường hầm mã hóa giữa thiết bị của người dùng và máy chủ, đảm bảo dữ liệu không thể bị đọc hoặc chỉnh sửa bởi bên thứ ba. VPN đặc biệt cần thiết khi sử dụng mạng Wi-Fi công cộng tại quán cà phê, sân bay, khách sạn...

#### c) Tránh sử dụng Wi-Fi công cộng không bảo vệ

Không nên đăng nhập tài khoản cá nhân, tài khoản ngân hàng, hoặc truy cập dữ liệu quan trọng trên các mạng Wi-Fi miễn phí không yêu cầu mật khẩu hoặc không rõ nguồn gốc. Nếu cần dùng, hãy kết hợp với VPN và tránh chia sẻ dữ liệu nhạy cảm.

#### d) Kích hoạt tường lửa (Firewall)

Tường lửa cá nhân giúp giám sát và lọc lưu lượng truy cập đến và đi từ thiết bị, từ đó ngăn chặn các kết nối trái phép hoặc phần mềm độc hại hoạt động ngầm.

e) Tắt chia sẻ mạng khi không cần thiết

Tắt chức năng chia sẻ tệp hoặc máy in khi kết nối vào các mạng không tin cậy giúp hạn chế khả năng bị xâm nhập.

f) Cập nhật router/modem định kỳ

Thiết bị mạng gia đình như router hoặc modem cũng cần được cập nhật firmware để vá các lỗ hổng bảo mật và đổi mật khẩu quản trị mặc định.

#### **4.4. Quản lý quyền truy cập trong tổ chức**

Đối với môi trường làm việc, việc quản lý quyền truy cập đóng vai trò then chốt trong bảo mật mạng nội bộ:

- Nguyên tắc “quyền tối thiểu” (Principle of Least Privilege): Người dùng chỉ được cấp quyền đủ để thực hiện công việc, tránh truy cập thừa thãi vào hệ thống quan trọng.
- Phân đoạn mạng (Network Segmentation): Giới hạn truy cập giữa các bộ phận để giảm thiểu thiệt hại khi có sự cố.
- Giám sát lưu lượng mạng: Sử dụng công cụ IDS/IPS (hệ thống phát hiện và ngăn chặn xâm nhập) để phát hiện hoạt động bất thường.

### **5. Chính sách bảo mật và tuân thủ**

#### **5.1. Khái niệm chính sách bảo mật**

Chính sách bảo mật thông tin là tập hợp các quy định, hướng dẫn và quy trình do tổ chức ban hành nhằm đảm bảo việc sử dụng, truy cập và xử lý thông tin được thực hiện một cách an toàn và có kiểm soát. Đây là công cụ quản lý thiết yếu để định hướng hành vi người dùng, giảm thiểu rủi ro bảo mật và nâng cao khả năng ứng phó trước các mối đe dọa mạng.

Chính sách bảo mật không chỉ áp dụng cho nhân viên CNTT, mà còn dành cho tất cả người dùng cuối – bao gồm cả nhân viên văn phòng, cộng tác viên, khách hàng nội bộ và bên thứ ba có quyền truy cập vào hệ thống của tổ chức.

#### **5.2. Các loại chính sách bảo mật phổ biến**

a) Chính sách sử dụng hợp lý (Acceptable Use Policy – AUP)

Quy định cách thức sử dụng tài nguyên CNTT (máy tính, internet, email, thiết bị lưu trữ...) một cách phù hợp và an toàn. Ví dụ: cấm truy cập vào trang web độc hại, không cài đặt phần mềm lạ, không dùng email công ty cho mục đích cá nhân.

b) Chính sách quản lý mật khẩu (Password Policy)

Yêu cầu người dùng tạo và duy trì mật khẩu mạnh, thay đổi định kỳ, không chia sẻ mật khẩu, và khuyến khích sử dụng xác thực nhiều yếu tố (MFA).

c) Chính sách phân quyền và truy cập (Access Control Policy)

Xác định quyền truy cập theo vai trò, nguyên tắc phân quyền tối thiểu (least privilege), và phương pháp quản lý quyền khi người dùng thay đổi công việc hoặc rời khỏi tổ chức.

d) Chính sách bảo vệ dữ liệu cá nhân (Data Protection Policy)

Quy định cách thu thập, lưu trữ, xử lý và chia sẻ dữ liệu cá nhân một cách hợp pháp, an toàn và minh bạch, phù hợp với các quy định pháp lý hiện hành.

e) Chính sách phản hồi và xử lý sự cố (Incident Response Policy)

Hướng dẫn quy trình phát hiện, báo cáo và xử lý sự cố an toàn thông tin. Bao gồm phân loại sự cố, vai trò chịu trách nhiệm và quy trình phục hồi.

### 5.3. Tuân thủ pháp luật và tiêu chuẩn bảo mật

Ngoài các chính sách nội bộ, tổ chức và người dùng cuối còn cần tuân thủ các quy định pháp lý và tiêu chuẩn quốc tế liên quan đến bảo mật, bao gồm:

- Luật an toàn thông tin mạng (tùy theo quốc gia): Quy định trách nhiệm cá nhân, tổ chức trong việc đảm bảo an toàn thông tin.
- Luật bảo vệ dữ liệu cá nhân (ví dụ: GDPR ở EU, Nghị định 13/2023/NĐ-CP ở Việt Nam): Bảo vệ quyền riêng tư của cá nhân, yêu cầu minh bạch trong việc xử lý dữ liệu cá nhân.
- Tiêu chuẩn bảo mật ISO/IEC 27001: Khung quản lý an toàn thông tin quốc tế được công nhận rộng rãi.
- PCIDSS, HIPAA, SOC 2... (tùy lĩnh vực): Các bộ tiêu chuẩn chuyên ngành quy định về bảo mật dữ liệu tài chính, y tế, hoặc dịch vụ số.

Việc không tuân thủ có thể dẫn đến mất mát dữ liệu, thiệt hại uy tín, xử phạt hành chính hoặc trách nhiệm hình sự.

### 5.4. Trách nhiệm của người dùng cuối trong việc tuân thủ

Người dùng cuối đóng vai trò trung tâm trong việc thực hiện và duy trì chính sách bảo mật. Một chính sách dù tốt đến đâu nhưng nếu không được thực hiện nghiêm túc từ phía người dùng thì vẫn có thể thất bại. Các trách nhiệm điển hình của người dùng bao gồm:

- Đọc, hiểu và tuân thủ các chính sách được ban hành.
- Không chia sẻ tài khoản, thông tin đăng nhập hoặc dữ liệu nhạy cảm.
- Báo cáo ngay lập tức khi phát hiện sự cố hoặc hành vi nghi ngờ.
- Tham gia đầy đủ các khóa huấn luyện hoặc kiểm tra nhận thức về bảo mật.

## 6. Phản ứng và xử lý sự cố an toàn thông tin

### 6.1. Khái niệm sự cố an toàn thông tin

Sự cố an toàn thông tin (Security Incident) là bất kỳ sự kiện hoặc hành động nào dẫn đến hoặc có khả năng dẫn đến:

- Mất tính bảo mật, toàn vẹn hoặc sẵn sàng của thông tin;
- Truy cập trái phép vào hệ thống hoặc dữ liệu;
- Vi phạm chính sách bảo mật nội bộ hoặc quy định pháp luật.

Sự cố có thể xảy ra dưới nhiều hình thức, từ việc người dùng bị lộ mật khẩu, nhiễm phần mềm độc hại, cho đến các cuộc tấn công mạng quy mô lớn như đánh cắp dữ liệu khách hàng hay phá hoại hệ thống.

## 6.2. Các loại sự cố phổ biến

Một số sự cố thường gặp mà người dùng cuối cần nhận biết:

- Thiết bị cá nhân bị nhiễm phần mềm độc hại (malware, ransomware)
- Mất hoặc rò rỉ mật khẩu, tài khoản bị truy cập trái phép
- Nhận được email lừa đảo hoặc bị lừa cung cấp thông tin nhạy cảm (phishing)
- Gửi nhầm thông tin nội bộ cho đối tượng không phù hợp
- Thiết bị bị đánh cắp hoặc thất lạc
- Truy cập website giả mạo, bị tấn công khi sử dụng Wi-Fi công cộng

## 6.3. Quy trình phản ứng sự cố

Để xử lý sự cố hiệu quả và giảm thiểu thiệt hại, các tổ chức thường áp dụng **quy trình phản ứng sự cố (Incident Response Process)** gồm các bước sau:

- a) Nhận diện (Identification)
  - Xác định dấu hiệu sự cố: thiết bị hoạt động bất thường, đăng nhập trái phép, cảnh báo từ phần mềm bảo mật...
  - Phân loại mức độ nghiêm trọng: sự cố nhỏ (cá nhân) hay có khả năng ảnh hưởng toàn tổ chức?
- b) Báo cáo (Reporting)
  - Người dùng cần báo cáo ngay cho bộ phận kỹ thuật, quản trị hệ thống hoặc quản lý trực tiếp.
  - Báo cáo nên ghi rõ: thời gian xảy ra, hành vi bất thường, những gì đã bị ảnh hưởng hoặc nghi ngờ.
- c) Cách ly (Containment)
  - Ngắt kết nối thiết bị khỏi mạng nếu nghi ngờ có mã độc hoặc bị tấn công.
  - Tạm thời khóa tài khoản liên quan hoặc thay đổi mật khẩu.
- d) Xử lý (Eradication & Recovery)
  - Quét và loại bỏ mã độc (nếu có)
  - Khôi phục dữ liệu từ bản sao lưu an toàn
  - Vá lỗ hổng hệ thống, cập nhật phần mềm, điều chỉnh cấu hình bảo mật
- e) Phân tích và học hỏi (Post-Incident Analysis)
  - Ghi nhận bài học kinh nghiệm, cập nhật quy trình nếu cần
  - Đào tạo lại người dùng nếu sự cố do yếu tố con người
  - Thống kê để phòng tránh sự cố tương tự trong tương lai

## 6.4. Vai trò của người dùng cuối trong ứng phó sự cố

Người dùng cuối có thể không trực tiếp xử lý kỹ thuật nhưng đóng vai trò quan trọng trong:

- Phát hiện và báo cáo kịp thời sự cố
- Không tự ý xử lý nếu không có kiến thức chuyên môn (tránh làm tình trạng nặng hơn)

- Tuân thủ đúng quy trình được tổ chức hướng dẫn
- Tham gia diễn tập an toàn thông tin, tập huấn về kỹ năng phản ứng sự cố

### **6.5. Tác động khi không xử lý đúng cách**

Việc phát hiện chậm trễ hoặc xử lý sai sự cố có thể dẫn đến hậu quả nghiêm trọng:

- Lây lan mã độc trong mạng nội bộ
- Mất dữ liệu quan trọng, ảnh hưởng đến hoạt động kinh doanh
- Bị đánh cắp thông tin khách hàng, gây tổn thất uy tín
- Vi phạm pháp luật về bảo vệ dữ liệu và phải chịu trách nhiệm pháp lý

## **7. Xây dựng nhận thức và văn hóa bảo mật**

### **7.1. Vai trò của nhận thức bảo mật**

Trong hệ sinh thái an toàn thông tin, yếu tố con người thường được coi là mắt xích yếu nhất nhưng đồng thời cũng là điểm then chốt để phòng ngừa rủi ro. Dù hệ thống có được trang bị công nghệ hiện đại đến đâu, nếu người dùng không nhận thức được hành vi an toàn thì nguy cơ bị tấn công hoặc vi phạm vẫn luôn tiềm ẩn.

Nhận thức bảo mật là khả năng nhận biết, đánh giá và phản ứng đúng với các tình huống liên quan đến an toàn thông tin. Việc nâng cao nhận thức không chỉ bảo vệ cá nhân mà còn góp phần bảo vệ tài sản chung của tổ chức và hệ thống xã hội.

### **7.2. Hành vi người dùng ảnh hưởng đến bảo mật**

Một số hành vi tưởng như vô hại nhưng thực tế là nguyên nhân chính dẫn đến sự cố bảo mật:

- Mở liên kết trong email lạ hoặc tải tệp đính kèm không rõ nguồn gốc
- Sử dụng cùng một mật khẩu cho nhiều tài khoản
- Không khóa thiết bị khi rời khỏi vị trí làm việc
- Lưu mật khẩu trong trình duyệt mà không có mã bảo vệ
- Đăng nhập vào tài khoản cá nhân từ các thiết bị công cộng

Những hành vi này thường xuất phát từ sự thiếu nhận thức, chủ quan hoặc thiếu quy trình đào tạo phù hợp.

### **7.3. Các hình thức đào tạo và nâng cao nhận thức**

Việc xây dựng một lực lượng người dùng hiểu biết về bảo mật cần được thực hiện liên tục và bài bản thông qua:

- Khóa huấn luyện định kỳ: Trang bị kiến thức cơ bản và kỹ năng thực tế về nhận diện mối nguy cơ, sử dụng phần mềm an toàn, phản ứng với sự cố...
- Mô phỏng tấn công (phishing simulation): Giúp người dùng trải nghiệm tình huống giả lập và học cách phản ứng đúng.
- Bản tin nội bộ và áp phích cảnh báo: Nhắc nhở thường xuyên về các nguy cơ mới, mẹo an toàn, hoặc hướng dẫn nhanh.

- Kiểm tra nhận thức định kỳ: Đánh giá mức độ hiểu biết và phát hiện các lỗ hổng trong kiến thức người dùng.

#### **7.4. Xây dựng văn hóa bảo mật**

Văn hóa bảo mật không chỉ là việc tuân thủ các quy định kỹ thuật, mà là một môi trường nơi mọi người có ý thức, trách nhiệm và hành động chủ động trong việc bảo vệ thông tin. Văn hóa này cần được thể hiện qua:

- Sự gương mẫu từ lãnh đạo: Khi ban lãnh đạo thực hiện nghiêm túc các quy tắc bảo mật, nhân viên sẽ có xu hướng làm theo.
- Thái độ tích cực với việc báo cáo sự cố: Khuyến khích người dùng không che giấu sai sót, mà kịp thời báo cáo để xử lý.
- Tích hợp bảo mật vào công việc hàng ngày: Bảo mật không nên là “thêm vào”, mà phải trở thành một phần của quy trình làm việc tự nhiên.
- Ghi nhận và khen thưởng: Tạo động lực bằng cách công nhận cá nhân có hành vi bảo mật tốt.

# CHƯƠNG III. XÂY DỰNG HỆ THỐNG

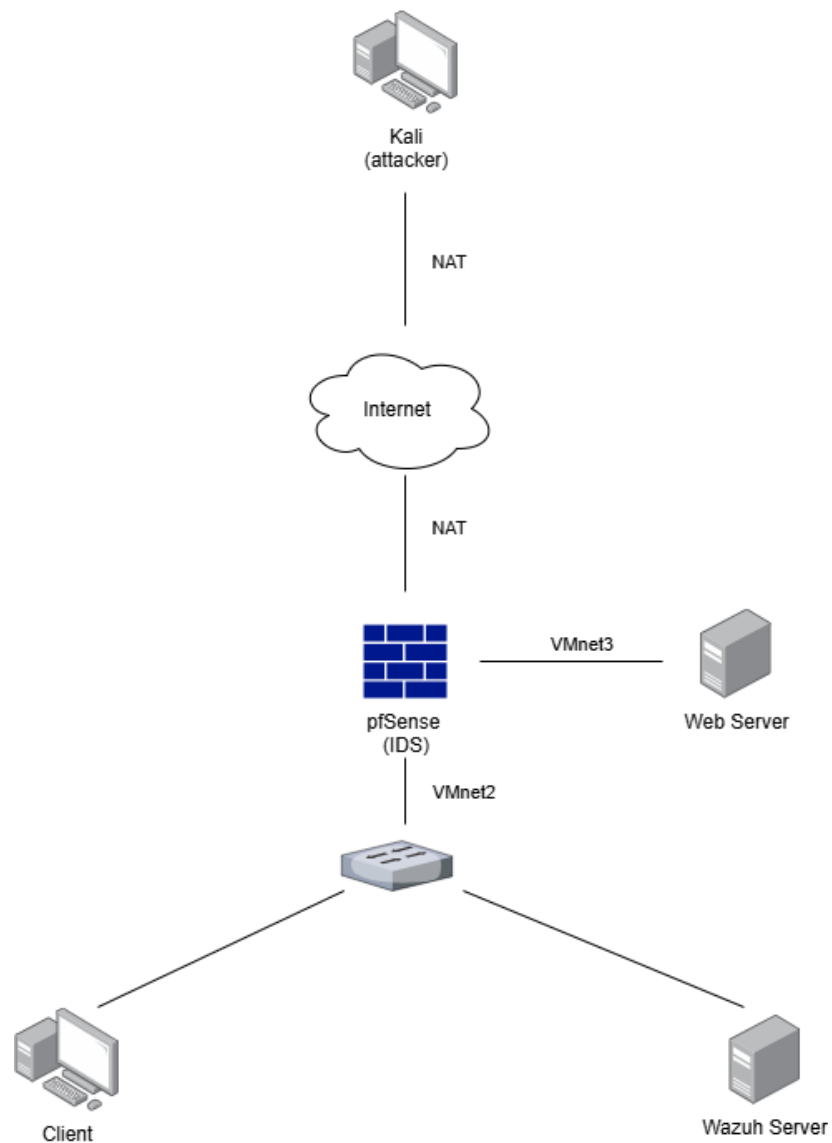
## 1. Bảng phân hoạch IP

*Bảng 1: Bảng phân hoạch IP triển khai hệ thống*

| Interface | Network Zone | Subnet        | Thiết bị              | Địa chỉ IP                     |
|-----------|--------------|---------------|-----------------------|--------------------------------|
| NAT       | WAN          | Tự VMware cấp | Kali Linux (attacker) | IP DHCP từ mạng NAT của VMware |
|           |              |               | pfSense               | IP DHCP từ mạng NAT của VMware |
| VMnet2    | LAN          | 172.0.0.0/24  | pfSense               | 172.0.0.1                      |
|           |              |               | Wazuh Server          | 172.0.0.10                     |
|           |              |               | Client                | 172.0.0.100                    |
| VMnet3    | DMZ          | 173.0.0.1/30  | pfSense               | 173.0.0.1                      |
|           |              |               | Web Server            | 173.0.0.2                      |



## 2. Sơ đồ mạng

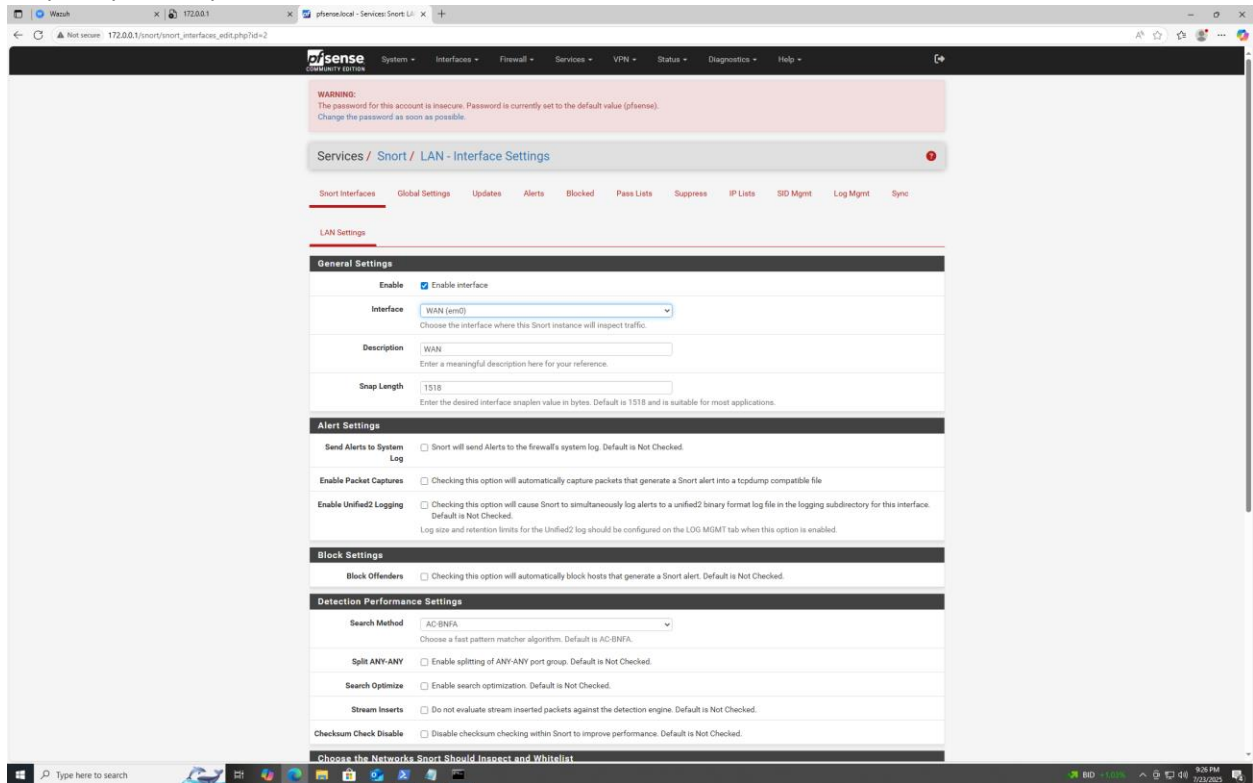


*Hình 9: Sơ đồ logic hệ thống mạng triển khai*

Vì triển khai hoàn toàn trong Vmware nên sẽ không có switch cho nên không vẽ được sơ đồ vật lý

### 3. Triển khai IDS

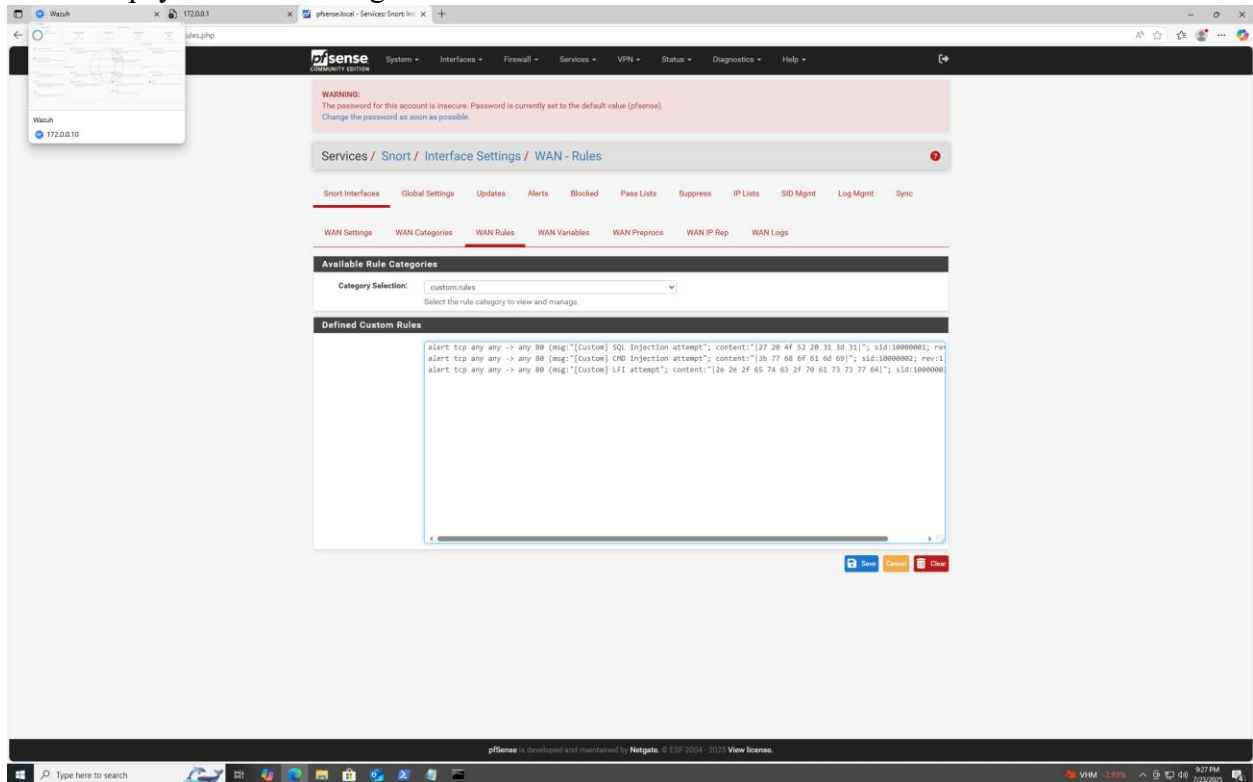
Thực hiện cài đặt Snort và khai báo interface Snort sẽ monitor



Hình 10: Bật interface để IDS monitor

Thêm rule cho Snort, những rule này thực hiện inject các lỗ hổng phổ biến tuy nhiên phải dùng

mã hash do syntax của Snort phiên bản mới không hỗ trợ syntax tương minh liên quan đến việc thêm các payload để tấn công



Hình 11: Thêm rule cho IDS

Sự kiện ghi nhận lại được tương ứng với các câu lệnh attack bên dưới

WARNING:  
The password for this account is insecure. Password is currently set to the default value (pfsense).  
Change the password as soon as possible.

Services / Snort / Alerts

Alert Log View Settings

Interface to Inspect: DMZ (em2) [v] Auto-refresh view [x] Alert lines to display: 250 [v] Save

Alert Log Actions [Download] [Clear]

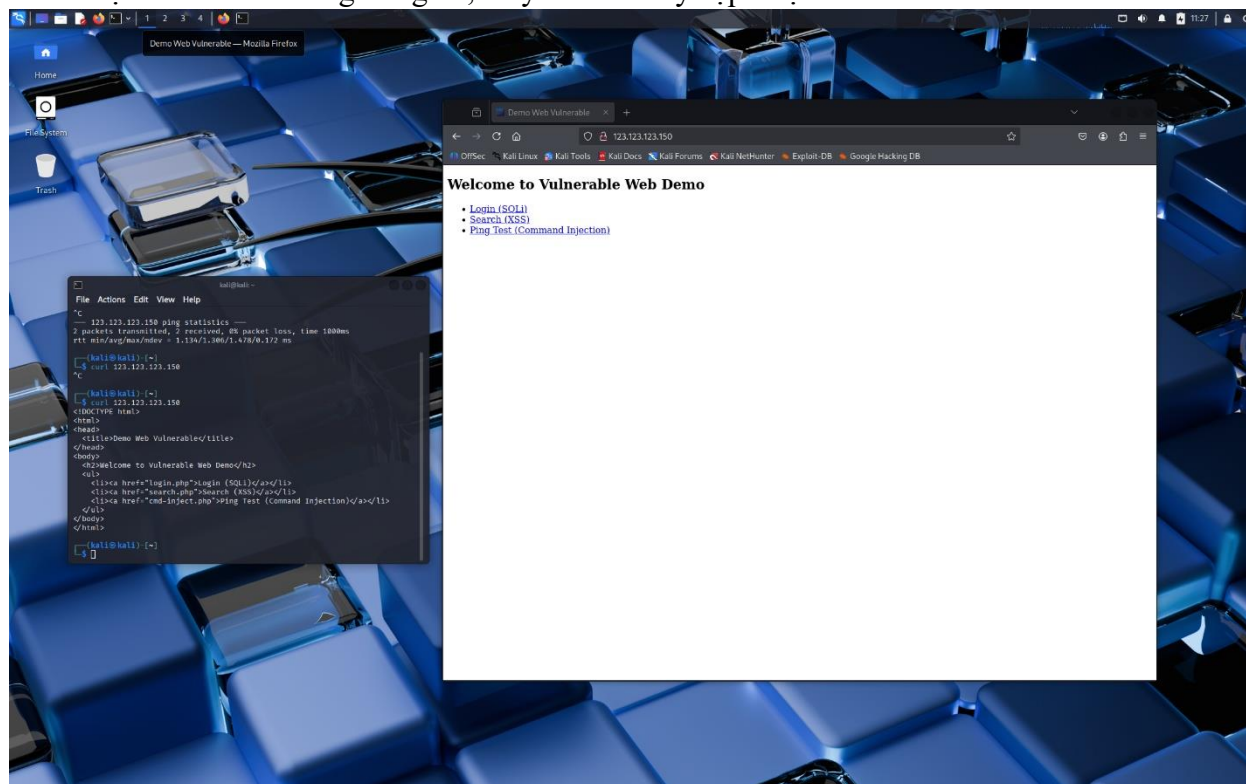
Alert Log View Filter [v]

4 Entries in Active Log

| Date                | Action         | Pri | Proto | Class                      | Source IP       | SPort | Destination IP | DPort | GUID:SID   | Description  |
|---------------------|----------------|-----|-------|----------------------------|-----------------|-------|----------------|-------|------------|--|
| 2025-07-23 19:48:13 | [Warning Icon] | 2   | TCP   | Attempted Information Leak | 123.123.123.151 | 40782 | 173.0.0.2      | 80    | 1.2049400  | ET WEB_SERVER /etc/passwd Detected in URI                    |
| 2025-07-23 19:48:13 | [Warning Icon] | 0   | TCP   |                            | 123.123.123.151 | 40782 | 173.0.0.2      | 80    | 1.10000003 | [Custom] LFI attempt   |
| 2025-07-23 19:47:04 | [Warning Icon] | 1   | TCP   | Web Application Attack     | 123.123.123.151 | 49830 | 173.0.0.2      | 80    | 1.2010920  | ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd/r) |
| 2025-07-23 19:46:29 | [Warning Icon] | 1   | TCP   | Web Application Attack     | 123.123.123.151 | 35614 | 173.0.0.2      | 80    | 1.2010920  | ET WEB_SERVER Exploit Suspected PHP Injection Attack (cmd/r) |

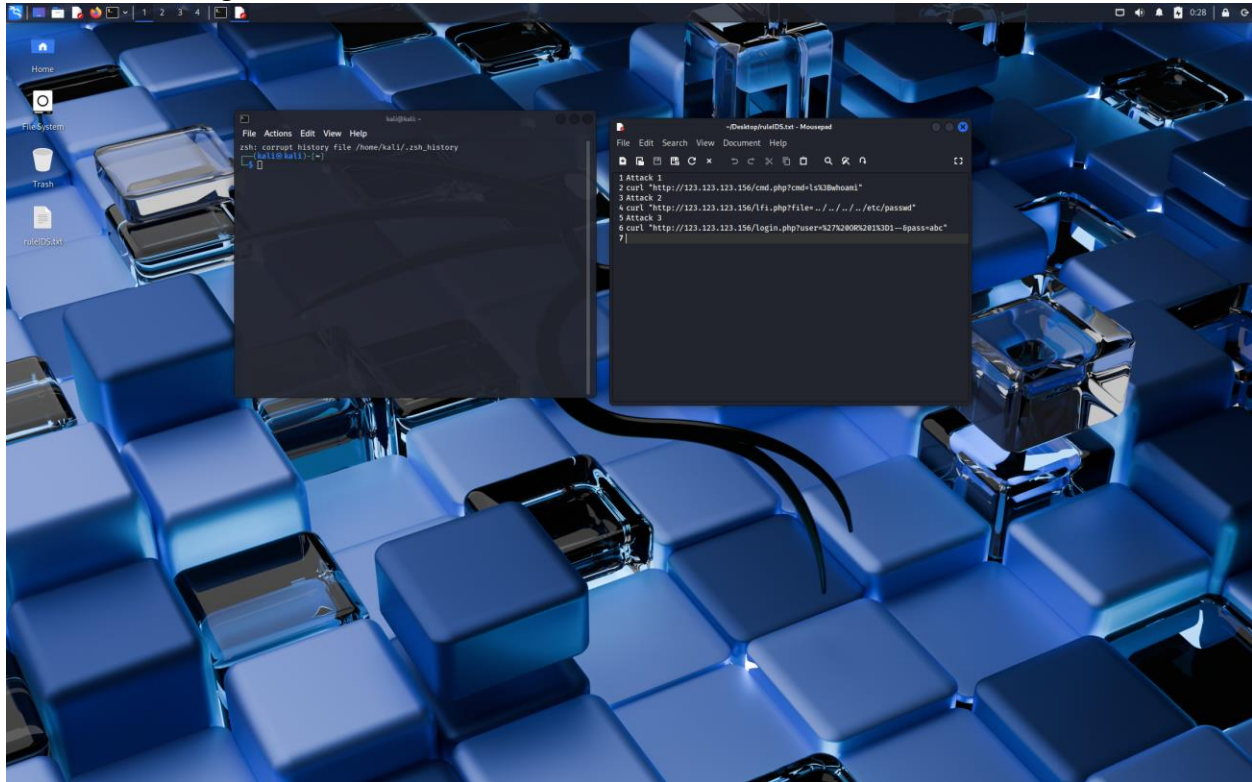
Hình 12: IDS gửi được cảnh báo khi hacker tấn công

Web được NAT Forwarding ra ngoài, máy hacker truy cập được



Hình 13: Hacker truy cập được web host ở DMZ

## Các lệnh tấn công



Hình 14: Các lệnh để tấn công web

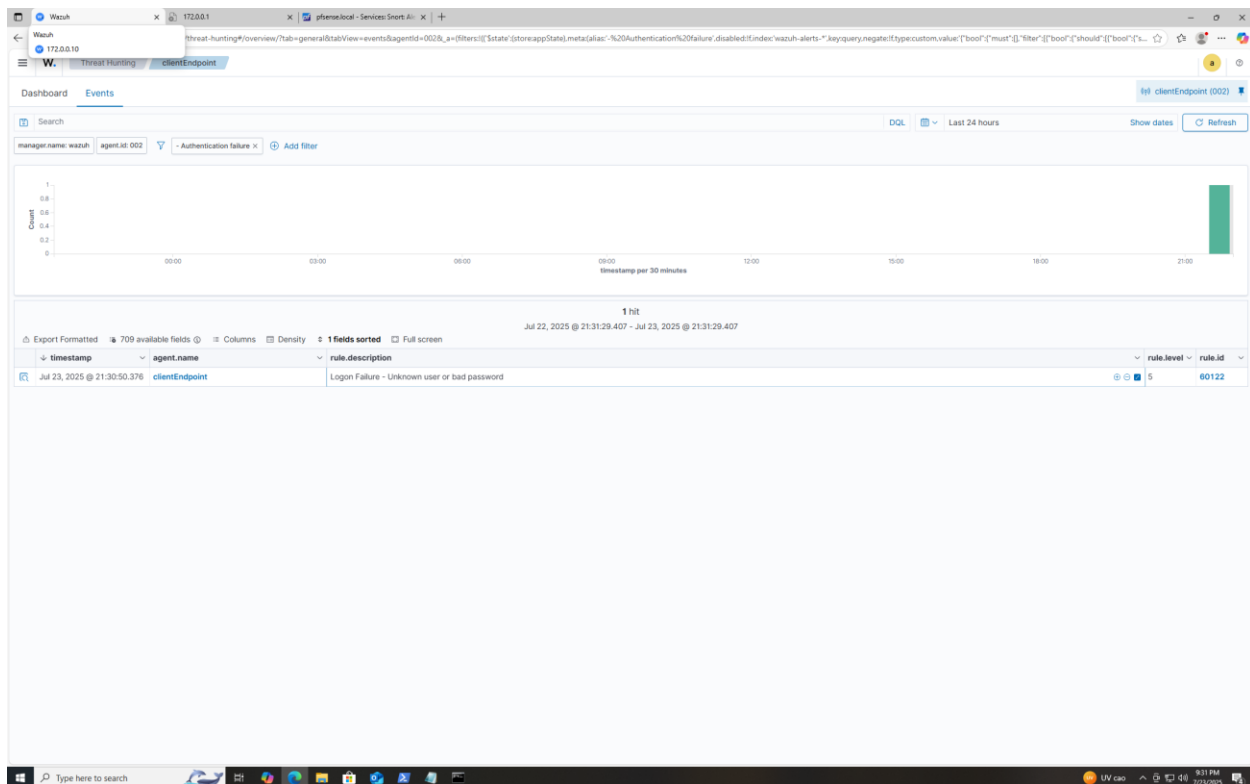
## 4. System Endpoint

### 4.1. Kịch bản 1

Người dùng thực hiện chạy ứng dụng với quyền admin nhưng không có pass và cố tình nhập sai, system endpoint sẽ ghi nhận lại

Demo bằng lệnh: `runas /user:administrator notepad` và nhập sai pass

Đây là rule đã tích hợp sẵn trong Wazuh nhằm ghi nhận việc audit hệ thống



Hình 15: System endpoint ghi nhận được log audit của người dùng cố gắng truy cập bằng tài khoản admin

## 4.2. Kịch bản 2

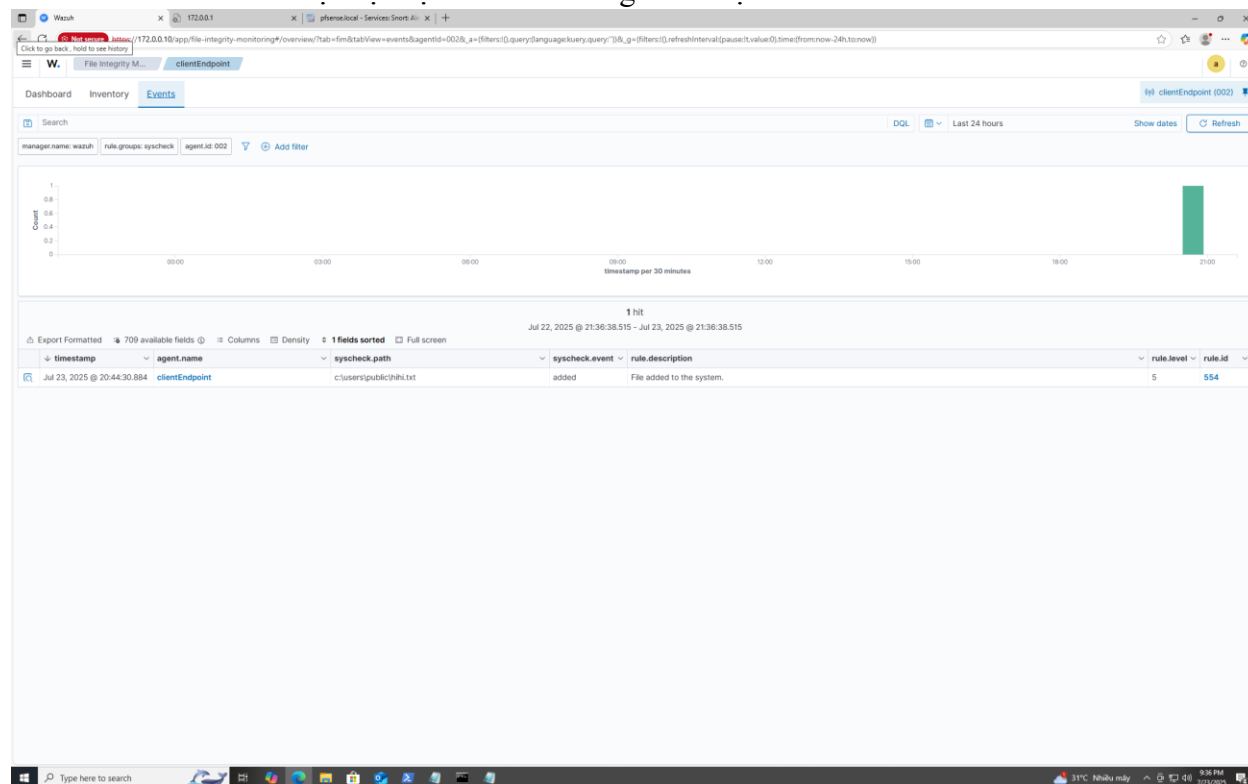
Kiểm tra tính toàn vẹn của thư mục, khi có file mới được thêm vào sẽ xuất hiện cảnh báo. Thường các mã độc sẽ tận dụng folder này để chứa file thực thi mã độc

Thêm `<directories check_all="yes" whodata="yes">C:\Users\Public</directories>` vào file cấu hình `ossec.conf` trong folder của `ossecagent` trong Program Files x86





Khi thêm vào sẽ xuất hiện sự kiện đối với đường dẫn được monitor



Hình 17: System endpoint ghi nhận được sự kiện folder monitor có file mới thêm vào

## CHƯƠNG IV. KẾT LUẬN

Kết luận về các phương pháp và giải pháp bảo mật người dùng cuối

Bảo mật người dùng cuối (endpoint security) là một trong những trụ cột quan trọng của hệ thống an toàn thông tin hiện đại. Khác với các giải pháp truyền thống chỉ tập trung bảo vệ mạng hoặc máy chủ trung tâm, bảo mật endpoint hướng đến việc bảo vệ từng thiết bị cá nhân, nơi mà kẻ tấn công thường lợi dụng như một điểm xâm nhập.

Qua quá trình nghiên cứu và triển khai, có thể rút ra một số kết luận quan trọng đối với các phương pháp và giải pháp bảo mật người dùng cuối như sau:

Không có một giải pháp duy nhất là đủ

Antivirus truyền thống tuy vẫn có vai trò nhất định, nhưng không còn đủ để đối phó với các dạng tấn công mới như ransomware, fileless malware hay các hành vi khai thác lỗ hổng zero-day.

Giải pháp phát hiện xâm nhập (HIDS, NIDS) như OSSEC, Wazuh, Snort giúp giám sát hành vi, nhật ký hệ thống và phát hiện các hành động bất thường, nhưng cần cấu hình kỹ và kết hợp nhiều nguồn dữ liệu để đạt hiệu quả cao.

EDR (Endpoint Detection & Response) và SIEM mang lại khả năng giám sát nâng cao và phản ứng kịp thời, tuy nhiên đòi hỏi tài nguyên hệ thống, kỹ năng triển khai và theo dõi liên tục.

→ Do đó, chỉ khi các giải pháp được triển khai đồng bộ, theo mô hình phòng thủ nhiều lớp (Defense-in-Depth), mới có thể đảm bảo an toàn thực sự cho người dùng cuối.

- Con người là mắt xích yếu nhất
  - + Dù có triển khai các công cụ bảo mật tiên tiến đến đâu, nếu người dùng thiếu nhận thức về an toàn thông tin (click vào file lạ, sử dụng mật khẩu yếu, chia sẻ quyền truy cập...), thì toàn bộ hệ thống vẫn có thể bị xâm nhập.
  - + Vì vậy, giáo dục và huấn luyện người dùng cuối là một phần không thể thiếu trong chiến lược bảo mật tổng thể.
- Bảo mật endpoint phải liên tục và thích ứng
  - + Các mối đe dọa mạng luôn thay đổi nhanh chóng, nên hệ thống bảo mật endpoint cũng cần có khả năng cập nhật định kỳ, mở rộng linh hoạt và tự động hóa phản ứng.
  - + Các giải pháp cần hỗ trợ tích hợp với nhau để tạo ra cái nhìn toàn diện (visibility) từ endpoint đến hệ thống trung tâm.
- Công cụ mã nguồn mở là giải pháp khả thi
  - + Trong môi trường nghiên cứu, học tập hoặc doanh nghiệp nhỏ, các công cụ mã nguồn mở như OSSEC, Wazuh, Suricata, ELK, pfSense mang lại hiệu quả bảo mật tốt với chi phí thấp, dễ tùy biến, dễ mở rộng.
  - + Tuy nhiên, cần đi kèm với kế hoạch giám sát, bảo trì và cập nhật liên tục để duy trì hiệu quả bảo vệ.

## Tổng kết

Các phương pháp và giải pháp bảo mật người dùng cuối đóng vai trò quyết định trong việc phát hiện sớm, ngăn chặn và giảm thiểu rủi ro tấn công mạng. Việc kết hợp nhiều kỹ thuật – từ antivirus, HIDS, EDR đến đào tạo người dùng – là hướng đi bền vững và hiệu quả nhất. Bảo mật endpoint không phải là đích đến, mà là một quá trình liên tục của sự giám sát, thích ứng và cải tiến theo thời gian.