**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: MẠNG MÁY TÍNH**

**ĐỀ TÀI: TÌM HIỂU VỀ BẢO MẬT MẠNG MÁY TÍNH**

**Giáo viên hướng dẫn: GV. Hoàng Trọng Nghĩa**

**Sinh viên thực hiện:** 1. Nguyễn Vũ Yến Nhi

2. Nguyễn Minh Sơn

3. Nguyễn Thị Yến

|  |  |  |  |
| --- | --- | --- | --- |
| **Stt** | **Mã sv** | **Họ và tên** | **Lớp** |
| **1** | **1771020523** | **Nguyễn Vũ Yến Nhi** | **CNTT 17-01** |
| **2** | **1771020599** | **Nguyễn Minh Sơn** | **CNTT 17-01** |
| **3** | **1771020777** | **Nguyễn Thị Yến** | **CNTT 17-01** |

**Hà Nội, năm 2025**

**BỘ GIÁO DỤC VÀ ĐÀO TẠO**

**TRƯỜNG ĐẠI HỌC ĐẠI NAM**

Logo, company name

Description automatically generated

**BÀI TẬP LỚN**

**TÊN HỌC PHẦN: MẠNG MÁY TÍNH**

**ĐỀ TÀI: TÌM HIỂU VỀ BẢO MẬT MẠNG MÁY TÍNH**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **STT** | **Mã Sinh Viên** | **Họ và Tên** | **Ngày Sinh** | **Điểm** | |
| **Bằng Số** | **Bằng Chữ** |
| **1** | **1771020523** | **Nguyễn Vũ Yến Nhi** | **22/11/2005** |  |  |
| **2** | **1771020599** | **Nguyễn Minh Sơn** | **13/11/2005** |  |  |
| **3** | **1771020777** | **Nguyễn Thị Yến** | **04/06/2005** |  |  |

**CÁN BỘ CHẤM THI 1 CÁN BỘ CHẤM THI 2**

**Hà Nội, năm 2025**

**LỜI NÓI ĐẦU**

Trong thời đại công nghệ thông tin bùng nổ, mạng máy tính đã trở thành xương sống của hầu hết các hoạt động kinh doanh, giáo dục, nghiên cứu và cả đời sống hàng ngày. Chúng ta ngày càng phụ thuộc vào Internet và các hệ thống mạng để trao đổi thông tin, thực hiện giao dịch tài chính, lưu trữ dữ liệu quan trọng cũng như kết nối với thế giới xung quanh. Tuy nhiên, bên cạnh những lợi ích to lớn mà mạng máy tính mang lại, các mối đe dọa an ninh mạng cũng ngày càng trở nên phức tạp và nguy hiểm hơn bao giờ hết.

Các cuộc tấn công mạng có thể gây ra hậu quả nghiêm trọng, từ đánh cắp thông tin cá nhân, phá hoại hệ thống dữ liệu, đến làm gián đoạn hoạt động của các tổ chức, doanh nghiệp và thậm chí cả hệ thống cơ sở hạ tầng quan trọng của một quốc gia. Những hình thức tấn công như mã độc, tấn công từ chối dịch vụ (DDoS), lừa đảo (phishing) hay xâm nhập trái phép vào hệ thống ngày càng tinh vi và khó phát hiện hơn. Chính vì vậy, bảo mật mạng máy tính đã trở thành một lĩnh vực quan trọng, đòi hỏi sự quan tâm đặc biệt từ cá nhân, tổ chức và cả chính phủ.

Việc tìm hiểu về bảo mật mạng không chỉ giúp chúng ta nhận thức được các mối đe dọa tiềm ẩn mà còn cung cấp kiến thức để áp dụng các biện pháp bảo vệ hiệu quả. Từ việc sử dụng mật khẩu mạnh, cập nhật phần mềm thường xuyên, thiết lập tường lửa, mã hóa dữ liệu cho đến các giải pháp bảo mật nâng cao như hệ thống phát hiện xâm nhập (IDS), xác thực đa yếu tố (MFA) và trí tuệ nhân tạo trong an ninh mạng – tất cả đều đóng vai trò quan trọng trong việc xây dựng một môi trường mạng an toàn.

Trong bài viết này, chúng ta sẽ cùng khám phá những khía cạnh quan trọng của bảo mật mạng máy tính, từ các khái niệm cơ bản, các mối đe dọa phổ biến cho đến các phương pháp và giải pháp giúp bảo vệ hệ thống mạng trước những nguy cơ ngày càng tinh vi. Hiểu và áp dụng bảo mật mạng không chỉ giúp bảo vệ dữ liệu cá nhân mà còn góp phần đảm bảo an toàn cho tổ chức và xã hội trong thế giới số hóa ngày nay.

**MỤC LỤC**

[CHƯƠNG 1. tổng quan về bảo mật mạng máy tính 8](#_Toc192327994)

[1.1 Khái niệm về bảo mật mạng: 8](#_Toc192327995)

[1.2 Vai trò của bảo mật mạng máy tính: 8](#_Toc192327996)

[1.2.1 Bảo vệ dữ liệu: 8](#_Toc192327997)

[1.2.2 Bảo vệ hệ thống: 9](#_Toc192327998)

[1.2.3 Bảo vệ người dùng: 9](#_Toc192327999)

[1.2.4 Bảo đảm hoạt động kinh doanh: 9](#_Toc192328000)

[1.3 Các mỗi đe dọa an ninh mạng phổ biến: 10](#_Toc192328001)

[1.3.1 Tấn công phần mềm độc hại (Malware): 10](#_Toc192328002)

[1.3.2 Tấn công từ chối dịch vụ (DDoS): 10](#_Toc192328003)

[1.3.3 Tấn công lừa đảo (Phishing): 10](#_Toc192328004)

[1.3.4 Xâm nhập trái phép (Hacking): 11](#_Toc192328005)

[1.3.5 Rò rỉ và đánh cắp dữ liệu: 11](#_Toc192328006)

[CHƯƠNG 2. các phương pháp bảo mật mạng máy tính 12](#_Toc192328007)

[2.1 Mã hóa dữ liệu: 12](#_Toc192328008)

[2.1.1 Định nghĩa: 12](#_Toc192328009)

[2.1.2 Các phương thức mã hóa phổ biến: 12](#_Toc192328010)

[2.2 Bảo mật Wifi: 13](#_Toc192328011)

[2.2.1 Các giao thức bảo mật Wi-Fi: 13](#_Toc192328012)

[2.2.2 Nguy cơ từ Wi-Fi công cộng: 13](#_Toc192328013)

[2.2.3 Các biện pháp bảo mật Wifi cá nhân: 14](#_Toc192328014)

[2.3 Tường lửa (Firewall): 14](#_Toc192328015)

[2.3.1 Định nghĩa: 14](#_Toc192328016)

[2.3.2 Phân loại tường lửa: 14](#_Toc192328017)

[2.3.3 Cách hoạt động của tường lửa: 15](#_Toc192328018)

[2.4 VPN và bảo mật khi truy cập internet: 15](#_Toc192328019)

[2.4.1 VPN (Virtual Private Network): 15](#_Toc192328020)

[2.4.2 Bảo mật khi truy cập internet: 16](#_Toc192328021)

[2.5 Xác thực người dùng: 16](#_Toc192328022)

[2.5.1 MFA (Multi-Factor Authentication): 16](#_Toc192328023)

[2.5.2 Xác thực hai yếu tố (2FA): 17](#_Toc192328024)

[CHƯƠNG 3. Tấn công mạng 18](#_Toc192328025)

[3.1 Giới thiệu về tấn công mạng: 18](#_Toc192328026)

[3.1.1 Định nghĩa: 18](#_Toc192328027)

[3.1.2 Mục tiêu: 18](#_Toc192328028)

[3.1.3 Phân loại tấn công mạng: 18](#_Toc192328029)

[3.1.4 Các giai đoạn của tấn công mạng: 19](#_Toc192328030)

[3.2 Các hình thức tấn công mạng phổ biến: 19](#_Toc192328031)

[3.2.1 Tấn công từ chối dịch vụ (DDoS): 19](#_Toc192328032)

[3.2.2 Tấn công man-in-the-middle (MITM): 21](#_Toc192328033)

[3.2.3 SQL Injection: 22](#_Toc192328034)

[CHƯƠNG 4. bảo mật mạng doanh nghiệp và cá nhÂn 23](#_Toc192328035)

[4.1 Giới thiệu về bảo mật mạng doanh nghiệp và cá nhân: 23](#_Toc192328036)

[4.1.1 Tầm quan trọng của bảo mật mạng: 23](#_Toc192328037)

[4.1.2 Những mối đe dọa phổ biến đối với bảo mật mạng: 23](#_Toc192328038)

[4.2 Bảo mật mạng doanh nghiệp: 24](#_Toc192328039)

[4.2.1 Các mối đe dọa an ninh mạng đối với doanh nghiệp: 24](#_Toc192328040)

[4.2.2 Các biện pháp bảo mật mạng doanh nghiệp: 24](#_Toc192328041)

[4.3 Bảo mật mạng cá nhân: 25](#_Toc192328042)

[4.3.1 Các mối đe dọa an ninh mạng đối với cá nhân: 25](#_Toc192328043)

[4.3.2 Các biện pháp bảo mật mạng cá nhân: 25](#_Toc192328044)

[CHƯƠNG 5. Công cụ bảo mật và thực hành 27](#_Toc192328045)

[5.1 Giới thiệu về công cụ bảo mật mạng: 27](#_Toc192328046)

[5.1.1 Tầm quan trọng của công cụ bảo mật: 27](#_Toc192328047)

[5.1.2 Phân loại công cụ bảo mật: 27](#_Toc192328048)

[5.2 Công cụ phân tích mạng Wireshark: 28](#_Toc192328049)

[5.2.1 Giới thiệu: 28](#_Toc192328050)

[5.2.2 Chức năng chính của Wireshark: 28](#_Toc192328051)

[5.2.3 Ứng dụng của Wireshark: 28](#_Toc192328052)

[5.3 Công cụ phát hiện xâm nhập Snort: 29](#_Toc192328053)

[5.3.1 Giới thiệu: 29](#_Toc192328054)

[5.3.2 Chức năng chính của Snort: 29](#_Toc192328055)

[5.4 Công cụ kiểm thử xâm nhập Metasploit: 29](#_Toc192328056)

[5.4.1 Giới thiệu: 29](#_Toc192328057)

[5.4.2 Chức năng: 30](#_Toc192328058)

[5.5 Hướng dẫn cơ bản về kiểm thử bảo mật mạng: 30](#_Toc192328059)

[5.5.1 Các giai đoạn của kiểm thử bảo mật mạng: 30](#_Toc192328060)

[5.5.2 Các kỹ thuật kiểm thử bảo mật mạng: 30](#_Toc192328061)

[5.6 Thực hành kiểm thử bảo mật mạng cơ bản: 31](#_Toc192328062)

[5.6.1 Sử dụng Nmap để quét cổng: 31](#_Toc192328063)

[5.6.2 Sử dụng Wireshark để phân tích lưu lượng mạng: 31](#_Toc192328064)

[5.6.3 Sử dụng Metasploit để khai thác lỗ hổng: 31](#_Toc192328065)

[5.6.4 Sử dụng Snort để phát hiện xâm nhập: 31](#_Toc192328066)

[CHƯƠNG 6. Xu hướng bảo mật mạng trong tương lai 32](#_Toc192328067)

[6.1 Bảo mật AI và Machine Learning: 32](#_Toc192328068)

[6.1.1 Sự phát triển của AI và Machine Learning trong bảo mật: 32](#_Toc192328069)

[6.1.2 Các ứng dụng của AI và Machine Learning trong bảo mật: 32](#_Toc192328070)

[6.2 Bảo mật mạng trong IoT: 33](#_Toc192328071)

[6.2.1 Sự gia tăng của thiết bị IoT: 33](#_Toc192328072)

[6.2.2 Các biện pháp bảo mật IoT: 33](#_Toc192328073)

[6.3 Zero Trust Security Model: 33](#_Toc192328074)

[6.3.1 Mô hình bảo mật Zero Trust: 33](#_Toc192328075)

[6.3.2 Các nguyên tắc của Zero Trust: 34](#_Toc192328076)

[6.3.3 Lợi ích của Zero Trust: 34](#_Toc192328077)

[6.3.4 Xu hướng phát triển: 34](#_Toc192328078)

**MỤC LỤC HÌNH ẢNH**

[Hình 1.1. Bảo mật mạng máy tính 9](#_Toc192328079)

[Hình 2.1. SSL/TLS 13](#_Toc192328080)

[Hình 2.2. RSA 13](#_Toc192328081)

[Hình 2.3. WPA2 14](#_Toc192328082)

[Hình 2.4. Firewall 15](#_Toc192328083)

[Hình 2.5. VPN 16](#_Toc192328084)

[Hình 3.1. Tấn công mạng 19](#_Toc192328085)

[Hình 3.2. Tấn công từ chối dịch vụ (DDoS) 20](#_Toc192328086)

[Hình 3.3. MITM 21](#_Toc192328087)

[Hình 3.4. SQL Injection 23](#_Toc192328088)

[Hình 5.1. Wireshark 28](#_Toc192328089)

[Hình 5.2. Snort 29](#_Toc192328090)

[Hình 5.3. Metasploit 30](#_Toc192328091)

[Hình 6.1. AI & Machine Learning 33](#_Toc192328092)

[Hình 6.2. IoT 34](#_Toc192328093)

[Hình 6.3. Zero Trust Security Model 35](#_Toc192328094)

# tổng quan về bảo mật mạng máy tính

## Khái niệm về bảo mật mạng:

Bảo mật mạng máy tính là việc đảm bảo rằng thông tin của cá nhân, tập thể, công ty hoặc doanh nghiệp luôn được bảo vệ, ngăn chặn việc truy cập trái phép vào dữ liệu.



Hình 1.1. Bảo mật mạng máy tính

## Vai trò của bảo mật mạng máy tính:

### Bảo vệ dữ liệu:

*Ngăn chặn truy cập trái phép:* Bảo mật mạng giúp ngăn chặn những kẻ tấn công truy cập trái phép vào hệ thống và đánh cắp dữ liệu quan trọng.

*Bảo vệ tính toàn vẹn của dữ liệu:* Bảo mật mạng đảm bảo rằng dữ liệu không bị thay đổi hoặc phá hủy bởi các tác nhân độc hại.

*Bảo vệ tính khả dụng của dữ liệu:* Bảo mật mạng đảm bảo rằng dữ liệu luôn sẵn sàng khi người dùng cần.

### Bảo vệ hệ thống:

*Ngăn chặn phần mềm độc hại:* Bảo mật mạng giúp ngăn chặn virus, mã độc và các phần mềm độc hại khác xâm nhập vào hệ thống.

*Ngăn chặn tấn công từ chối dịch vụ (DoS):* Bảo mật mạng giúp ngăn chặn các cuộc tấn công DoS làm tê liệt hệ thống.

*Bảo vệ các thiết bị mạng:* Bảo mật mạng giúp bảo vệ các thiết bị mạng như router, switch và firewall khỏi các cuộc tấn công.

### Bảo vệ người dùng:

*Bảo vệ quyền riêng tư:* Bảo mật mạng giúp bảo vệ thông tin cá nhân của người dùng khỏi bị đánh cắp hoặc lạm dụng.

*Bảo vệ tài khoản trực tuyến:* Bảo mật mạng giúp bảo vệ tài khoản ngân hàng, email và các tài khoản trực tuyến khác của người dùng khỏi bị hack.

*Đảm bảo an toàn khi giao dịch trực tuyến:* Bảo mật mạng giúp đảm bảo rằng các giao dịch trực tuyến của người dùng được thực hiện an toàn.

### Bảo đảm hoạt động kinh doanh:

*Bảo vệ tài sản trí tuệ:* Bảo mật mạng giúp bảo vệ các tài sản trí tuệ của doanh nghiệp như bí mật kinh doanh và bằng sáng chế.

*Đảm bảo hoạt động liên tục:* Bảo mật mạng giúp đảm bảo rằng hệ thống của doanh nghiệp luôn hoạt động ổn định và không bị gián đoạn.

*Tạo dựng niềm tin với khách hàng:* Bảo mật mạng giúp tạo dựng niềm tin với khách hàng rằng thông tin của họ được bảo vệ an toàn.

## Các mỗi đe dọa an ninh mạng phổ biến:

### Tấn công phần mềm độc hại (Malware):

Phần mềm độc hại là bất kỳ phần mềm nào được thiết kế để gây hại cho hệ thống máy tính, mạng hoặc dữ liệu. Bao gồm virus, worm, trojan, ransomware, spyware, và adware.

Cách thức hoạt động:

* Lây lan qua email, trang web độc hại, USB, hoặc các lỗ hổng phần mềm.
* Gây ra các thiệt hại như đánh cắp dữ liệu, phá hủy hệ thống, hoặc mã hóa dữ liệu đòi tiền chuộc.

Ví dụ:

* WannaCry (ransomware): Mã hóa dữ liệu và đòi tiền chuộc.
* Emotet (trojan): Đánh cắp thông tin tài chính và lây lan sang các hệ thống khác.

### Tấn công từ chối dịch vụ (DDoS):

Tấn công DDoS làm quá tải hệ thống mục tiêu bằng lượng lớn lưu lượng truy cập, khiến hệ thống không thể phục vụ người dùng hợp pháp.

Cách thức hoạt động:

* Sử dụng mạng botnet (các máy tính bị nhiễm độc) để tạo ra lượng truy cập lớn.
* Gây ra sự gián đoạn dịch vụ, thiệt hại về tài chính và uy tín.

Ví dụ: Các cuộc tấn công DDoS vào các trang web của ngân hàng hoặc chính phủ.

### Tấn công lừa đảo (Phishing):

Tấn công lừa đảo sử dụng các email, tin nhắn hoặc trang web giả mạo để đánh lừa người dùng cung cấp thông tin cá nhân.

Cách thức hoạt động:

* Kẻ tấn công giả mạo các tổ chức uy tín để lừa người dùng tiết lộ mật khẩu, thông tin tài khoản ngân hàng, hoặc số thẻ tín dụng.
* Gây ra thiệt hại về tài chính và đánh cắp danh tính.

Ví dụ: Email giả mạo từ ngân hàng yêu cầu người dùng xác nhận thông tin tài khoản.

### Xâm nhập trái phép (Hacking):

Xâm nhập trái phép là hành động truy cập vào hệ thống máy tính hoặc mạng mà không được phép.

Cách thức hoạt động:

* Kẻ tấn công khai thác các lỗ hổng bảo mật để xâm nhập vào hệ thống.
* Gây ra thiệt hại như đánh cắp dữ liệu, phá hoại hệ thống hoặc cài đặt phần mềm độc hại.

Ví dụ: Kẻ tấn công xâm nhập vào hệ thống của một công ty để đánh cắp thông tin khách hàng.

### Rò rỉ và đánh cắp dữ liệu:

Rò rỉ dữ liệu là sự cố mà thông tin nhạy cảm bị lộ ra ngoài do lỗi bảo mật hoặc tấn công mạng. Đánh cắp dữ liệu là hành động tội phạm khi kẻ tấn công có được thông tin giá trị.

Cách thức hoạt động:

* Do lỗi bảo mật, nhân viên nội bộ, hoặc tấn công mạng.
* Gây ra thiệt hại về tài chính, uy tín và pháp lý.

Ví dụ: Thông tin thẻ tín dụng của khách hàng bị rò rỉ từ cơ sở dữ liệu của một công ty.

# các phương pháp bảo mật mạng máy tính

## Mã hóa dữ liệu:

### Định nghĩa:

Mã hóa dữ liệu là quá trình chuyển đổi dữ liệu từ dạng có thể đọc được (plaintext) sang dạng không thể đọc được (ciphertext) để bảo vệ tính bảo mật của dữ liệu.

Chỉ những người có khóa giải mã phù hợp mới có thể chuyển đổi ciphertext trở lại plaintext.

### Các phương thức mã hóa phổ biến:

#### SSL/TLS (Secure Sockets Layer/Transport Layer Security):



Hình 2.1. SSL/TLS

Sử dụng để mã hóa dữ liệu truyền qua internet, đặc biệt là trong các giao dịch trực tuyến.

Đảm bảo tính bảo mật và toàn vẹn của dữ liệu giữa trình duyệt và máy chủ web.

#### AES (Advanced Encryption Standard):

Một thuật toán mã hóa đối xứng phổ biến, được sử dụng rộng rãi trong nhiều ứng dụng bảo mật.

Mã hóa và giải mã dữ liệu bằng cùng một khóa.

#### RSA Algorithm in Cryptography: Rivest Shamir Adleman Explained | SplunkRSA (Rivest-Shamir-Adleman):

Hình 2.2. RSA

Một thuật toán mã hóa bất đối xứng, sử dụng hai khóa khác nhau: khóa công khai (public key) và khóa riêng tư (private key).

Khóa công khai được sử dụng để mã hóa dữ liệu, và khóa riêng tư được sử dụng để giải mã dữ liệu.

## Bảo mật Wifi:

Hình 2.3. WPA2

### Các giao thức bảo mật Wi-Fi:

* WPA2 (Wi-Fi Protected Access 2):
  + Một giao thức bảo mật Wi-Fi mạnh mẽ, sử dụng thuật toán mã hóa AES.
  + Được khuyến nghị sử dụng cho hầu hết các mạng Wi-Fi.
* WPA3 (Wi-Fi Protected Access 3):
  + Giao thức bảo mật Wi-Fi mới nhất, cung cấp khả năng bảo mật cao hơn so với WPA2.
  + Bổ sung các tính năng bảo mật như mã hóa cá nhân hóa và bảo vệ chống lại các cuộc tấn công đoán mật khẩu.

### Nguy cơ từ Wi-Fi công cộng:

* Wi-Fi công cộng thường không được bảo mật, khiến dữ liệu của người dùng dễ bị đánh cắp.
* Kẻ tấn công có thể tạo ra các điểm truy cập Wi-Fi giả mạo để đánh lừa người dùng.
* Người dùng nên tránh truy cập các thông tin nhạy cảm khi sử dụng Wi-Fi công cộng.

### Các biện pháp bảo mật Wifi cá nhân:

*Đổi tên SSID và ẩn SSID:* Đặt tên Wi-Fi (SSID) không tiết lộ thông tin cá nhân hoặc tên nhà mạng. Có thể ẩn SSID để hạn chế khả năng bị phát hiện bởi người lạ.

*Sử dụng mật khẩu mạnh*: Đặt mật khẩu dài, chứa chữ hoa, chữ thường, số và ký tự đặc biệt.

*Bật tường lửa và lọc địa chỉ MAC*: Bật Firewall trên router để chặn truy cập trái phép. Lọc địa chỉ MAC để chỉ cho phép các thiết bị được xác nhận kết nối vào mạng.

*Cập nhật firmware router thường xuyên*: Các bản cập nhật giúp sửa lỗi bảo mật và nâng cao hiệu suất router.

## Tường lửa (Firewall):

### Định nghĩa:



Hình 2.4. Firewall

Tường lửa là một hệ thống bảo mật mạng, giám sát và kiểm soát lưu lượng mạng ra vào hệ thống. Cho phép hoặc chặn lưu lượng mạng dựa trên các quy tắc bảo mật được xác định trước.

### Phân loại tường lửa:

#### Tường lửa phần cứng:

* Thiết bị vật lý được cài đặt giữa mạng nội bộ và internet.
* Cung cấp hiệu suất cao và khả năng bảo mật mạnh mẽ.

#### Tường lửa phần mềm:

* Phần mềm được cài đặt trên máy tính hoặc máy chủ.
* Cung cấp khả năng bảo vệ cho từng thiết bị riêng lẻ.

### Cách hoạt động của tường lửa:

* Lọc gói tin (Packet Filtering Firewall).
* Kiểm tra trạng thái kết nối (Stateful Inspection Firewall).
* Firewall Proxy (Application-Level Firewall).
* Firewall thế hệ mới (Next-Generation Firewall – NGFW).

## VPN và bảo mật khi truy cập internet:

### VPN (Virtual Private Network):

* Tạo ra một kết nối mạng riêng ảo, mã hóa lưu lượng truy cập internet của người dùng.
* Giúp bảo vệ quyền riêng tư và bảo mật của người dùng khi truy cập internet.
* ẩn địa chỉ IP người dùng.



Hình 2.5. VPN

*Cách thức hoạt động:*

* Khi kết nối với VPN, lưu lượng truy cập internet sẽ được chuyển hướng qua một máy chủ VPN.
* Máy chủ VPN sẽ mã hóa dữ liệu và ẩn địa chỉ IP.
* Điều này khiến cho việc theo dõi hoạt động trực tuyến trở nên khó khăn hơn.

### Bảo mật khi truy cập internet:

* Sử dụng VPN khi truy cập các trang web nhạy cảm hoặc sử dụng Wi-Fi công cộng.
* Sử dụng mật khẩu mạnh và duy nhất.
* Cập nhật phần mềm diệt virus và phần mềm bảo mật thường xuyên.
* Cẩn thận với các email và trang web lừa đảo.

## Xác thực người dùng:

### MFA (Multi-Factor Authentication):

#### Định nghĩa:

MFA (Multi-Factor Authentication) – Xác thực đa yếu tố là một phương thức bảo mật yêu cầu người dùng xác minh danh tính bằng nhiều yếu tố thay vì chỉ một mật khẩu. Điều này giúp tăng cường bảo mật, ngăn chặn truy cập trái phép ngay cả khi mật khẩu bị lộ.

#### Các yếu tố xác thực trong MFA:

MFA thường kết hợp ít nhất hai trong ba yếu tố xác thực sau:

* Yếu tố kiến thức (Knowledge Factor) – Những gì người dùng biết như: mật khẩu, mã PIN, câu hỏi bảo mật.
* Yếu tố sở hữu (Possession Factor) – Những gì người dùng có như: điện thoại di động, USB bảo mật, thẻ thông minh.
* Yếu tố sinh trắc học (Inherence Factor) – Đặc điểm sinh học của người dùng: vân tay, nhận diện khuôn mặt, quét võng mạc, giọng nói.

#### Cách hoạt động của MFA:

* Bước 1: Người dùng nhập tên đăng nhập và mật khẩu.
* Bước 2: Hệ thống yêu cầu xác thực bằng một yếu tố khác, như mã OTP qua SMS hoặc ứng dụng xác thực.
* Bước 3: Nếu xác minh thành công, người dùng được cấp quyền truy cập.

### Xác thực hai yếu tố (2FA):

#### Định nghĩa:

2FA (Two-Factor Authentication – Xác thực hai yếu tố) là một dạng của MFA (Xác thực đa yếu tố) yêu cầu người dùng cung cấp hai phương thức xác thực khác nhau để đăng nhập vào hệ thống hoặc tài khoản trực tuyến.

#### Cách hoạt động của 2FA:

* Yếu tố kiến thức: mật khẩu, mã PIN, câu hỏi bảo mật.
* Yếu tố sở hữu: Mã OTP qua SMS, ứng dụng xác thực (Google Authenticator, Microsoft Authenticator), khóa bảo mật phần cứng (YubiKey).
* Yếu tố sinh trắc học: Vân tay, nhận diện khuôn mặt, quét võng mạc

#### Các phương thức xác thực 2FA phổ biến:

*Mã OTP qua SMS, Email:* Hệ thống gửi mã OTP (One-Time Password) đến số điện thoại hoặc email.

* Dễ sử dụng và không cần ứng dụng bên thứ ba.

*Ứng dụng xác thực (Authenticator Apps):* Các ứng dụng phổ biến: Google Authenticator, Microsoft Authenticator, Authy.

* An toàn hơn OTP qua SMS vì không phụ thuộc vào mạng di động.

*Khóa bảo mật phần cứng (Security Key):* Thiết bị như: YubiKey, Titan Security Key.

* Bảo mật cao, không thể bị tấn công từ xa.

# Tấn công mạng

## Giới thiệu về tấn công mạng:

### Tấn công mạng là gì? Ví dụ về tấn công mạng? Trách nhiệm phòng ngừa tình huống nguy hiểm về an ninh mạng đối với lực lượng chuyên trách bảo vệ anĐịnh nghĩa:

Hình 3.1. Tấn công mạng

Tấn công mạng là hành động cố ý xâm nhập, phá hoại hoặc gây gián đoạn hoạt động của hệ thống mạng, máy tính hoặc thiết bị kết nối.

### Mục tiêu:

Mục tiêu của tấn công mạng có thể là đánh cắp dữ liệu, phá hoại hệ thống, tống tiền hoặc gây gián đoạn dịch vụ.

### Phân loại tấn công mạng:

#### Tấn công từ bên ngoài:

Tấn công từ bên ngoài là những cuộc tấn công được thực hiện bởi các đối tượng không có quyền truy cập hợp lệ vào hệ thống hoặc mạng của tổ chức. Tin tặc có thể sử dụng nhiều phương pháp khác nhau để xâm nhập, đánh cắp thông tin hoặc làm gián đoạn hoạt động của hệ thống.

#### Tấn công từ bên trong:

Tấn công từ bên trong xảy ra khi người có quyền truy cập hợp lệ vào hệ thống (nhân viên, đối tác, nhà cung cấp) cố tình hoặc vô tình gây ra rủi ro bảo mật. Những cuộc tấn công này khó phát hiện hơn vì kẻ tấn công đã có quyền truy cập vào hệ thống.

### Các giai đoạn của tấn công mạng:

* Trinh sát (reconnaissance): Thu thập thông tin về mục tiêu.
* Quét lỗ hổng (scanning): Tìm kiếm các lỗ hổng bảo mật.
* Xâm nhập (exploitation): Khai thác lỗ hổng để xâm nhập vào hệ thống.
* Duy trì quyền truy cập (maintaining access): Cài đặt backdoor để duy trì quyền truy cập.
* Xóa dấu vết (covering tracks): Xóa nhật ký hoạt động để che giấu hành vi.

## Các hình thức tấn công mạng phổ biến:

### Tấn công từ chối dịch vụ (DDoS):

#### DDoS Là Gì? Tấn Công DDoS Là Gì?Định nghĩa:

Hình 3.2. Tấn công từ chối dịch vụ (DDoS)

DDoS (Distributed Denial of Service – Tấn công từ chối dịch vụ phân tán) là một hình thức tấn công mạng nhằm làm quá tải máy chủ, website hoặc hệ thống mạng bằng cách gửi một lượng lớn yêu cầu từ nhiều thiết bị khác nhau.

Mục tiêu của DDoS là khiến hệ thống không thể xử lý kịp lượng truy cập và dẫn đến tình trạng chậm chạp hoặc ngừng hoạt động hoàn toàn.

**Ví dụ:** Một website thương mại điện tử bị tấn công DDoS vào ngày giảm giá, khiến khách hàng không thể truy cập để mua hàng.

#### Cách thức hoạt động:

DDoS hoạt động bằng cách tạo ra lưu lượng truy cập giả mạo để làm cạn kiệt tài nguyên của hệ thống. Gồm 3 bước chính:

* + Bước 1: Tin tặc thiết lập mạng botnet.
* Hacker lây nhiễm mã độc vào hàng ngàn máy tính, thiết bị IoT (camera an ninh, router, điện thoại thông minh).
  + Bước 2: Botnet gửi lưu lượng truy cập lớn đến mục tiêu.
* Hacker chỉ đạo botnet gửi hàng triệu yêu cầu giả mạo đến hệ thống mục tiêu.
  + Bước 3: Hệ thống mục tiêu bị quá tải và ngừng hoạt động. Máy chủ hoặc mạng không thể xử lý hết lượng yêu cầu, dẫn đến:
* Giảm tốc độ (chậm phản hồi, trang web load lâu).
* Ngừng hoạt động hoàn toàn (không thể truy cập).
* Tốn tài nguyên hệ thống và gây thiệt hại tài chính.

#### Các loại tấn công DDoS:

*Tấn công dựa trên lưu lượng (Volumetric Attack):* Gây nghẽn băng thông bằng cách gửi lượng lớn dữ liệu đến hệ thống.

* Ví dụ: Hacker dùng botnet gửi hàng triệu gói tin UDP đến một website, làm nghẽn toàn bộ đường truyền mạng.

*Tấn công giao thức (Protocol Attack):* Lợi dụng lỗ hổng của giao thức mạng để tiêu tốn tài nguyên máy chủ.

* Ví dụ: Hacker gửi hàng triệu yêu cầu kết nối TCP nhưng không hoàn tất, làm hệ thống cạn kiệt tài nguyên.

*Tấn công ứng dụng (Application Layer Attack):* Nhắm vào các ứng dụng web hoặc dịch vụ trực tuyến, gây quá tải.

* Ví dụ: Botnet gửi hàng triệu yêu cầu HTTP GET/POST đến website, làm máy chủ quá tải.

### Tấn công man-in-the-middle (MITM):

#### A diagram of a computer connection AI-generated content may be incorrect.Định nghĩa:

Hình 3.3. MITM

Tấn công Man-in-the-Middle (MITM) là một hình thức tấn công trung gian, trong đó kẻ tấn công chen vào giữa hai bên giao tiếp để đánh cắp, thay đổi hoặc chặn thông tin mà không bị phát hiện.

**Ví dụ:** Khi bạn đăng nhập vào ngân hàng trực tuyến, kẻ tấn công có thể chặn thông tin đăng nhập của bạn nếu kết nối không an toàn.

#### Cách thức hoạt động:

* Bước 1: Kẻ tấn công chặn kết nối.
* Kẻ tấn công xâm nhập vào đường truyền giữa người dùng và máy chủ.
* Điều này có thể xảy ra trên Wi-Fi công cộng, mạng nội bộ không bảo mật
* Bước 2: Đánh chặn và thao túng dữ liệu.
* Kẻ tấn công đọc, thay đổi hoặc ghi lại dữ liệu mà người dùng gửi đi.
* Nếu dữ liệu không được mã hóa, tin tặc có thể thu thập thông tin như mật khẩu, số thẻ tín dụng.
* Bước 3: Gửi dữ liệu đã chỉnh sửa đến đích.
* Sau khi đánh cắp hoặc thay đổi thông tin, kẻ tấn công tiếp tục chuyển dữ liệu đến máy chủ hoặc người dùng để tránh bị phát hiện.
* Kết quả là người dùng không hề nhận ra rằng họ đang bị theo dõi hoặc thao túng dữ liệu.

#### Các loại tấn công MITM phổ biến:

* ARP Spoofing (Giả mạo ARP): Kẻ tấn công gửi các gói tin giả mạo trong mạng nội bộ (LAN) để đánh lừa thiết bị nạn nhân, khiến dữ liệu được gửi đến hacker thay vì máy chủ thật.
* Ví dụ: Hacker trong quán cà phê chặn kết nối giữa bạn và bộ định tuyến (router), sau đó thu thập dữ liệu cá nhân.
* DNS Spoofing (Giả mạo DNS): Kẻ tấn công thay đổi kết quả tra cứu DNS, khiến nạn nhân truy cập vào một trang web giả mạo thay vì trang web chính thống.
* Ví dụ: Bạn gõ địa chỉ "banking.com", nhưng kẻ tấn công điều hướng bạn đến một trang web giả mạo giống hệt, nơi bạn nhập mật khẩu mà không hay biết.
* HTTPS Stripping (Loại bỏ HTTPS): Kẻ tấn công buộc trình duyệt của nạn nhân chuyển từ HTTPS (bảo mật) sang HTTP (không bảo mật) để có thể theo dõi dữ liệu.
* Ví dụ: Khi bạn đăng nhập vào email, hacker chặn yêu cầu HTTPS và buộc trình duyệt sử dụng HTTP, khiến thông tin của bạn dễ bị đánh cắp.

### What is SQL Injection? Tutorial & Examples | Web Security AcademySQL Injection:

Hình 3.4. SQL Injection

#### Định nghĩa:

SQL Injection (SQLi) là một kỹ thuật tấn công mạng trong đó hacker chèn (inject) các đoạn mã SQL độc hại vào các truy vấn của ứng dụng web để thao túng hoặc truy cập trái phép vào cơ sở dữ liệu. Nếu ứng dụng không kiểm soát đầu vào chặt chẽ, hacker có thể đánh cắp dữ liệu, xóa bảng, thậm chí chiếm quyền điều khiển hệ thống.

#### Cách hoạt động của SQL Injection:

SQL Injection khai thác lỗ hổng bảo mật từ các ứng dụng web sử dụng truy vấn SQL nhưng không kiểm tra đầu vào của người dùng đúng cách. Tin tặc có thể chèn mã SQL vào các ô nhập dữ liệu như:

* Form đăng nhập (username, password)
* Thanh tìm kiếm
* URL parameters
* API request

#### Các loại SQL Injection phổ biến:

* Tấn công SQL Injection truyền thống (Classic SQLi): Hacker trực tiếp nhập mã SQL độc hại vào các trường input (username, password, search bar, v.v.).
* Tấn công SQLi dựa trên lỗi (Error-Based SQLi): Hacker khai thác thông báo lỗi từ cơ sở dữ liệu để lấy thông tin bảng, cột.
* Tấn công SQLi mù (Blind SQLi): Hệ thống không hiển thị lỗi nhưng hacker có thể gửi truy vấn và quan sát phản hồi (đúng/sai).
* Tấn công SQLi nội suy (Union-Based SQLi): Hacker sử dụng câu lệnh UNION SELECT để hợp nhất dữ liệu từ nhiều bảng.

# bảo mật mạng doanh nghiệp và cá nhÂn

## Giới thiệu về bảo mật mạng doanh nghiệp và cá nhân:

### Tầm quan trọng của bảo mật mạng:

#### Đối với doanh nghiệp:

Một cuộc tấn công mạng có thể gây rò rỉ dữ liệu khách hàng, ảnh hưởng đến uy tín, thiệt hại tài chính và gián đoạn hoạt động kinh doanh. Do đó, việc xây dựng hệ thống bảo mật mạnh mẽ giúp doanh nghiệp tránh bị tấn công và đảm bảo vận hành ổn định.

#### Đối với cá nhân:

Người dùng cá nhân cũng dễ trở thành mục tiêu của các cuộc tấn công, từ lừa đảo trực tuyến (phishing), đánh cắp mật khẩu, đến xâm nhập tài khoản ngân hàng. Việc áp dụng các biện pháp bảo mật giúp bảo vệ thông tin cá nhân và tài sản số khỏi hacker.

### Những mối đe dọa phổ biến đối với bảo mật mạng:

* Tấn công mạng (Cyber Attacks): Các cuộc tấn công từ hacker nhằm đánh cắp, thay đổi hoặc phá hủy dữ liệu.
* Mã độc (Malware): Virus, ransomware, spyware có thể xâm nhập hệ thống để đánh cắp hoặc mã hóa dữ liệu.
* Tấn công lừa đảo (Phishing): Kẻ xấu giả mạo email hoặc trang web để lừa người dùng cung cấp thông tin nhạy cảm.
* Xâm nhập trái phép (Unauthorized Access): Hacker lợi dụng lỗ hổng bảo mật để truy cập trái phép vào hệ thống.

## Bảo mật mạng doanh nghiệp:

### Các mối đe dọa an ninh mạng đối với doanh nghiệp:

* Tấn công DDoS (Distributed Denial of Service): Tin tặc gửi lượng lớn yêu cầu đến hệ thống mạng của doanh nghiệp, làm quá tải máy chủ và khiến dịch vụ bị gián đoạn.
* Ransomware: Mã độc tống tiền mã hóa dữ liệu của doanh nghiệp và yêu cầu một khoản tiền chuộc để mở khóa.
* Phishing (Tấn công lừa đảo): Hacker gửi email hoặc tạo trang web giả mạo để đánh cắp thông tin đăng nhập, tài khoản ngân hàng hoặc dữ liệu quan trọng.
* Tấn công vào chuỗi cung ứng: Hacker lợi dụng lỗ hổng bảo mật của các đối tác, nhà cung cấp để xâm nhập vào hệ thống doanh nghiệp.
* Rò rỉ dữ liệu và đánh cắp tài sản trí tuệ: Tin tặc có thể xâm nhập vào hệ thống để đánh cắp dữ liệu khách hàng, thông tin nội bộ hoặc tài sản trí tuệ của doanh nghiệp.
* Gián điệp mạng: Đối thủ cạnh tranh hoặc tổ chức tội phạm có thể tấn công mạng doanh nghiệp để thu thập thông tin mật, chiến lược kinh doanh.

### Các biện pháp bảo mật mạng doanh nghiệp:

#### Xây dựng chính sách bảo mật:

Xác định các rủi ro và biện pháp phòng ngừa: Doanh nghiệp cần phân tích các rủi ro tiềm ẩn, đánh giá mức độ ảnh hưởng và triển khai các biện pháp giảm thiểu rủi ro.

Đào tạo nhân viên về an ninh mạng: Nhân viên là một trong những yếu tố dễ bị tấn công nhất, do đó cần tổ chức các khóa huấn luyện về nhận diện phishing, quản lý mật khẩu và bảo vệ dữ liệu.

Xây dựng quy trình ứng phó sự cố: Xây dựng kế hoạch xử lý sự cố bảo mật giúp doanh nghiệp phản ứng nhanh chóng và giảm thiểu thiệt hại khi bị tấn công.

#### Triển khai các giải pháp bảo mật kỹ thuật:

* Tường lửa (Firewall): Kiểm soát lưu lượng mạng, ngăn chặn truy cập trái phép từ bên ngoài.
* Hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS): Giám sát mạng để phát hiện và chặn các cuộc tấn công đang diễn ra.
* VPN (Virtual Private Network): Mã hóa dữ liệu khi truy cập mạng từ xa, bảo vệ thông tin của doanh nghiệp khi làm việc trực tuyến.
* Phần mềm diệt virus và bảo vệ chống malware: Ngăn chặn các mã độc xâm nhập vào hệ thống.

## Bảo mật mạng cá nhân:

### Các mối đe dọa an ninh mạng đối với cá nhân:

Cá nhân ngày càng trở thành mục tiêu của các cuộc tấn công mạng do sử dụng nhiều thiết bị kết nối internet và lưu trữ thông tin cá nhân trực tuyến. Một số mối đe dọa phổ biến bao gồm:

* Phishing (Tấn công lừa đảo): Kẻ tấn công giả mạo email, trang web hoặc tin nhắn để lừa người dùng cung cấp thông tin cá nhân như tài khoản ngân hàng, mật khẩu.
* Malware (Mã độc): Virus, ransomware, spyware có thể lây nhiễm vào máy tính hoặc điện thoại và đánh cắp dữ liệu.
* Đánh cắp danh tính: Hacker thu thập thông tin cá nhân để thực hiện các hành vi gian lận như mở tài khoản ngân hàng hoặc vay tiền.
* Mất dữ liệu cá nhân: Do lỗi người dùng, phần mềm độc hại hoặc các cuộc tấn công mạng, dữ liệu quan trọng có thể bị mất hoặc bị xóa.

### Các biện pháp bảo mật mạng cá nhân:

#### Bảo vệ thiết bị cá nhân:

Cài đặt phần mềm diệt virus và tường lửa: Ngăn chặn mã độc và bảo vệ thiết bị khỏi các cuộc tấn công từ bên ngoài.

* Cập nhật phần mềm hệ điều hành và ứng dụng: Các bản cập nhật thường đi kèm với các bản vá bảo mật giúp khắc phục lỗ hổng.
* Sử dụng mật khẩu mạnh cho thiết bị và tài khoản: Tạo mật khẩu dài, có ký tự đặc biệt và không sử dụng lại mật khẩu cũ.

#### Bảo vệ tài khoản trực tuyến:

* Sử dụng xác thực đa yếu tố (MFA/2FA): Kích hoạt bảo mật hai lớp để tăng cường an toàn cho tài khoản.
* Kiểm tra hoạt động tài khoản thường xuyên: Theo dõi lịch sử đăng nhập để phát hiện dấu hiệu bất thường.
* Tránh nhấp vào các liên kết và tải xuống tập tin không rõ nguồn gốc: Giúp ngăn chặn các cuộc tấn công phishing và malware.

#### Bảo vệ thông tin cá nhân:

Cẩn thận khi chia sẻ thông tin trên mạng xã hội: Hạn chế công khai các thông tin nhạy cảm như địa chỉ, số điện thoại, ngày sinh.

Sử dụng VPN khi truy cập mạng công cộng: VPN giúp mã hóa dữ liệu và bảo vệ quyền riêng tư khi sử dụng Wi-Fi công cộng.

Kiểm tra các cài đặt quyền riêng tư trên trang web và ứng dụng: Hạn chế ứng dụng thu thập dữ liệu cá nhân quá mức.

# Công cụ bảo mật và thực hành

## Giới thiệu về công cụ bảo mật mạng:

### Tầm quan trọng của công cụ bảo mật:

* Công cụ bảo mật giúp chuyên gia và người dùng đánh giá, kiểm tra và tăng cường bảo mật hệ thống.
* Hỗ trợ phát hiện và khắc phục các lỗ hổng bảo mật.
* Tự động hóa các tác vụ bảo mật, tiết kiệm thời gian và công sức.

### Phân loại công cụ bảo mật:

* Công cụ phân tích mạng: Wireshark, tcpdump, Nmap.
* Công cụ phát hiện xâm nhập: Snort, Suricata.
* Công cụ kiểm thử xâm nhập: Metasploit, Nessus.
* Công cụ phân tích lỗ hổng: OpenVAS, Nikto.
* Công cụ bẻ khóa mật khẩu: John the Ripper, Hashcat.

## Công cụ phân tích mạng Wireshark:

### Giới thiệu:



Hình 5.1. Wireshark

Wireshark là một công cụ phân tích giao thức mạng mã nguồn mở, được sử dụng rộng rãi để giám sát và kiểm tra các gói tin trên mạng.

Wireshark thường được sử dụng bởi quản trị viên mạng, chuyên gia bảo mật và nhà phát triển phần mềm để kiểm tra lưu lượng mạng và phát hiện các vấn đề bảo mật.

### Chức năng chính của Wireshark:

* Bắt gói tin mạng: Wireshark có thể thu thập dữ liệu trực tiếp từ card mạng và hiển thị thông tin chi tiết về từng gói tin.
* Lọc và phân tích gói tin: Hỗ trợ các bộ lọc mạnh mẽ giúp người dùng tìm kiếm thông tin cụ thể trong hàng ngàn gói tin.
* Hiển thị thông tin giao thức: Cung cấp chi tiết về các giao thức được sử dụng trong mạng, giúp người dùng hiểu cách dữ liệu được truyền tải.
* Phân tích lưu lượng mạng: Hỗ trợ phân tích các thông số hiệu suất mạng, giúp phát hiện lỗi và tối ưu hóa hệ thống.

### Ứng dụng của Wireshark:

* Phân tích lưu lượng mạng: Giúp quản trị viên xác định các vấn đề như tắc nghẽn mạng, mất gói tin và hiệu suất kém.
* Kiểm tra và gỡ lỗi các ứng dụng mạng: Nhà phát triển có thể kiểm tra cách ứng dụng của họ truyền dữ liệu trên mạng.
* Phân tích các cuộc tấn công mạng: Hỗ trợ chuyên gia bảo mật phát hiện các dấu hiệu tấn công như tấn công từ chối dịch vụ (DDoS), quét cổng, khai thác lỗ hổng.
* Giám sát mạng trong thời gian thực: Giúp theo dõi các hoạt động mạng và phát hiện các kết nối đáng ngờ.

## Snort] Hướng dẫn cài đặt snort - Trang tin tức từ Cloud365 - Nhân HòaCông cụ phát hiện xâm nhập Snort:

Hình 5.2. Snort

### Giới thiệu:

* Snort là hệ thống phát hiện xâm nhập (IDS) mã nguồn mở.
* Giám sát lưu lượng mạng và phát hiện các hoạt động đáng ngờ.
* Sử dụng các quy tắc để phát hiện các cuộc tấn công.

### Chức năng chính của Snort:

* Phân tích lưu lượng mạng: Theo dõi và kiểm tra các gói tin để tìm kiếm dấu hiệu tấn công.
* Phát hiện các cuộc tấn công dựa trên quy tắc: Sử dụng danh sách quy tắc để xác định các mối đe dọa như quét cổng, DDoS, khai thác lỗ hổng.
* Ghi nhật ký hoạt động: Lưu trữ thông tin về các sự kiện bảo mật để phân tích sau này.
* Cảnh báo khi phát hiện tấn công: Thông báo ngay lập tức nếu có hoạt động đáng ngờ hoặc vi phạm quy tắc an ninh.

## Metasploit for Beginners — A Guide to the Powerful Exploitation Framework | by Manish Shivanandhan | Jan, 2025 | MediumCông cụ kiểm thử xâm nhập Metasploit:

Hình 5.3. Metasploit

### Giới thiệu:

Metasploit là một framework kiểm thử xâm nhập (penetration testing framework) mã nguồn mở, giúp các chuyên gia bảo mật kiểm tra và đánh giá mức độ an toàn của hệ thống. Đây là một trong những công cụ phổ biến nhất trong lĩnh vực an ninh mạng.

### Chức năng:

* Kiểm thử xâm nhập: Thực hiện các bài kiểm tra bảo mật để xác định lỗ hổng của hệ thống.
* Khai thác lỗ hổng bảo mật: Tận dụng các lỗ hổng đã biết để xâm nhập hệ thống mục tiêu.
* Tạo và triển khai payload: Phát triển các mã khai thác để kiểm tra độ an toàn của hệ thống.
* Thu thập thông tin mục tiêu: Hỗ trợ các kỹ thuật thu thập thông tin để xác định các điểm yếu trong hệ thống bảo mật.

## Hướng dẫn cơ bản về kiểm thử bảo mật mạng:

### Các giai đoạn của kiểm thử bảo mật mạng:

* Thu thập thông tin (reconnaissance): Thu thập thông tin về mục tiêu.
* Quét lỗ hổng (scanning): Tìm kiếm các lỗ hổng bảo mật.
* Khai thác (exploitation): Khai thác các lỗ hổng để xâm nhập.
* Duy trì quyền truy cập (maintaining access): Duy trì quyền truy cập vào hệ thống.
* Báo cáo (reporting): Báo cáo các lỗ hổng và đề xuất các biện pháp khắc phục.

### Các kỹ thuật kiểm thử bảo mật mạng:

* Kiểm thử xâm nhập (penetration testing): Mô phỏng các cuộc tấn công mạng.
* Phân tích lỗ hổng (vulnerability assessment): Tìm kiếm và đánh giá các lỗ hổng.
* Kiểm tra bảo mật cấu hình (security configuration review): Kiểm tra cấu hình hệ thống.
* Kiểm tra an ninh không dây (wireless security testing): Kiểm tra an ninh mạng wifi.

## Thực hành kiểm thử bảo mật mạng cơ bản:

### Sử dụng Nmap để quét cổng:

Xác định các cổng đang mở trên hệ thống mục tiêu.

Xác định các dịch vụ đang chạy trên các cổng.

### Sử dụng Wireshark để phân tích lưu lượng mạng:

Bắt và phân tích lưu lượng mạng giữa hai máy tính.

Xác định các giao thức đang được sử dụng.

Phân tích nội dung của các gói tin.

### Sử dụng Metasploit để khai thác lỗ hổng:

Tìm kiếm và khai thác các lỗ hổng bảo mật trên hệ thống mục tiêu.

Thực hiện các lệnh từ xa trên hệ thống mục tiêu.

### Sử dụng Snort để phát hiện xâm nhập:

Cài đặt và cấu hình Snort để giám sát lưu lượng mạng.

Tạo các quy tắc để phát hiện các cuộc tấn công.

Xem nhật ký hoạt động của Snort.

# Xu hướng bảo mật mạng trong tương lai

## Sự khác biệt giữa AI, Machine Learning, Deep Learning ?Bảo mật AI và Machine Learning:

### Sự phát triển của AI và Machine Learning trong bảo mật:

AI và Machine Learning đang được sử dụng ngày càng rộng rãi trong bảo mật mạng để tự động hóa các tác vụ, phát hiện các mối đe dọa và cải thiện khả năng phản ứng sự cố.

Các hệ thống AI có thể phân tích lượng lớn dữ liệu để phát hiện các mẫu tấn công và hành vi bất thường.

Machine Learning có thể được sử dụng để xây dựng các mô hình dự đoán rủi ro và ngăn chặn các cuộc tấn công.

Hình 6.1. AI & Machine Learning

### Các ứng dụng của AI và Machine Learning trong bảo mật:

* Phát hiện xâm nhập: AI có thể phát hiện các hành vi bất thường trong lưu lượng mạng.
* Phân tích phần mềm độc hại: Machine Learning có thể phân tích các mẫu mã độc để xác định các mối đe dọa mới.
* Quản lý rủi ro: AI có thể đánh giá rủi ro an ninh mạng dựa trên dữ liệu lịch sử và các yếu tố khác.
* Tự động hóa phản ứng sự cố.

## Bảo mật mạng trong IoT:

### Sự gia tăng của thiết bị IoT:



Hình 6.2. IoT

Số lượng thiết bị IoT đang tăng lên nhanh chóng, tạo ra một bề mặt tấn công lớn hơn.

Thiết bị IoT thường có lỗ hổng bảo mật và có thể bị tấn công để thực hiện các cuộc tấn công DDoS hoặc đánh cắp dữ liệu.

### Các biện pháp bảo mật IoT:

* Thiết kế bảo mật ngay từ đầu: Xây dựng các tính năng bảo mật vào thiết bị IoT ngay từ giai đoạn thiết kế.
* Cập nhật phần mềm thường xuyên: Cung cấp các bản cập nhật phần mềm để vá các lỗ hổng.
* Sử dụng mật khẩu mạnh và duy nhất: Thay đổi mật khẩu mặc định và sử dụng mật khẩu mạnh.
* Phân đoạn mạng: cô lập các thiết bị IoT trên một mạng riêng.

## Zero Trust Security Model:

### Mô hình bảo mật Zero Trust:



Hình 6.3. Zero Trust Security Model

Mô hình Zero Trust giả định rằng không có người dùng hoặc thiết bị nào được tin cậy, ngay cả khi họ ở bên trong mạng.

Mọi yêu cầu truy cập đều phải được xác minh, bất kể nguồn gốc của chúng.

Nguyên tắc "không bao giờ tin tưởng, luôn xác minh".

### Các nguyên tắc của Zero Trust:

* Xác minh rõ ràng: Xác minh danh tính của người dùng và thiết bị.
* Đặc quyền tối thiểu: Chỉ cấp quyền truy cập cần thiết.
* Giả định vi phạm: Giả định rằng hệ thống đã bị xâm phạm và liên tục giám sát hoạt động.

### Lợi ích của Zero Trust:

* Giảm thiểu rủi ro tấn công nội bộ.
* Tăng cường bảo mật cho các ứng dụng và dữ liệu trên đám mây.
* Cho phép truy cập an toàn từ mọi nơi.

### Xu hướng phát triển:

* Zero Trust và AI.
* Zero Trust và SASE (Secure Access Service Edge).

**KẾT LUẬN**

Đề tài "Tìm hiểu về bảo mật mạng máy tính" đã cung cấp một cái nhìn toàn diện về lĩnh vực bảo mật mạng, một yếu tố không thể thiếu trong thời đại công nghệ số. Bằng việc đi sâu vào các khía cạnh từ cơ bản đến nâng cao, đề tài đã giúp người đọc hiểu rõ về các mối đe dọa an ninh mạng phổ biến, các phương pháp phòng chống hiệu quả, cũng như những xu hướng bảo mật tiên tiến đang định hình tương lai. Ưu điểm nổi bật của đề tài là tính toàn diện, bao quát nhiều khía cạnh quan trọng của bảo mật mạng, từ việc bảo vệ dữ liệu cá nhân đến bảo vệ hệ thống mạng doanh nghiệp. Bên cạnh đó, tính cập nhật của đề tài cũng là một điểm mạnh, khi đề cập đến các xu hướng bảo mật mới nhất như bảo mật AI, IoT và Zero Trust, giúp người đọc nắm bắt được những thay đổi và phát triển của lĩnh vực này. Tính thực tiễn của đề tài được thể hiện qua việc cung cấp các hướng dẫn và ví dụ cụ thể về kiểm thử bảo mật và sử dụng các công cụ bảo mật, giúp người đọc có thể áp dụng kiến thức vào thực tế. Tuy nhiên, đề tài cũng tồn tại một số nhược điểm. Do phạm vi quá rộng lớn, một số phần có thể chưa được phân tích sâu sắc, đòi hỏi người đọc phải tự tìm hiểu thêm để có cái nhìn chi tiết hơn. Bên cạnh đó, tính kỹ thuật của một số phần cũng có thể gây khó khăn cho những người đọc không có nền tảng kỹ thuật vững chắc. Một nhược điểm khác là sự thay đổi nhanh chóng của lĩnh vực bảo mật mạng, khiến một số thông tin có thể nhanh chóng trở nên lỗi thời. Để khắc phục những nhược điểm này, hướng phát triển của đề tài có thể tập trung vào việc nghiên cứu chuyên sâu vào một lĩnh vực cụ thể của bảo mật mạng, chẳng hạn như bảo mật đám mây, bảo mật IoT hoặc bảo mật AI. Việc phát triển các công cụ bảo mật mới để đối phó với các mối đe dọa tiên tiến cũng là một hướng đi tiềm năng. Xây dựng một hệ thống bảo mật mạng hoàn chỉnh cho một doanh nghiệp hoặc tổ chức cụ thể cũng là một ứng dụng thực tiễn của đề tài. Ngoài ra, việc tiếp tục nghiên cứu và cập nhật các xu hướng bảo mật mới nhất là rất quan trọng để đảm bảo an toàn cho hệ thống và dữ liệu trong thời đại số hóa. Nâng cao nhận thức của cộng đồng về an ninh mạng thông qua các hoạt động tuyên truyền, giáo dục cũng là một hướng phát triển cần được chú trọng. Tóm lại, đề tài "Tìm hiểu về bảo mật mạng máy tính" là một đề tài có giá trị và tính ứng dụng cao. Việc tiếp tục nghiên cứu và phát triển trong lĩnh vực này là rất cần thiết để bảo vệ hệ thống và dữ liệu khỏi những rủi ro ngày càng gia tăng trong thế giới kỹ thuật số.

**DANH MỤC TÀI LIỆU THAM KHẢO**

[1] J. F. Kurose & K. W. Ross. *Computer Networking: A Top-down Approach*. 7th

edition, Hoboken, New Jersey: Pearson, 2018

[2] Andrew S. Tanenbaum and David J. Wetherall. *Computer Networks*. 5th Edition,

Pearson Education, Inc., publishing as Prentice Hall, 2011