# 1. CCNA

Cơ bản về mạng: hiểu những điều cơ bản về công nghệ mạng, chẳng hạn như cách các thiết bị giao tiếp và cách dữ liệu được truyền đi

Công nghệ chuyển mạch (switch) LAN: hiểu cách các bộ chuyển mạch hoạt động và cách cấu hình chúng để có hiệu suất tối ưu

Công nghệ định tuyến (router) IPv4 và IPv6: tìm hiểu cách bộ định tuyến xử lý các gói tin và định tuyến dữ liệu giữa các mạng

Công nghệ WAN: hiểu về Mạng diện rộng (WAN) và cách chúng được sử dụng để kết nối các mạng phân tán về mặt địa lý

Dịch vụ cơ sở hạ tầng: tìm hiểu về DHCP, DNS và các dịch vụ mạng thiết yếu khác

Bảo mật cơ sở hạ tầng: hiểu cách bảo mật các thiết bị mạng và triển khai các biện pháp bảo mật cơ bản

Quản lý cơ sở hạ tầng: tìm hiểu về SNMP, Syslog và các công cụ khác để giám sát và quản lý mạng

# 2. Giao thức mạng

## 2.1 SSL/TLS: Secure Socket Layer/Transport Layer Security

Các giao thức mã hóa được thiết kế để cung cấp tính an toàn và toàn vẹn cho dữ liệu khi truyền qua mạng. Chủ yếu được dùng để đảm bảo an toàn cho những thông tin bí mật (như số thẻ, tt đăng nhập) khi truyền giữa client và server.

SSL đã được thay thế hoàn toàn bởi TLS.

Các bước thiết lập kết nối SSL/TLS:

- **Handshake**

2 bên đồng ý sử dụng version SSL/TLS + thuật toán mã hóa nào

- **Trao đổi khóa**

Public và private key được dùng để tạo session key, vốn được dùng để mã hóa và giải mã dữ liệu được truyền đưa. Session key sẽ được sử dụng trong một khoảng thời gian nhất định và chỉ có thể dùng cho phiên giao dịch này

- **Xác minh chứng chỉ**

Server cung cấp chứng chỉ điện tử, chứa thông tin về khóa công khai + thông tin server. Client kiểm tra chứng chỉ đã được cấp bởi CA đáng tin chưa + đã hết hạn chưa

- **Giao tiếp an toàn**

Xong 3 bước trên, client và server có thể trao đổi dữ liệu 1 cách an toàn bằng khóa đã đc chia sẻ.

Ưu điểm:

- **Đường truyền an toàn**

SSL/TLS cung cấp đường hầm được mã hóa an toàn để truyền dữ liệu giữa máy khách và máy chủ, bảo vệ thông tin nhạy cảm khỏi bị nghe lén, chặn và giả mạo.

- **Xác thực**

SSL/TLS sử dụng chứng chỉ số để xác thực máy chủ và (đôi khi) xác thực máy khách. Điều này giúp đảm bảo rằng các bên liên quan trong giao tiếp là những người mà họ tuyên bố.

- **Tính toàn vẹn**

SSL/TLS bao gồm các cơ chế để xác nhận dữ liệu nhận được không bị giả mạo trong quá trình truyền, duy trì tính toàn vẹn của thông tin được gửi.

Các điểm khác biệt:

**Bảo mật:** TLS cung cấp bảo mật tốt hơn do sử dụng các thuật toán mã hóa mạnh hơn, bộ mã hóa được cập nhật và cơ chế trao đổi khóa được cải thiện.

**Hiệu suất**: TLS giảm số lượng vòng lặp cần thiết cho quy trình bắt tay, dẫn đến thời gian kết nối nhanh hơn.

**Khả năng tương thích ngược**: TLS được thiết kế để tương thích ngược với SSL 3.0, cho phép các hệ thống sử dụng TLS giao tiếp với những hệ thống vẫn đang sử dụng SSL. Tuy nhiên, nên tắt hỗ trợ SSL 3.0 để tránh các cuộc tấn công tiềm ẩn.

## 2.2 SSH: Secure Shell

SSH, hay Secure Shell, là một giao thức mạng mã hóa cung cấp phương pháp bảo mật và được mã hóa để quản lý các thiết bị mạng và truy cập máy chủ từ xa.

Các tính năng chính

**Mã hóa**: SSH sử dụng nhiều thuật toán mã hóa khác nhau để đảm bảo tính bảo mật và toàn vẹn của dữ liệu được truyền giữa máy khách và máy chủ.

**Xác thực**: SSH hỗ trợ nhiều phương pháp xác thực, bao gồm xác thực dựa trên mật khẩu, khóa công khai và xác thực dựa trên máy chủ, cung cấp tính linh hoạt trong việc xác minh danh tính của các bên giao tiếp một cách an toàn.

**Chuyển tiếp cổng**: SSH cho phép chuyển tiếp các cổng mạng, cho phép người dùng tạo đường hầm cho các giao thức khác một cách an toàn, chẳng hạn như HTTP hoặc FTP, thông qua kết nối được mã hóa.

**Truyền tệp an toàn**: SSH cung cấp hai giao thức truyền tệp, SCP (Giao thức sao chép an toàn) và SFTP (Giao thức truyền tệp SSH), để truyền tệp an toàn giữa máy khách cục bộ và máy chủ từ xa.

Các trường hợp sử dụng phổ biến

**Quản trị hệ thống từ xa**: Quản trị viên có thể truy cập và quản lý các hệ thống từ xa một cách an toàn, chẳng hạn như máy chủ và thiết bị mạng, bằng cách sử dụng SSH để thực thi lệnh và định cấu hình cài đặt.

**Chuyển tệp an toàn**: Các nhà phát triển và quản trị viên có thể chuyển tệp an toàn giữa các hệ thống bằng SCP hoặc SFTP, bảo vệ dữ liệu nhạy cảm khỏi bị nghe lén.

**Truy cập ứng dụng từ xa**: Người dùng có thể truy cập ứng dụng từ xa một cách an toàn bằng cách tạo đường hầm SSH, cho phép họ kết nối với các dịch vụ mà nếu không sẽ không thể truy cập được do tường lửa hoặc các hạn chế mạng khác.

Mẹo sử dụng SSH an toàn

**Vô hiệu hóa root**: Để giảm nguy cơ truy cập trái phép, bạn nên vô hiệu hóa root và sử dụng tài khoản người dùng chuẩn có quyền sudo cho các tác vụ quản trị.

**Sử dụng xác thực dựa trên khóa**: Để tăng cường bảo mật hơn nữa, hãy không cho phép xác thực dựa trên mật khẩu và thay vào đó sử dụng xác thực khóa công khai, khiến kẻ tấn công khó truy cập hơn thông qua các cuộc tấn công brute force.

**Cập nhật phần mềm SSH**: Thường xuyên cập nhật phần mềm máy khách và máy chủ SSH của bạn để đảm bảo bạn có các bản vá và tính năng bảo mật mới nhất.

## 2.3 TCP: Transmission Control Protocol

TCP là một giao thức đáng tin cậy, hướng kết nối, đảm bảo dữ liệu được truyền chính xác giữa các ứng dụng qua mạng.

Các bước:

**Thiết lập kết nối:** sử dụng bắt tay 3 bước, bên dưới đã ghi

**Truyền dữ liệu:** phân mảnh dữ liệu thành các gói tin nhỏ hơn để truyền đi trên mạng. Mỗi gói tin chứa một phần của dữ liệu gốc và được đánh số thứ tự để đảm bảo thứ tự chính xác khi đến được máy tính đích.

**Kiểm soát luồng dữ liệu:**

- TCP sử dụng cơ chế cửa sổ trượt để điều chỉnh số lượng gói tin được gửi và nhận trong cùng một thời điểm. Cơ chế này giúp đảm bảo rằng mạng không bị quá tải và dữ liệu không bị mất.
- Người gửi và người nhận sử dụng tác vụ ACK (acknowledgment) và cửa sổ cùng có kích thước để điều chỉnh quy mô của dòng thông tin dữ liệu.

**Đóng kết nối:**

- Khi quá trình truyền dữ liệu hoàn tất, người gửi gửi một gói tin FIN (Finish) để bắt đầu quá trình đóng kết nối.
- Người nhận nhận được gói tin FIN và gửi một gói tin ACK để xác nhận.
- Sau khi nhận được xác nhận, người gửi gửi một gói tin ACK cuối cùng để hoàn tất quá trình đóng kết nối.

## 2.4 IP: Internet Protocol

Đề cập đến cách dữ liệu được truyền qua các mạng.

**Địa chỉ IP**: Địa chỉ IP là mã định danh duy nhất được gán cho mỗi thiết bị được kết nối với mạng, như máy tính hoặc điện thoại thông minh. Nó bao gồm một chuỗi các số được phân tách bằng dấu chấm (ví dụ: 192.168.1.1). Địa chỉ IP có thể là IPv4 (32 bit) hoặc định dạng IPv6 (128 bit) mới hơn, cung cấp nhiều địa chỉ khả dụng hơn. Chúng cho phép các thiết bị gửi và nhận các gói dữ liệu đến và đi từ các thiết bị khác trên internet.

**Định tuyến IP**: Định tuyến IP là quá trình hướng các gói dữ liệu từ địa chỉ IP này sang địa chỉ IP khác thông qua các bộ định tuyến. Các bộ định tuyến này giúp tìm ra đường dẫn hiệu quả nhất cho dữ liệu khi nó di chuyển qua mạng, đảm bảo rằng giao tiếp nhanh chóng và đáng tin cậy.

**Giao thức IP:**

- TCP: Được thiết kế để đảm bảo truyền các gói dữ liệu theo thứ tự, không có lỗi, TCP được sử dụng cho các ứng dụng mà độ tin cậy quan trọng hơn tốc độ, chẳng hạn như truyền tệp, email và duyệt web.
- UDP: Một giao thức nhanh hơn, không kết nối, không đảm bảo thứ tự hoặc tính toàn vẹn của các gói dữ liệu, làm cho nó phù hợp với các ứng dụng thời gian thực như phát trực tuyến video và chơi game trực tuyến.

**Rủi ro bảo mật IP:**

- Giả mạo IP
- Tấn công DDoS
- Tấn công Man-in-the-Middle

Bảo mật:

- Tường lửa
- VPN
- Cập nhật thường xuyên
- IDPS

## 2.5 UDP: User Datagram Protocol

## 2.6 FTP: File Transfer Protocol

Chuyển file giữa 2 máy tính qua mạng TCP.

FTP hoạt động theo mô hình máy khách-máy chủ, trong đó một máy tính đóng vai trò là máy khách (người gửi hoặc người yêu cầu) và máy tính còn lại đóng vai

trò là máy chủ (người nhận hoặc nhà cung cấp). Máy khách khởi tạo kết nối với máy chủ, thường bằng cách cung cấp tên người dùng và mật khẩu để xác thực, sau đó yêu cầu truyền tệp.

FTP sử dụng hai kênh riêng biệt để thực hiện các hoạt động của mình:

**Kênh điều khiển**: Kênh này được sử dụng để thiết lập kết nối giữa máy khách và máy chủ và gửi lệnh, chẳng hạn như chỉ định tệp sẽ được truyền, chế độ truyền và cấu trúc thư mục.

**Kênh dữ liệu**: Kênh này được sử dụng để truyền dữ liệu tệp thực tế giữa máy khách và máy chủ.

2 chế độ truyền tệp:

**Chế độ ASCII**: Chế độ này được sử dụng để truyền tệp văn bản. Chế độ này chuyển đổi các kết thúc dòng của tệp đang được truyền để khớp với định dạng được sử dụng trên hệ thống đích.

**Chế độ nhị phân**: Chế độ này được sử dụng để truyền tệp nhị phân, chẳng hạn như hình ảnh, tệp âm thanh và tệp thực thi. Không có chuyển đổi dữ liệu nào được thực hiện trong quá trình truyền.

Bảo mật:

- Tên người dùng và mật khẩu được truyền dưới dạng văn bản thuần túy, cho phép bất kỳ ai có thể chặn dữ liệu xem chúng.
- Dữ liệu được truyền giữa máy khách và máy chủ không được mã hóa theo mặc định, khiến dữ liệu dễ bị nghe lén.
- FTP không cung cấp cách xác thực danh tính của máy chủ, khiến máy chủ dễ bị tấn công trung gian.

Để giảm thiểu những rủi ro bảo mật này, một số giải pháp thay thế an toàn cho giao thức FTP đã được phát triển, chẳng hạn như FTPS (FTP Secure) và SFTP (SSH File Transfer Protocol), giúp mã hóa dữ liệu truyền và cung cấp các tính năng bảo mật bổ sung.

## 3. Handshake

Quá trình thiết lập kết nối giữa 2 thiết bị, 1 phần của giao thức an toàn.

### 3.1 Bắt tay 3 bước (TCP)

- **SYN**: bên A khởi đầu = cách gửi gói SYN (synchronize) cho bên B để thiết lập kết nối
- **SYN-ACK**: bên B phản hồi = cách gửi lại SYN-ACK cho A
- **ACK**: bên A gửi gói ACK cho bên B

Sau khi hoàn thành 3 bước, kết nối đã đc thiết lập, dữ liệu có thể được truyền 1 cách an toàn giữa 2 bên.

### 3.2 TLS handshake

Dùng để thiết lập kết nối an toàn tới các giao thức SSL/TLS

- **Client Hello**: Client gửi tin nhắn "Client Hello", bao gồm các bộ mã hóa được hỗ trợ, phiên bản SSL/TLS và một giá trị ngẫu nhiên.
- **Server Hello**: Server trả lời bằng tin nhắn "Server Hello", chọn phiên bản SSL/TLS cao nhất và bộ mã hóa tương thích, cùng với giá trị ngẫu nhiên của nó.
- **Xác thực**: Server chia sẻ chứng chỉ số của mình, cho phép client xác minh danh tính của mình bằng cách sử dụng một cơ quan cấp chứng chỉ (CA) đáng tin cậy.
- **Trao đổi khóa**: Cả hai bên trao đổi thông tin cần thiết (như khóa công khai) để tạo khóa bí mật chung sẽ được sử dụng để mã hóa và giải mã.

Sau khi hoàn thành 4 bước, kết nối đã đc thiết lập, dữ liệu có thể được truyền 1 cách an toàn giữa 2 bên.

## 4. Hệ điều hành

### 4.1 Windows

Windows được biết đến với giao diện người dùng đồ họa (GUI) và hỗ trợ nhiều ứng dụng khác nhau, khiến nó trở thành lựa chọn linh hoạt cho cả mục đích sử dụng cá nhân và chuyên nghiệp.

Các tính năng chính

**Dễ sử dụng**: Windows được thiết kế với giao diện thân thiện với người dùng, giúp người dùng dễ dàng điều hướng, quản lý tệp và truy cập ứng dụng.

**Khả năng tương thích**: Windows tương thích với nhiều loại phần cứng và phần mềm, bao gồm hầu hết các thiết bị ngoại vi như máy in, webcam, v.v.

**Cập nhật thường xuyên**: Microsoft cung cấp các bản cập nhật thường xuyên cho Windows, giúp duy trì bảo mật, sửa lỗi và nâng cao các tính năng.

**Cộng đồng người dùng lớn**

**Hỗ trợ ứng dụng đa dạng**: Windows hỗ trợ rất nhiều ứng dụng, bao gồm các công cụ năng suất văn phòng, trò chơi, phần mềm đa phương tiện, v.v.

Tính năng bảo mật

**Windows Defender**: Phần mềm diệt vi-rút tích hợp cung cấp khả năng bảo vệ theo thời gian thực chống lại phần mềm độc hại, phần mềm tống tiền và các mối đe dọa khác.

**Tường lửa Windows:** Tính năng này giúp bảo vệ thiết bị của bạn khỏi truy cập hoặc xâm nhập trái phép bằng cách chặn các kết nối mạng có khả năng gây hại.

**User Account Control (UAC)**: UAC giúp ngăn chặn các thay đổi trái phép đối với cài đặt hệ thống bằng cách nhắc người dùng cấp quyền quản trị khi thực hiện các sửa đổi hệ thống.

**Windows Update**: Các bản cập nhật thường xuyên đảm bảo hệ thống của bạn được cập nhật các bản vá bảo mật, bản sửa lỗi và cải tiến tính năng mới nhất.

**BitLocker**: Một tính năng mã hóa đĩa có trong một số phiên bản Windows, BitLocker giúp bảo mật dữ liệu của bạn bằng cách cung cấp mã hóa cho ổ cứng hoặc thiết bị lưu trữ ngoài của bạn.

## 4.2 Linux

Linux là một hệ điều hành mã nguồn mở được ưa chuộng rộng rãi do tính linh hoạt, ổn định và các tính năng bảo mật của nó. Là một hệ điều hành dựa trên Unix, Linux có giao diện dòng lệnh, cho phép người dùng thực hiện nhiều tác vụ khác nhau thông qua các lệnh văn bản.

Các tính năng chính

**Mã nguồn mở**: Bất kỳ ai cũng có thể xem, sửa đổi và phân phối mã nguồn Linux, thúc đẩy sự hợp tác và cải tiến liên tục trong cộng đồng HĐH.

**Thiết kế mô-đun**: Linux có thể được tùy chỉnh cho nhiều môi trường điện toán khác nhau, chẳng hạn như máy tính để bàn, máy chủ và hệ thống nhúng.

**Tính ổn định và hiệu suất**: Linux nổi tiếng với khả năng xử lý tải nặng mà không bị sập, khiến nó trở thành lựa chọn lý tưởng cho máy chủ.

**Bảo mật mạnh mẽ**: Linux có các cơ chế bảo mật mạnh mẽ, chẳng hạn như quyền tệp, tường lửa tích hợp và hệ thống đặc quyền người dùng mở rộng.

**Cộng đồng lớn**

Các biện pháp bảo mật tốt nhất cho Linux

**Luôn cập nhật hệ thống của bạn**: Cập nhật thường xuyên hạt nhân, gói hệ điều hành và phần mềm đã cài đặt để đảm bảo bạn có các bản vá bảo mật mới nhất.

**Bật tường lửa**: Cấu hình và bật tường lửa, chẳng hạn như iptables, để kiểm soát lưu lượng mạng đến và đi.

**Sử dụng mật khẩu mạnh và tài khoản người dùng**: Tạo các tài khoản riêng biệt với mật khẩu mạnh cho những người dùng khác nhau và chỉ cấp cho họ các đặc quyền cần thiết.

**Vô hiệu hóa các dịch vụ không sử dụng**: Các dịch vụ không cần thiết có thể là rủi ro bảo mật tiềm ẩn

**Triển khai chính sách Linux tăng cường bảo mật (SELinux)**: SELinux cung cấp hệ thống kiểm soát truy cập bắt buộc (MAC) hạn chế quyền truy cập của người dùng và quy trình vào tài nguyên hệ thống.

# 5. Router + Switch

## 5.1 Router

Bộ định tuyến là một thiết bị mạng chịu trách nhiệm chuyển tiếp các gói dữ liệu giữa các mạng máy tính. Gói dl có thể là email hoặc trang web. Bộ định tuyến thường đuoqfng đặt ở nơi 2 or nhiều mạng giao nhau.

Chức năng của bộ định tuyến

**Quyết định tuyến**: Bộ định tuyến phân tích các gói dữ liệu đến và đưa ra quyết định về đường dẫn nào sẽ chuyển tiếp dữ liệu dựa trên địa chỉ IP đích và điều kiện mạng.

**Kết nối các mạng**: Bộ định tuyến rất cần thiết trong việc kết nối các mạng khác nhau với nhau. Chúng cho phép giao tiếp giữa mạng gia đình của bạn và internet rộng hơn, cũng như giữa các mạng khác nhau trong một tổ chức.

**Quản lý lưu lượng**: Bộ định tuyến quản lý luồng dữ liệu để đảm bảo hiệu suất tối ưu và tránh tắc nghẽn mạng. Họ có thể ưu tiên một số loại dữ liệu nhất định, chẳng hạn như phát trực tuyến video, để đảm bảo trải nghiệm người dùng tốt hơn.

Các loại bộ định tuyến

**Bộ định tuyến có dây**: Sử dụng cáp Ethernet để kết nối các thiết bị với mạng. Chúng thường đi kèm với nhiều cổng ethernet

**Bộ định tuyến không dây**: sử dụng Wi-Fi để truyền dữ liệu giữa các thiết bị và là loại bộ định tuyến phổ biến nhất

**Bộ định tuyến lõi**: Hoạt động trong xương sống của internet, chỉ đạo các gói dữ liệu giữa các mạng chính (như ISP). Các bộ định tuyến này là các thiết bị hiệu suất cao có khả năng xử lý lượng lớn lưu lượng dữ liệu.

## 5.2 Switch

Switch là một thiết bị mạng kết nối các thiết bị với nhau trên mạng máy tính. Bộ chuyển mạch đóng vai trò thiết yếu trong việc quản lý lưu lượng truy cập và đảm bảo rằng dữ liệu đến đích dự định một cách hiệu quả.

Các chức năng chính:

**Quản lý traffic thông minh**: Thiết bị chuyển mạch giám sát các gói dữ liệu khi chúng đi qua mạng, chỉ chuyển tiếp chúng đến các thiết bị cần nhận dữ liệu. Điều này tối ưu hóa hiệu suất mạng và giảm tắc nghẽn.

**Chuyển mạch lớp 2:** Thiết bị chuyển mạch hoạt động ở lớp liên kết dữ liệu (Lớp 2) của mô hình OSI (Kết nối hệ thống mở). Họ sử dụng địa chỉ MAC để xác định thiết bị và xác định đường dẫn thích hợp cho các gói dữ liệu.

**Tên miền phát sóng**: Một switch tạo ra các miền xung đột riêng biệt, chia một miền phát sóng thành nhiều miền nhỏ hơn, giúp giảm thiểu tác động của lưu lượng phát sóng đến hiệu suất mạng.

**Bảng địa chỉ MAC**: Thiết bị chuyển mạch duy trì bảng địa chỉ MAC, lưu trữ ánh xạ địa chỉ MAC đến các giao diện vật lý thích hợp, giúp switch xác định đích đến của các gói dữ liệu một cách hiệu quả.

Các loại Switch:

**Switch không được quản lý**: Các thiết bị chuyển mạch này là các thiết bị plug-and-play đơn giản không yêu cầu cấu hình. Chúng phù hợp nhất cho các mạng nhỏ hoặc những nơi không cần các tính năng nâng cao và cài đặt tùy chỉnh.

**Switch được quản lý**: Các thiết bị chuyển mạch này cung cấp mức độ kiểm soát và tùy chỉnh cao hơn, cho phép quản trị viên mạng giám sát, quản lý và bảo mật lưu lượng mạng. Thiết bị chuyển mạch được quản lý thường được sử dụng trong các mạng hoặc môi trường cấp doanh nghiệp yêu cầu các tính năng bảo mật nâng cao và tối ưu hóa lưu lượng.

## 6. Các tấn công mạng

7. Các tầng OSI
3 tầng thấp nhất: hardware
Tầng giữa transport; trái tim của tầng OSI
3 tầng cao nhất: software
Physical
Data link: kiểm tra đg truyền, gói thành các khung dl
Network: xử lý dl
Transport: vận chuyển dl qua các mạng, vd router, giao thức tcp và udp
Session: tạo và duy trì kết nối giữa các hệ thống
Presentation: dịch tt dạng này sang dạng khác, vd ascii -> binary
Application: thứ ng dùng tg tác, vd gg chrome, microsoft egde
8. Các tầng TCP/IP, các giao thức mỗi tầng
Application: HTTP, FTP
Transport: TCP, UDP
Internet: IP

Network Interface: Ethernet

9. Giới thiệu bản thân, ủa ủa :v

Trước tiên, em xin cảm ơn cty vì đã cho em 1 cơ hội được pv hôm nay. Tên em là Bùi Yến Linh, sv năm 4 chuyên ngành attt ở hvktmm. Em dự kiến sẽ tốt nghiệp tháng 12 năm nay với bằng khá…

10. Có kn vs các ứng dụng bảo mật chưa? (set up SIEM, IDS, IPS,...): t bảo chưa 🙂

11. Kiểm thử ư d web tn? Ns qua về 1 lỗ hổng (t chọn SQLi)

12. Định hướng tg lai: t ns quản trị hệ thống