TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

AN TOÀN THÔNG TIN- INFORMATION SECURITY

CHƯƠNG 2

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

BIỆN PHÁP PHÁT HIỆN VÀ PHÒNG CHỐNG TẤN CÔNG

Giảng viên: TS. Trần Thế Vinh

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

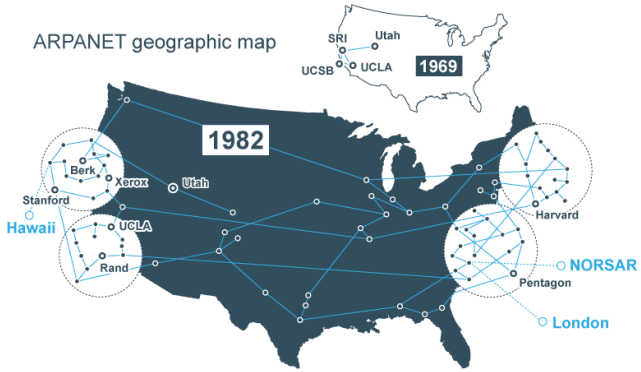
LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

Nguồn gốc lịch sử:

- Nguồn gốc của **thuật ngữ giao thức truyền thông** có thể bắt nguồn từ nữa sau của những năm 1960. Các bản ghi đầu tiên mô tả các giao thức truyền thông có liên quan đến ARPANET (U.S Advanced Research Projects Agency Network – Mạng lưới cơ quan dự án nghiên cứu cao cấp của Hoa Kỳ), mạng máy tính công cộng đầu tiên ra mắt vào năm 1969 và cuối cùng ngừng hoạt động vào năm 1989. Giao thức 1822 được triển khai trên ARPANET như một điểm khởi đầu, xác định đường truyền tin nhắn đến một IMP (Interface Message Processor – Bộ xử lý tin nhắn)

- Năm 1970, Giao thức điều khiển mạng (Network Control Protocol – NCP) được triển khai trên ARPANET. NCP là một trong những ví dụ sớm nhất về phân lớp giao thức vì giao diện NCP cho phép các giải pháp phần mềm kết nối với nhau trên các mạng ARPANET, bằng cách tận dụng các giao thức truyền thông cấp cao hơn cho các mục đích này

- Chương trình kiểm soát truyền tải (Transmission Control Program – TCP) cũng được xây dựng vào năm 1970 (bởi các nhà nghiên cứu Robert E. Kahn và Vint Cerf)



Sự phát triển của ARPANET, 1969-1982

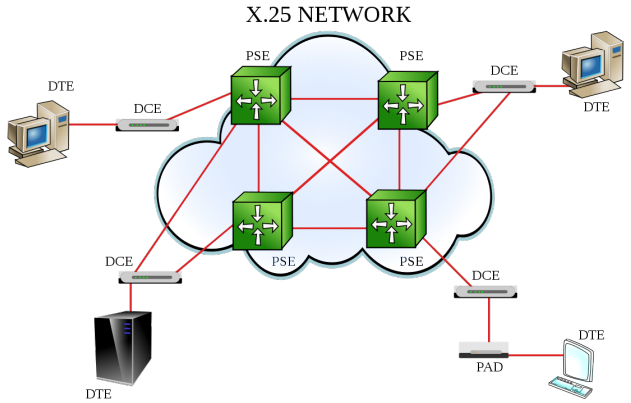
Robert E. Kahn

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

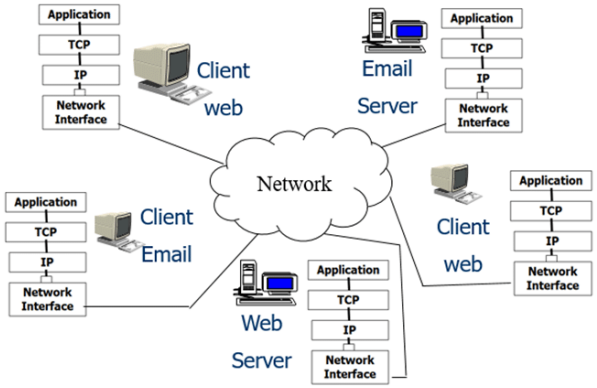
LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

Nguồn gốc lịch sử (tiếp):

- Sự phát triển của **tiêu chuẩn X.25** dựa trên các mạch ảo của ITU-T vào năm 1976 là một cộc mốc quan trọng khác trong lịch sử của lĩnh vực giao thức truyền thông. Trong những năm qua, các nhà sản xuất phần cứng máy tính lớn đã phát triển các giao thức độc quyền của riêng họ. Chẳng hạn như hệ thống mạng Xerox (Xerox Network Systems) và Hệ thống kiến trúc mạng (Systems Network Architecture – SNA) của IBM.



- Năm 1982, Bộ quốc phòng Hoa Kỳ tuyên bố **TCP/IP** là giao thức truyền thông tiêu chuẩn cho tất cả các mạng máy tính quân sự. TCP/IP đã được cài đặt trên SATNET(một mạng vệ tinh ban đầu đã hình thành nên một phân đoạn đầu tiên của Internet) vào năm 1982 và trên ARPANET vào năm 1983. Trong suốt những năm 1980, TCP/IP đã dần được phát triển như một bộ giao thức module phức tạp và đã trở thành một thành phần cốt lõi của Internet.



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

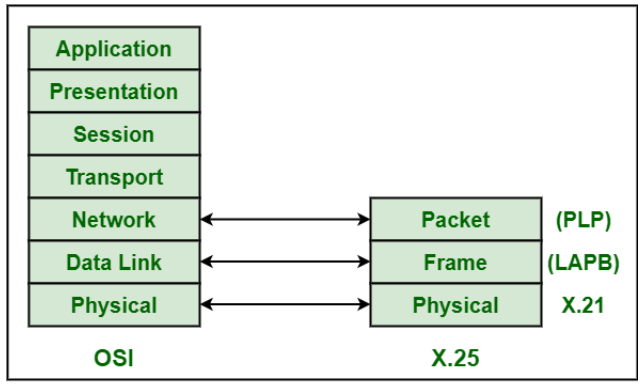
LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

Cuộc chiến của giao thức truyền thông:

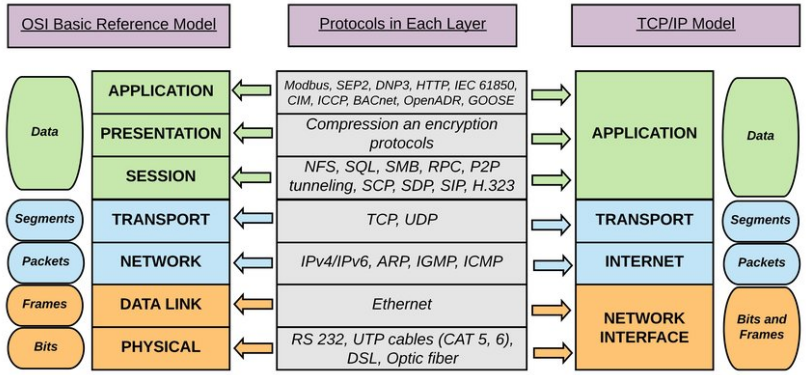
Cái gọi là cuộc chiến giao thức truyền thông là một giai đoạn kéo dài khoảng từ những năm 1970 đến đầu những năm 1990. Khi các bên khác nhau trong cộng đồng khoa học máy tính quốc tế, bao gồm các nhà nghiên cứu cá nhân, các nhóm nhà khoa học và các tổ chức, liên tục tranh luận sôi nổi về việc lựa chọn một bộ giao thức truyền thông sẽ hỗ trợ hiệu suất mạng tốt nhất.

Về cơ bản, cuộc chiến giao thức là cuộc chiến của 2 kiến trúc tiêu chuẩn giao tiếp cơ bản:

- **TCP/IP** : được phát triển bởi Bộ quốc phòng Hoa Kỳ (DoD – Department of Defense)
- Các tiêu chuẩn giao diện được phát triển bởi các nhà nghiên cứu máy tính ở Châu Âu (chủ yếu là Vương quốc Anh và Pháp) – đầu tiên là tiêu chuẩn **X.25** và sau là tiêu chuẩn **OSI** (Open Systems Interconnection)



X.25 Layer Mapping with OSI Model



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

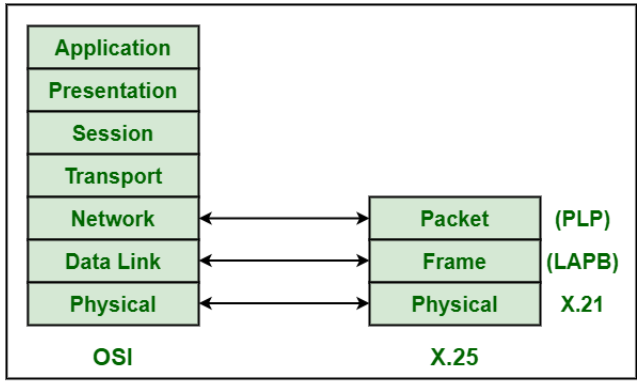
LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

TCP/IP vs X.25:

Phiên bản đầu tiên của Chương trình kiểm soát truyền tải (TCP), trước giao thức TCP/IP được xây dựng vào năm 1974. Nghiên cứu về một giao thức truyền thông mạng phổ quát, được hỗ trợ bởi cơ sở hạ tầng ARPANET và các nhà nghiên cứu ARPANET là một phần của Tổ chức mạng quốc tế. Nhóm được tạo ra để hình thành một giao thức cho internet hoạt động

Các nhà nghiên cứu từ các tổ chức và nhóm quốc tế khác nhau nhằm mục đích cùng nhau thống nhất về một tiêu chuẩn giao thức đầu cuối (end-to-end). Nhưng cuộc tranh luận giữa những người ủng hộ 2 cách tiếp cận khác nhau đối với truyền thông dữ liệu: Datagram và mạch ảo. Đã biến các quy trình thành điều mà tạp chí Computerworld báo cáo về qua trình hình thành giao diện tiêu chuẩn cho các mạng truyền thông chuyển mạch. Nó được mô tả là "cuộc chiến dành tiêu chuẩn truy cập"

Mạng sử dụng X.25 phổ biến vào cuối những năm 1970 và 1980 với các công ty viễn thông và trong các hệ thống giao dịch tài chính như máy rút tiền tự động.
Tuy nhiên, hầu hết người dùng đã chuyển sang hệ thống Internet Protocol (IP). X.25 đã được sử dụng cho đến năm 2015.



X.25 Layer Mapping with OSI Model

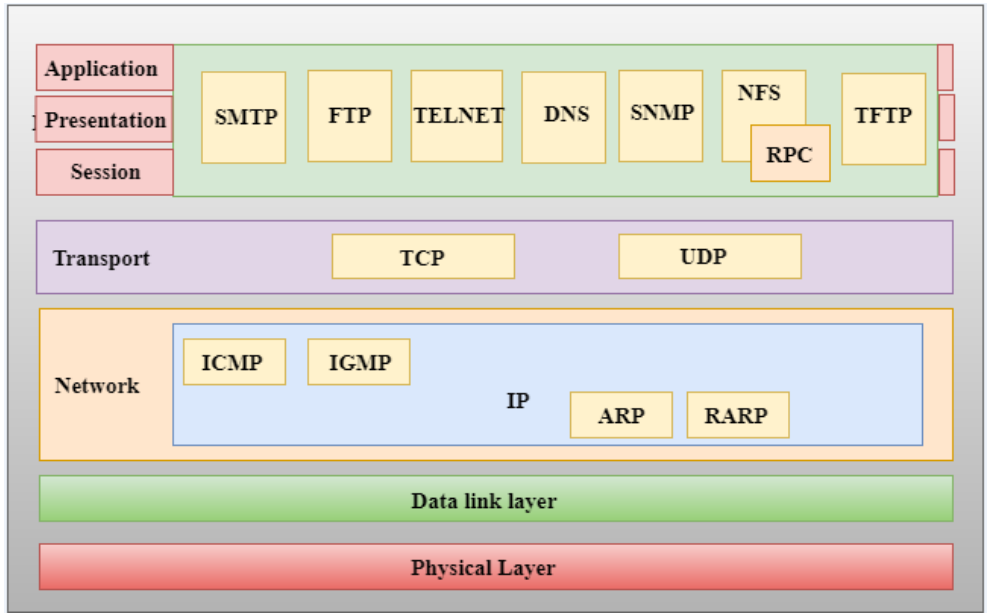
LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

TCP/IP (hay còn gọi là bộ giao thức Internet):

Giao thức (lúc đầu được đặt tên IP/TCP) trong phiên bản thứ 4 của nó đã được cài đặt trên SATNET vào năm 1982, trên ARPANET vào năm 1983 và trở thành một mô hình mạng tiêu chuẩn hiện được gọi là TCP/IP (đôi khi còn được gọi là mô hình DARPA, mô hình ARPANET hay mô hình Bộ quốc phòng (DoD)

TCP/IP chứa nhiều lớp giao thức và sử dụng các cách tiếp cận khác nhau để truyền dữ liệu, được biết đến với tên gọi "Bộ giao thức Internet".



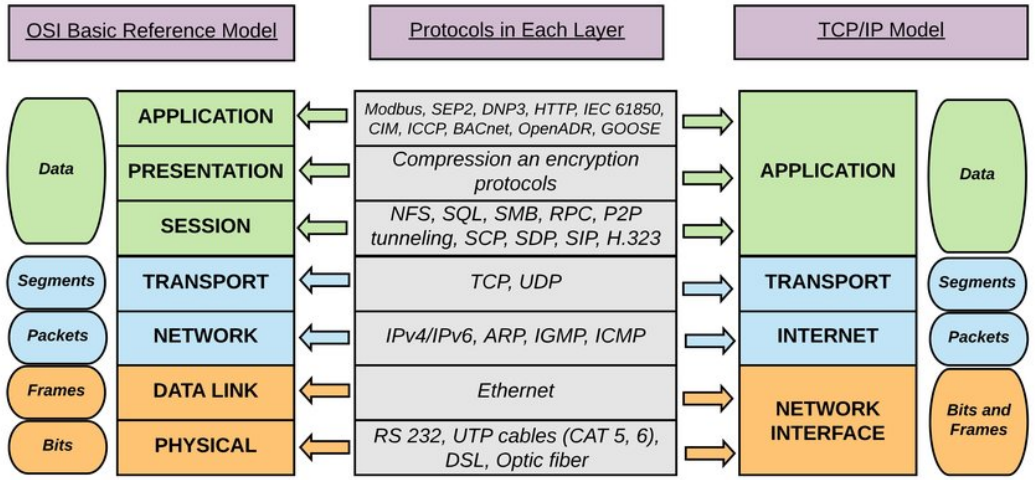
LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

Mô hình OSI (Open Systems Interconnection):

Mô hình tham chiếu OSI được xác định vào cuối những năm 1970 và được xuất bản vào năm 1984. Nó cung cấp nền tảng cho sự phối hợp phát triển tiêu chuẩn ISO từ mục đích kết nối hệ thống. Trong mô hình OSI, các giao diện truyền thông được tổ chức thành 7 lớp:

- Lớp vật lý (Physical layer)
- Lớp liên kết dữ liệu (Data link layer)
- Lớp mạng lưới (Network layer)
- Lớp vận chuyển (Transport layer)
- Lớp phiên (Session layer)
- Lớp trình bày (Presentation layer)
- Lớp ứng dụng (Application layer)



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

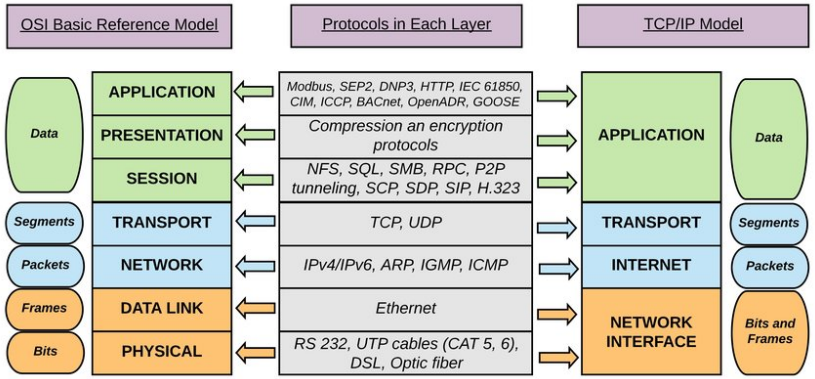
LỊCH SỬ GIAO THỨC TRUYỀN THÔNG

Mô hình OSI (Open Systems Interconnection) vs TCP/IP:

Bộ giao thúc Internet(TCP/IP) sử dụng một kiến trúc khác, kết hợp các lớp liên kết vật lý và dữ liệu của mô hình OSI thành một lớp liên kết duy nhất. Ngoài ra, TCP/IP có một lớp ứng dụng cho tất cả các giao thức trái ngược với các lớp ứng dụng, lớp trình bày và lớp phiên trong mô hình OSI

Cuộc tranh luận xung quanh mô hình giao thức cơ bản phù hợp nhất đặc biệt sôi nổi, điều này cho phép các nhà sử học của lĩnh vực khoa học máy tính đặt tên cho giai đoạn kéo dài từ cuối những năm 1980 đến giữa những năm 1990 là " Cuộc chiến tiêu chuẩn Internet – OSI"

"Cuộc chiến" cuối cùng đã ngã ngũ với phần thắng thuộc về TCP/IP nhờ bộ giao thức Internet tiếp tục mở rộng và cuối cùng phát triển thành IPv6, đây vẫn là phiên bản mới nhất của tiêu chuẩn.
Mô hình tham chiếu giao thức OSI không được phổ biến và áp dụng rộng rãi như vậy. Tuy nhiên, nó vẫn còn phù hợp và ngày nay, nó được sử dụng trong một số lĩnh vực nhất định như điện toán đám mây. Tiêu chuẩn X.25 cũng không biến mất hoàn toàn, nó ứng dụng trong một số thị trường ngách.

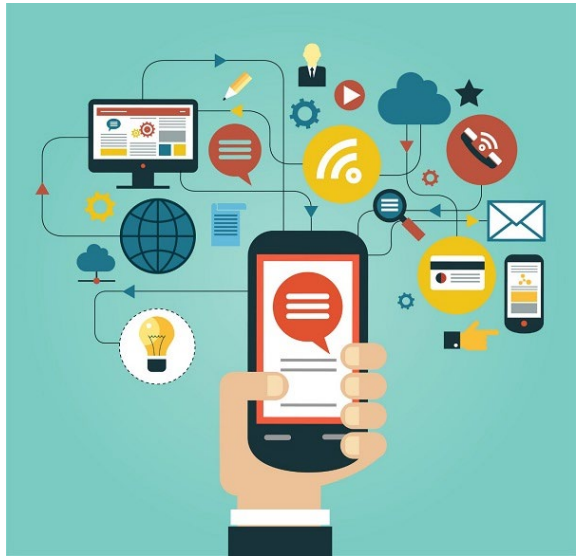


LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

KHÁI NIỆM GIAO THỨC TRUYỀN THÔNG

Khái niệm và định nghĩa:

- **Giao thức truyền thông - Communication protocol**, hay còn được dịch là giao thức giao tiếp, giao thức liên mạng, giao thức tương tác hay giao thức trao đổi thông tin, là một tập hợp các quy tắc chuẩn cho phép hai hoặc nhiều thực thể trong một hệ thống thông tin liên lạc để trao đổi thông tin, dữ liệu qua các kênh truyền thông.
- **Giao thức** sẽ định nghĩa các quy tắc (rule), cú pháp (syntax), ngữ nghĩa (semantics). sự đồng bộ (synchronization) trong quá trình truyền thông và có thể thêm phương pháp khắc phục lỗi trên đường truyền.
- **Giao thức truyền thông** có thể được thực thi trên phần cứng, phần mềm hoặc cả hai.

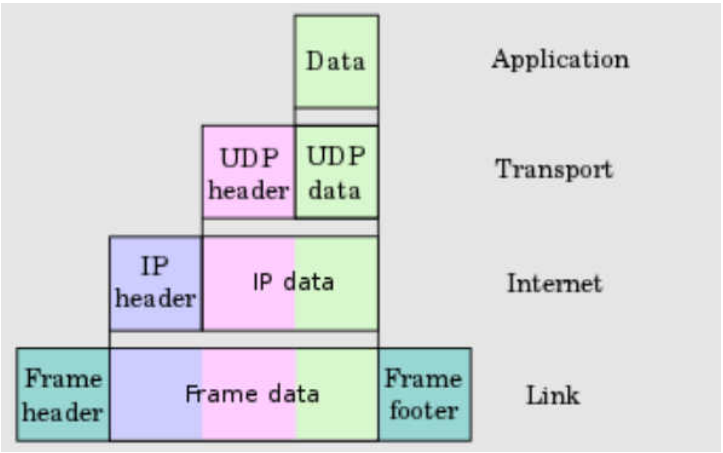


LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

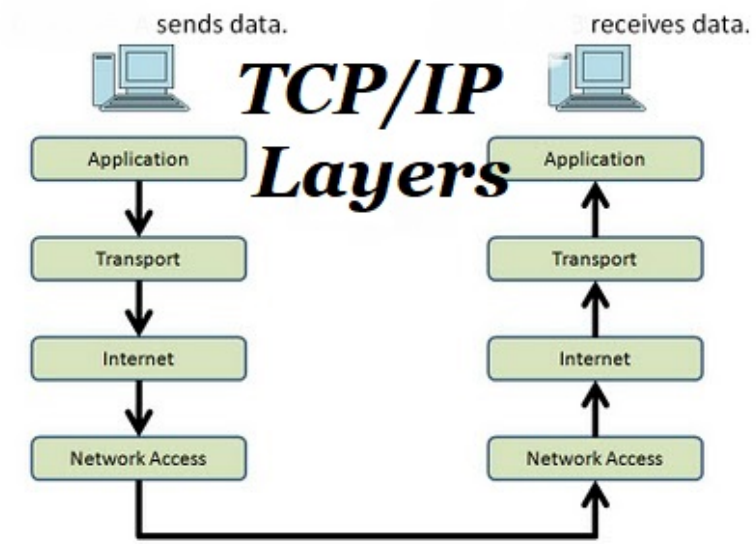
CÁCH THỨC HOẠT ĐỘNG

- **Cách thức hoạt động của giao thức truyền thông**: khi dữ liệu được truyền trên mạng sẽ được chia thành nhiều giai đoạn xử lý, bao gồm cả hệ thống. Ở mỗi giai đoạn sẽ lại có một số hoạt động được diễn ra theo các mô hình về giao thức mạng và khi đó người dùng không thể biết được nó diễn ra ở giao đoạn nào trong mô hình tiêu chuẩn. Mô hình hoạt động này được gọi là mô hình OSI.

- Tuy nhiên các giai đoạn sẽ hoạt động theo một trình tự nhất định giống nhau trên mỗi máy tính mạng. Đối với những giai đoạn ở máy tính gửi thì sẽ phải được thực hiện từ trên xuống dưới. Còn ở đối với máy tính nhận dữ liệu thì chúng phải được thực hiện từ dưới lên.



Mô hình TCP/IP

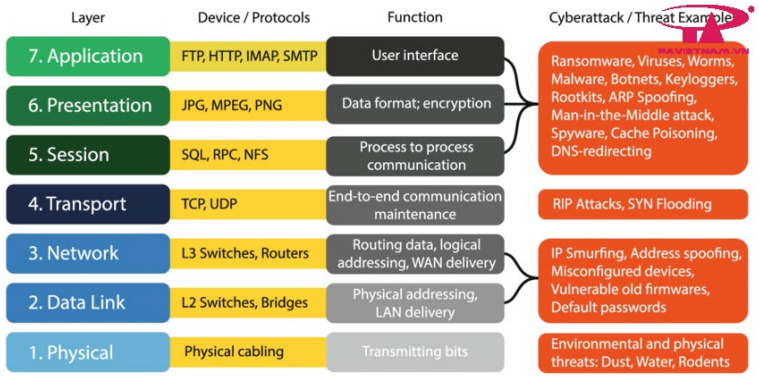


LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

GIAO THỨC TRUYỀN THÔNG

Có nhiều giao thức được sử dụng để giao tiếp hoặc truyền đạt thông tin trên Internet, dưới đây là một số các giao thức tiêu biểu:

TCP (Transmission Control Protocol): thiết lập kết nối giữa các máy tính để truyền dữ liệu. Nó chia nhỏ dữ liệu ra thành những gói (packet) và đảm bảo việc truyền dữ liệu thành công.
IP (Internet Protocol): định tuyến (route) các gói dữ liệu khi chúng được truyền qua Internet, đảm bảo dữ liệu sẽ đến đúng nơi cần nhận.
HTTP (HyperText Transfer Protocol): cho phép trao đổi thông tin (chủ yếu ở dạng siêu văn bản) qua Internet.
HTTPs (Hypertext Transfer Protocol Security (SSL/TLS)): tương tự như HTTP nhưng sử dụng với kết nối bảo mật (SSL/TLS).
SSH (Secure Shell): được sử dụng để quản lý các thiết bị mạng một cách an toàn ở cấp lệnh(thay thế cho giao thức Telnet)
FTP (File Transfer Protocol): cho phép trao đổi tập tin qua Internet.
DNS(Domain Name System): dùng để chuyển đổi tên miền thành địa chỉ IP.
SMTP (Simple Mail Transfer Protocol): cho phép gởi các thông điệp thư điện tử (email) qua Internet.
POP3 (Post Office Protocol, phiên bản 3): cho phép nhận các thông điệp thư điện tử qua Internet.
MIME (Multipurpose Internet Mail Extension): một mở rộng của giao thức SMTP, cho phép gởi kèm các tập tin nhị phân, phim, nhạc,... theo thư điện tử.
WAP (Wireless Application Protocol): cho phép trao đổi thông tin giữa các thiết bị không dây, như điện thoại di động.



Lớp; Thiết bị/Giao thức; Chức năng; Tấn công mạng/mối đe dọa

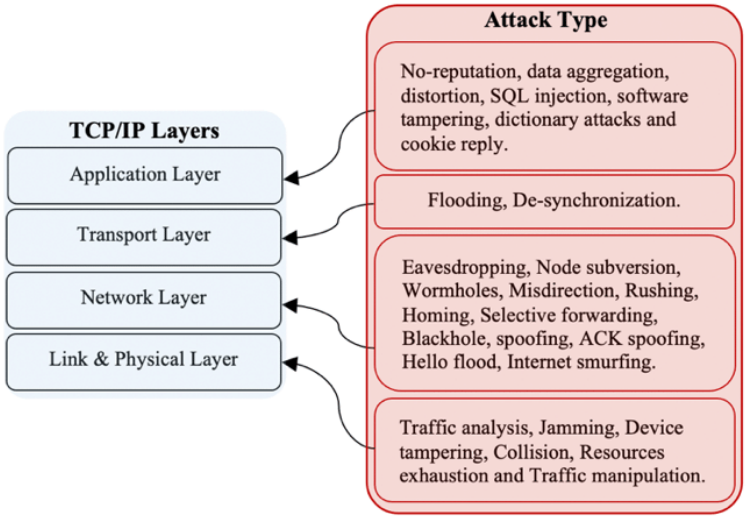
Mô hình OSI

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

GIAO THỨC TRUYỀN THÔNG

TCP/IP (Transmission Control Protocol/ Internet Protocol)

- TCP/IP là bộ giao thức cho phép kết nối các hệ thống mạng không đồng nhất với nhau. Ngày nay, TCP/IP được sử dụng rộng rãi trong các mạng cục bộ cũng như trên mạng Internet toàn cầu.
- Tuy nhiên, TCP/IP là một giao thức mở nên các hacker có thể tìm thấy những lỗ hổng của nó một cách dễ dàng bằng cách thử nhiều kiểu tấn công khác nhau. Nhiều cuộc tấn công nhằm vào bộ giao thức TCP/IP bao gồm cả các cuộc tấn công giả mạo, tấn công từ chối dịch vụ, tấn công xác thực định tuyến.
- Các công cụ khác nhau đã được thiết kế để phân tích và xác định sự có mặt của các lỗ hổng và cách thức thực hiện khai thác chúng trong bộ giao thức TCP/IP như tường lửa, hệ thống phát hiện xâm nhập, phân tích giao thức, nghe lén và quét lỗ hổng.
- Tên TCP/IP liên quan đến hai giao thức quan trọng nhất trong bộ giao thức - Giao thức kiểm soát truyền tải (Transmission Control Protocol - TCP) và Giao thức Internet (Internet Protocol - IP)



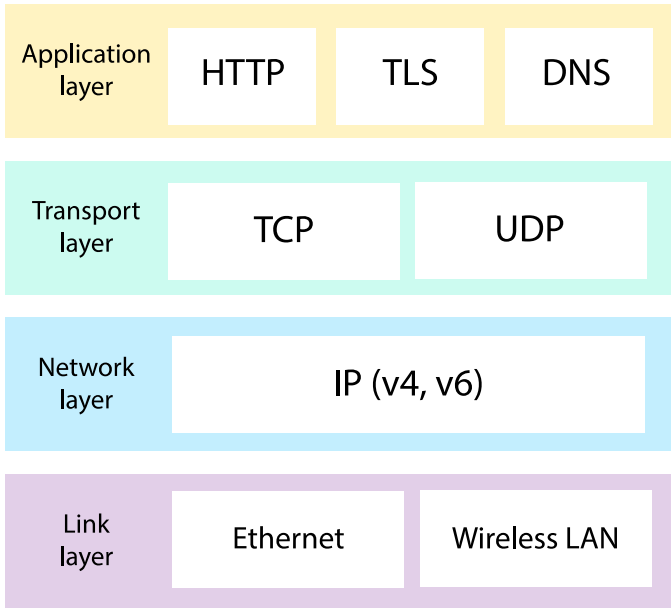
LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

GIAO THỨC TRUYỀN THÔNG

Giao thức IP

Nhiệm vụ chính của giao thức IP là cung cấp khả năng kết nối các mạng con thành liên kết mạng để truyền dữ liệu, vai trò của IP là vai trò của giao thức tầng mạng trong mô hình OSI. Giao thức IP là một giao thức kiểu không liên kết (connectionlees) có nghĩa là không cần có giai đoạn thiết lập liên kết trước khi truyền dữ liệu.

Khi giao thức IP được khởi động nó trở thành một thực thể tồn tại trong máy tính và bắt đầu thực hiện những chức năng của mình, lúc đó thực thể IP là cấu thành của tầng mạng, nhận yêu cầu từ các tầng trên nó và gửi yêu cầu xuống các tầng dưới nó.



Đối với thực thể IP ở máy nguồn, khi nhận được một yêu cầu gửi từ tầng trên, nó thực hiện các bước sau đây:

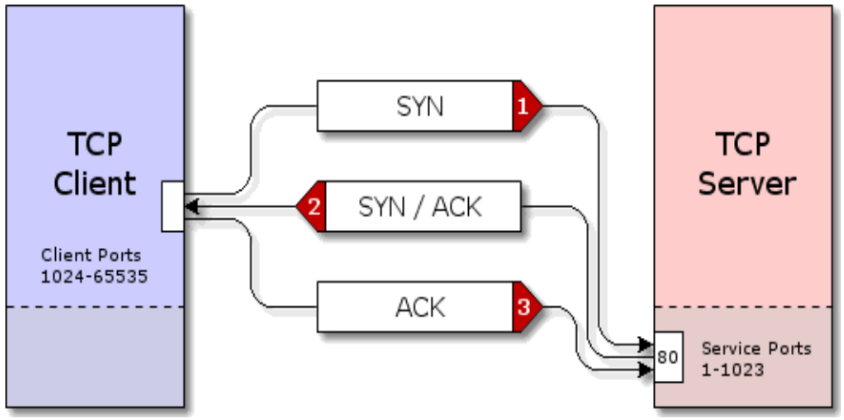
- Tạo một IP datagram dựa trên tham số nhận được.
- Tính checksum và ghép vào header của gói tin.
- Ra quyết định chọn đường: hoặc là trạm đích nằm trên cùng mạng hoặc một gateway sẽ được chọn cho chặng tiếp theo.
- Chuyển gói tin xuống tầng dưới để truyền qua mạng.

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

GIAO THỨC TRUYỀN THÔNG

Giao thức điều khiển truyền dữ liệu TCP

TCP là một giao thức "hướng kết nối" (connection oriented), nghĩa là cần phải thiết lập liên kết giữa hai thực thể TCP trước khi chúng trao đổi dữ liệu với nhau. Giữa client và server muốn thực hiện kết nối để trao đổi thông tin thì chúng phải thực hiện qua ba bước sau (cơ chế bắt tay ba bước) như Hình 1.



Hình 1. Thiết lập kết nối TCP giữa client và server

- **Bước 1**: Client gửi gói tin SYN tới server thông báo yêu cầu thiết lập kết nối. Lúc này một kết nối tiềm năng (potential connection) đã được thiết lập giữa client và server.
- **Bước 2**: Server sau khi nhận được tín hiệu SYN trên sẽ gửi lại cho client gói tin SYN/ACK xác nhận việc thiết lập liên kết.
- **Bước 3**: Client sau khi nhận được gói tin SYN/ACK trên, nó sẽ gửi tiếp cho Server gói tin ACK. Kết thúc bước này giữa client và server đã hoàn thành một kết nối.

với **SYN**: là một bit cờ (flag) trong gói tin TCP/IP dùng để thông báo bắt đầu kết nối, **ACK**: là một bit cờ (flag) trong gói tin TCP/IP của bên nhận gửi cho bên gửi để thông báo đã nhận được gói tin, **SEQ**: là số thứ tự của gói tin.

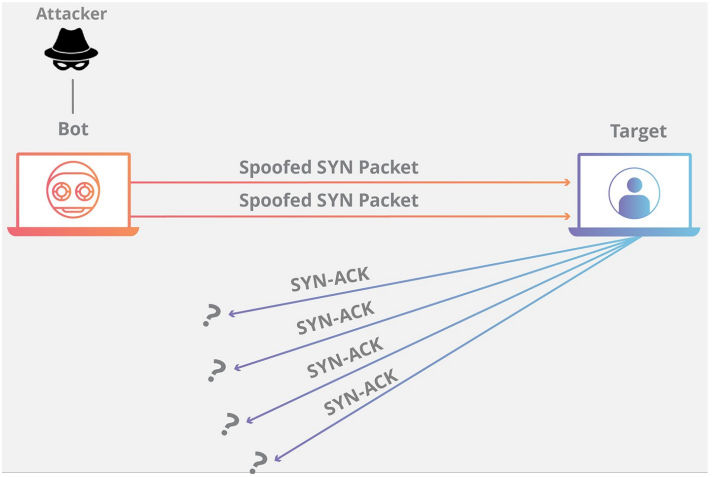
LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Tấn công TCP Syn Flood

Kiểu tấn công TCP SYN flood là một kiểu tấn công trực tiếp vào máy chủ bằng cách tạo ra một số lượng lớn các kết nối TCP nhưng không hoàn thành các kết nối này.

Hacker sử dụng cơ chế bắt tay ba bước trong quá trình thiết lập kết nối giữa hai thực thể TCP. Máy hacker sử dụng một địa chỉ giả mạo và gửi hàng loạt bản tin yêu cầu kết nối tới máy tính nạn nhân với bit SYN được bật (bước 1), khi đó nạn nhân nhận được gói tin này ngay lập tức nó sẽ dành một phần bộ nhớ cho kết nối này, máy tính nạn nhân nhận được yêu cầu trên thì trả lời lại với bản tin bit ACK, SEQ được bật (bước 2) và chờ để hacker trả lời, nhưng hacker không trả lời điều này sẽ làm cho máy tính nạn nhân luôn ở trong tình trạng chờ và dần dần sẽ cạn kiệt tài nguyên không thể phục vụ được nữa

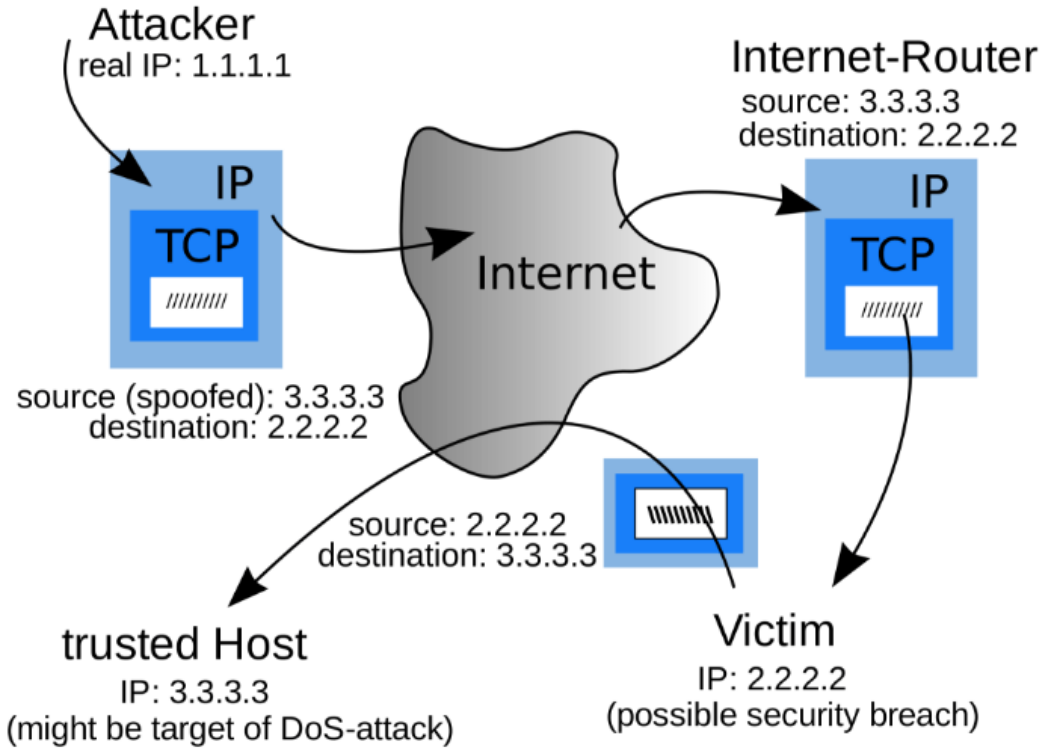


LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Địa chỉ IP giả mạo liên quan đến việc tạo ra các gói TCP/IP sử dụng địa chỉ IP giả với mục đích để che giấu danh tính hoặc giả mạo danh tính chủ sở hữu của địa chỉ IP được sử dụng.



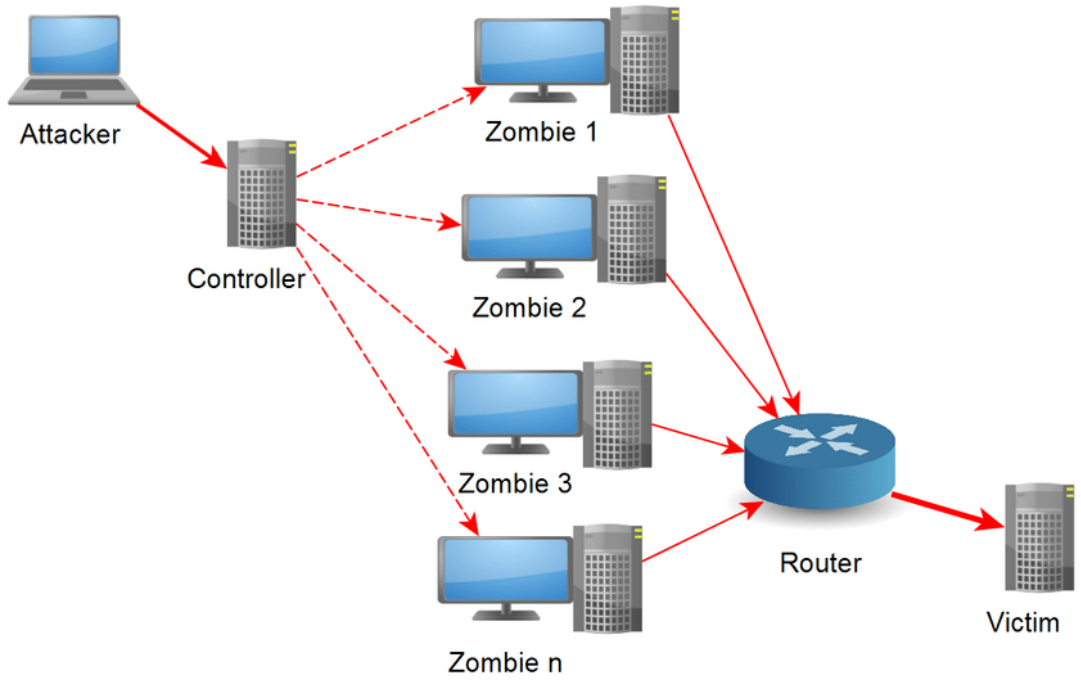
Hành vi này có thể thực hiện các cuộc tấn công khác nhau như sau:

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Tấn công từ chối dịch vụ (Denial of Service Attack - DoS): Hacker có thể gửi một số lượng lớn các gói tin yêu cầu kết nối (SYN) tới máy nạn nhân mà không cần quan tâm phản hồi (ACK) vì Hacker sẽ không nhận được bất kỳ gói tin phản hồi từ các nạn nhân [5]. Tất cả gói phản hồi sẽ được hướng tới các địa chỉ IP giả mạo. Ngoài ra, danh tính của kẻ tấn công cũng sẽ không được tiết lộ. Cuộc tấn công này làm cho nạn nhân bị loại khỏi dịch vụ.



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Tấn công từ chối dịch vụ phản xạ phân tán (Distributed Reflection DOS- DRDoS): Mục tiêu chính của DRDoS là chiếm đoạt toàn bộ băng thông của máy nạn nhân, làm tắc nghẽn hoàn toàn đường kết nối từ máy nạn nhân vào xương sống của Internet và làm tiêu hao tài nguyên. Trong suốt quá trình máy nạn nhân bị tấn công bằng DRDoS, không một máy khách nào có thể kết nối được vào máy nạn nhân đó, tất cả các dịch vụ chạy trên nền TCP/IP như: DNS, HTTP, FTP, POP3, ... đều bị vô hiệu hóa.

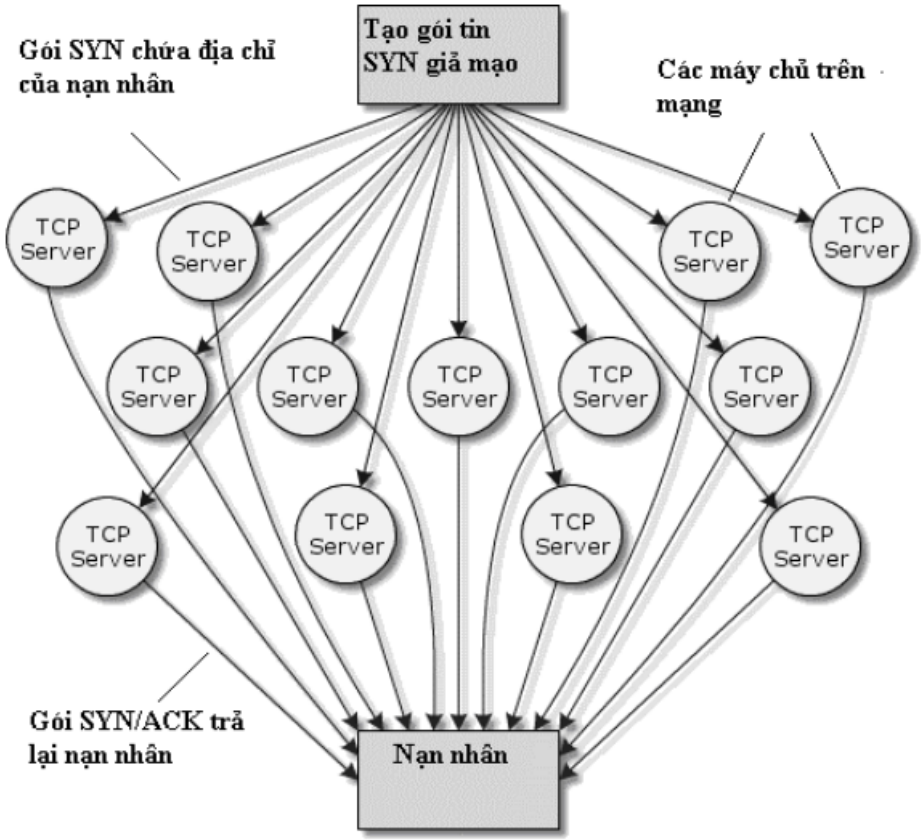
Hacker sử dụng các server phản xạ, hacker sẽ gửi yêu cầu kết nối (SYN) tới các server có bandwidth rất cao trên mạng – server phản xạ, các gói tin yêu cầu kết nối này mang địa chỉ IP giả - chính là địa chỉ IP của máy nạn nhân. Các server phản xạ này gửi lại máy nạn nhân các gói SYN/ACK dẫn tới hiện tượng nhân băng thông – bandwidth multiplication (Hình 2).

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Tấn công từ chối dịch vụ phản xạ phân tán (Distributed Reflection DOS- DRDoS):



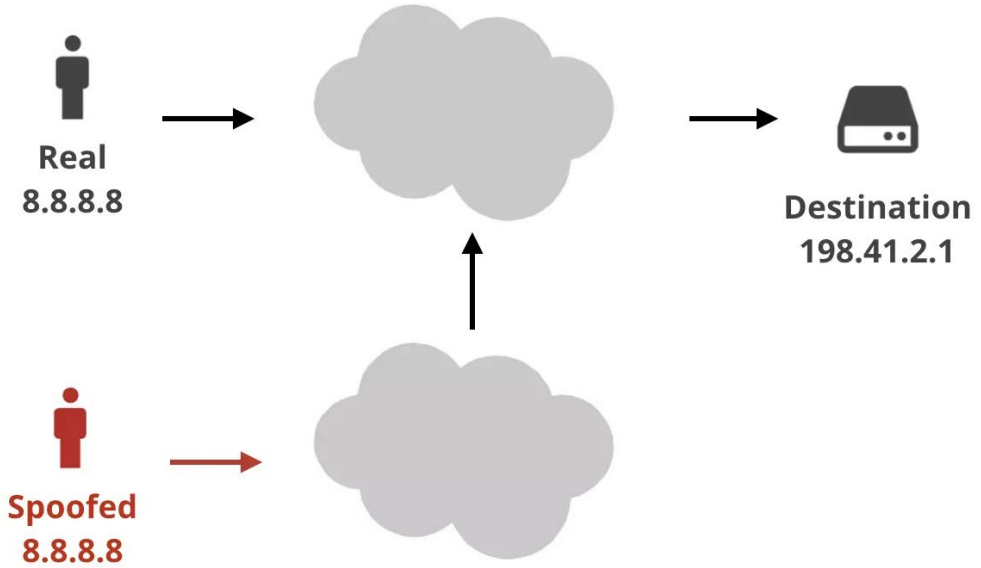
Hình 2. Tấn công kiểu DRDoS.

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Tấn công môi trường xác thực bằng địa chỉ IP: Là tấn công môi trường xác thực dựa trên địa chỉ IP. Trong trường hợp mạng nội bộ, xác thực bằng địa chỉ IP, không cần một tên đăng nhập hoặc mật khẩu để truy cập. Hacker có thể giả địa chỉ IP để có được quyền truy cập trái phép vào máy tính nạn nhân mà không xác thực.

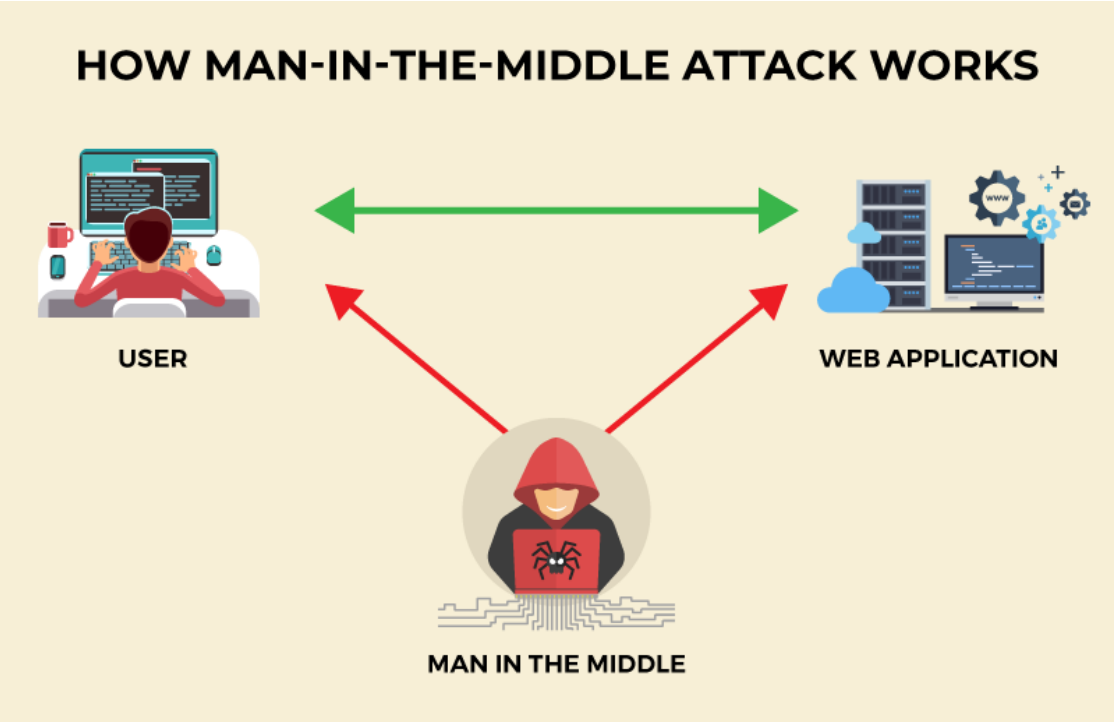


LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Kiểu tấn công người đứng giữa (Man in The Middle Attack): Nó liên quan đến việc hack một phiên liên lạc được xác thực giữa hai máy tính A và B. Hacker sau khi hoàn thành các bước xác thực sẽ giả mạo địa chỉ IP của một nạn nhân A hoặc B đã được xác thực và nhận được các gói tin qua lại giữa hai máy A và B



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

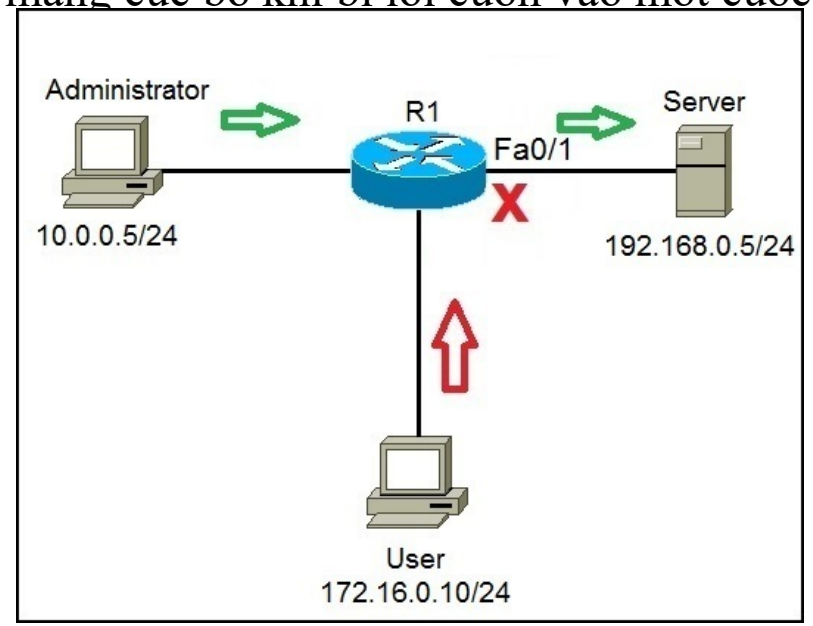
TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Các biện pháp bảo vệ chống lại giả mạo địa chỉ IP (IP Spoofing):

Dùng mật mã xác thực: Nếu cả hai đầu của cuộc nói chuyện đã được xác thực, khả năng tấn công theo kiểu Man-in-the-Middle Attack có thể được ngăn chặn. Mã hoá traffic giữa các thiết bị (giữa 2 router, hoặc giữa 2 hệ thống đầu cuối và router) bằng một IPSec tunnel.

Dùng danh sách kiểm tra truy cập Access Control List (ACL) trên các interface của router. Một ACL có thể được dùng để loại bỏ những traffic từ bên ngoài mà lại được đóng gói bởi một địa chỉ trong mang cục bộ khi bị lôi cuốn vào một cuộc tấn công DDoS.



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Giả mạo địa chỉ IP (IP Spoofing)

Các biện pháp bảo vệ chống lại giả mạo địa chỉ IP (IP Spoofing):

Bộ lọc các gói dữ liệu: Điều này ngăn chặn các gói tin gửi đến, chúng không đáp ứng các tiêu chí chính sách bảo mật, như các yêu cầu ping từ bên ngoài mạng được lọc. Tương tự như vậy, gói tin đi ra cũng có thể được lọc dựa trên tiêu chí địa chỉ cổng, IP của nguồn hoặc đích.

Sử dụng lớp trên: Kết hợp cơ chế phòng vệ ở tầng trên có thể ngăn chặn IP giả mạo như sử dụng số thứ tự trong trường số thứ tự của gói tin TCP ở tầng giao vận như vậy kẻ tấn công phải đoán được số thứ tự cũng trước khi giả mạo gói tin.

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Hack kết nối (Connection Hacking):

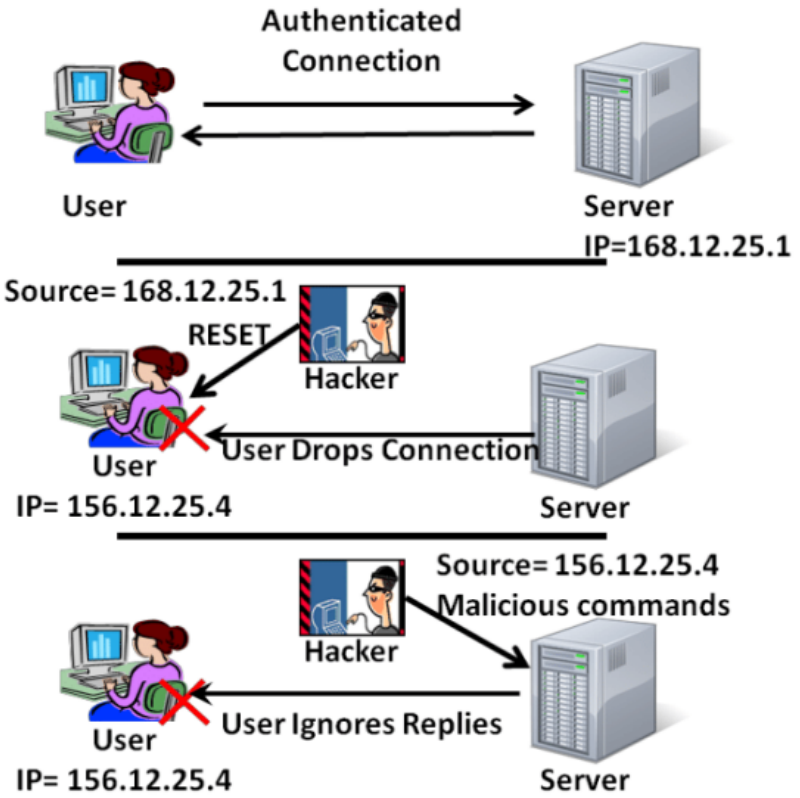
Xác thực giữa User và Server diễn ra trong giai đoạn đầu thiết lập kết nối. Từ đó không có yêu cầu xác nhận. Như hình bên, hacker có thể lợi dụng điều này bằng cách giả mạo địa chỉ IP của Server (168.12.25.1) gửi một thiết lập lại cho User và sau đó hacker tiếp tục giả mạo địa chỉ IP của User (156.12.25.4) tiếp tục phiên làm việc với Server bằng sử dụng địa chỉ IP giả mạo.

Một cách khác của việc hack phiên liên lạc là Hacker có thể ăn cắp tập tin cookie được lưu trữ trên máy nạn nhân hoặc có được cookie của máy nạn nhân bằng cách nghe lén (Sniffer) các gói tin trên mạng không được mã hóa. Sau đó, những cookie có thể được sử dụng với các Web server để thiết lập một phiên xác thực.

Các biện pháp phòng chống hack kết nối được chỉ ra như sau:

• **Mã hóa**: Mã hóa bảo đảm cho việc trao đổi gói tin giữa User và Server không bị Hacker đọc được nội dung và cũng không thể sử dụng chúng cho việc cướp quyền.

• **Sử dụng tái xác thực**: Yêu cầu xác thực định kỳ sau một thời gian nhất định.



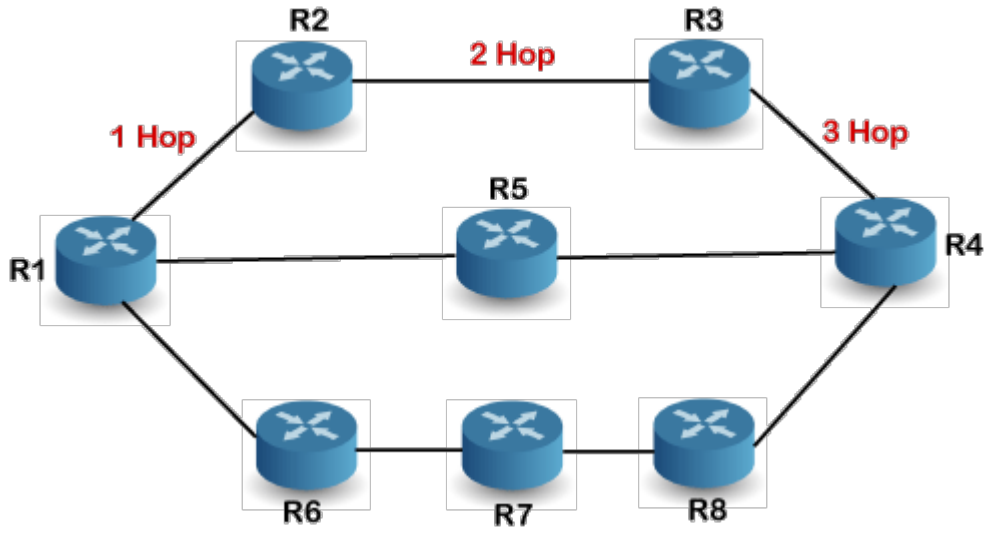
LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Tấn công giao thức định tuyến RIP:

Routing Information Protocol (RIP) là một giao thức định tuyến được sử dụng trong bộ giao thức TCP/IP để định tuyến các gói dựa trên số chặng (hop). Trước khi đưa ra quyết định định tuyến RIP đếm số bước nhảy trên mọi hướng có thể và chọn đường đi tới đích có số bước nhảy ngắn nhất. Giá trị đếm hop tối đa có thể là 15 hop và bất cứ trường hợp nào lớn hơn 15 được coi là vô hạn. Cơ chế này được sử dụng để tránh gói tin rơi vào vòng lặp.

Phiên bản chuẩn của RIP không có phần xác thực. Thông tin cung cấp trong bản tin RIP thường được sử dụng mà không có sự kiểm tra xác thực lại chính nó. Hacker có thể giả mạo 1 bản tin RIP, ví dụ xác định máy X có tuyến ngắn nhất ra ngoài mạng. Như vậy, mọi gói tin gửi ra từ mạng này sẽ được định tuyến qua X và máy X có thể kiểm soát, sửa đổi gói tin.



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Tấn công giao thức định tuyến RIP:

Để phòng chống lại tấn công giao thức RIP, người ta sử dụng một số biện pháp:

- Sử dụng thuật toán xác thực mật khẩu đơn giản, làm cho việc tấn công qua RIP khó khăn hơn.
- Giải pháp IPsec VPN cũng cung cấp khả năng mã hóa thông tin định tuyến qua các routers sử dụng IPsec VPN.
- Các gói dữ liệu được lọc dựa trên mã nguồn và đích.
- Phân tích nhật ký (log) thường xuyên nhằm phát hiện bất thường.
- Kiểm tra các đường truyền trước khi chấp nhận

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Tấn công tràn ngập gói tin ICMP:

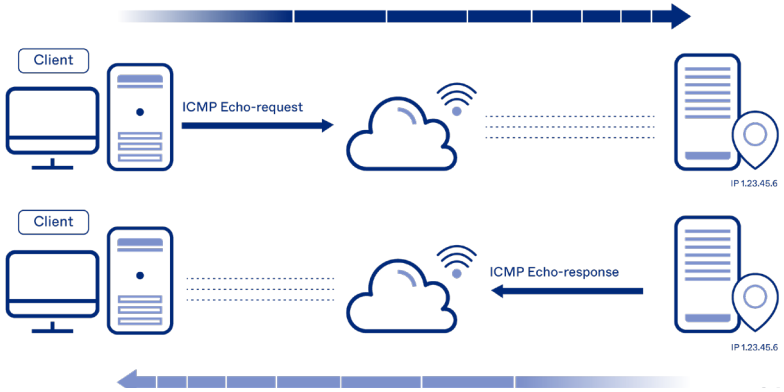
Giao thức Internet Control Message Protocol (ICMP) thực hiện truyền các thông báo điều khiển (báo cáo về tình trạng lỗi trên mạng ...) giữa các gateway hay các trạm của liên mạng. Tình trạng lỗi có thể là: một datagram không thể tới được đích của nó, hoặc một router không đủ bộ đệm để lưu và chuyển một datagram.

Ping là một chương trình dùng để báo cho người sử dụng biết hai host trên mạng có thông với nhau không. Ping dựa trên giao thức ICMP. Nó cho phép người sử dụng gửi các gói tin tới một hệ thống ở xa và hiển thị khoảng thời gian từ khi gửi gói tin đến khi nhận được phản hồi từ phía nhận (Round Trip Time: RTT). Gói tin được gửi đi là ICMP echo request, gói tin phản hồi là ICMP echo response.

Hacker sẽ sử dụng giao thức ICMP này để tấn công nạn nhân theo cách sau:

• **Bước 1**: Kẻ tấn công giả mạo là nạn nhân, gửi đi một lệnh Ping với địa chỉ IP là của nạn nhân và địa chỉ đích là dạng broadcast của một mạng nào đó. Sau bước này tất cả các host trong mạng 10.0.0.x sẽ nhận được gói tin ICMP từ host của nạn nhân.

• **Bước 2**: Do sự nhầm lẫn như trên mà tất cả các host trong mạng 10.0.0.x đều gửi về cho nạn nhân một gói tin ICMP echo response. Hàng loạt các gói tin dạng này là nguyên nhân gây lên hện tượng làm băng thông tới host của nạn nhân bị chiếm dụng. Nạn nhân sẽ không thể giao dịch với các host khác trên mạng.



LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

TẤN CÔNG TCP/IP

Tấn công tràn ngập gói tin ICMP:

Phòng chống lại các cuộc tấn công ICMP có bằng các biện pháp sau đây:

- Đối với các firewall cứng, kích hoạt cơ chế ICMP Flooding Protection.
- Đối với các firewall mềm trên linux như iptables, có thể sử dụng luật sau:

```
# iptables –A INPUT –p icmp –m limit –limit 2/second –limit-burst 2 –j ACCEPT
```

- Đối với hệ điều hành window, chặn toàn bộ các gói tin ping bằng cách sử dụng lệnh sau trên cmd:

```
# netsh firewall set icmpsetting type all mode disable
```

LỖ HỔNG GIAO THỨC TRUYỀN THÔNG

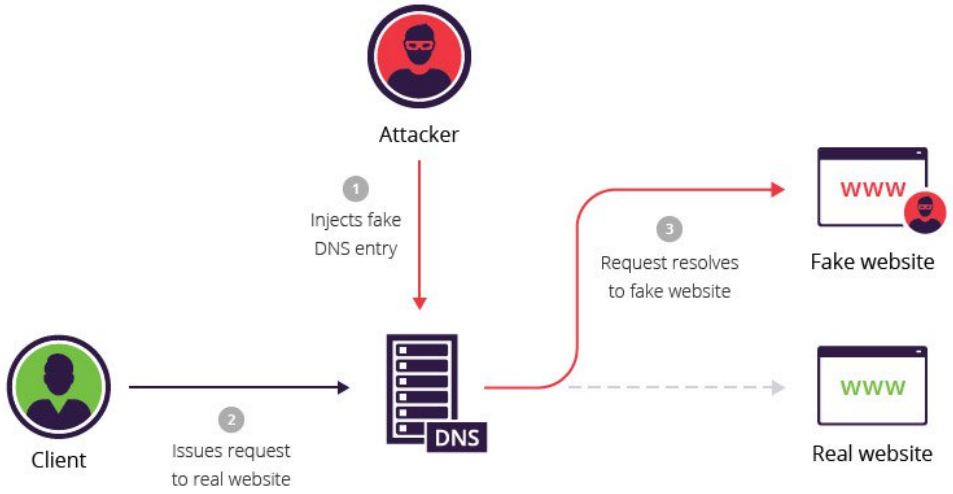
TẤN CÔNG TCP/IP

Tấn công giả mạo DNS(DNS Snoffing Attack) :

Domain Name System (DNS) là một dịch vụ được sử dụng trong lớp ứng dụng để ánh xạ một địa chỉ IP sang một tên miền và ngược lại. Tấn công giả mạo DNS liên quan tới nhiễm độc bộ nhớ đệm DNS (DNS cache poisoning), hay còn được gọi là giả mạo DNS, là một kiểu tấn công khai thác lỗ hổng trong hệ thống tên miền (DNS – domain name system) để chuyển hướng lưu lượng truy cập Internet từ máy chủ hợp pháp tới các máy chủ giả mạo.

Cách phòng chống giả mạo DNS được đề cập:

- Sử dụng xác thực dựa trên địa chỉ IP thay vì dựa trên tên miền.
- Sử dụng mã hóa để ngăn chặn giả mạo DNS.



BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Công cụ dò tìm mạng (Network Sniffer Tools):

Công cụ dò tìm mạng (Network Sniffer Tool) - là công cụ, phần mềm hoặc phần cứng, được các quản trị viên dùng theo dõi, chuẩn đoán, phát hiện các sự cố mà không thay đổi hoặc chuyển hướng các gói tin nhằm giúp cải thiện hoạt động hệ thống mạng.

Wireshark: là phần mềm phân tích gói mạng (network packet analyzer). Nhiệm vụ của nó là nắm bắt tất cả các gói mạng rồi hiển thị dữ liệu của gói đó một cách chi tiết nhất. Nó bắt các gói tin trực tiếp, và có thể phân tích chúng trong chế độ offline. Các gói này có thể bao gồm Ethernet, IEEE 802.11, PPP, và loopback. Wireshark có thể làm việc trên nhiều nền tảng như Windows, Linux, OS X, Solaris, NetBSD, FreeBSD. Nó cung cấp giao diện đồ họa và giao diện dòng lệnh.

Tcpdump: là phần mềm miễn phí được sử dụng để phân tích các gói tin TCP/IP bằng cách sử dụng giao diện dòng lệnh. Công cụ này hoạt động chủ yếu trên Linux, nhưng cũng có thể làm việc trên các hệ điều hành khác như Solaris, BSD, HPUX, AIX và Windows thông qua WinDump

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Công cụ dò tìm mạng (Network Sniffer Tools):

Kismet: không chỉ là công cụ phân tích gói tin mà còn là một hệ thống phát hiện xâm nhập (IDS). Nó có thể bắt các gói tin trên mạng không dây sử dụng chuẩn 802.11a/b/g/n, các kết quả được hiển thị bằng cách sử dụng giao diện dòng lệnh. Kismet được viết bằng C ++ và có thể làm việc trên các hệ điều hành Linux, Solaris, BSD, Mac OS X, HP-UX và AIX.

Ettercap: là một công cụ khai thác và tấn công trên mạng LAN. Nó có khả năng dò tìm tất cả các máy và tiến hành nghe lén, đây là một công cụ không thể thiếu khi tấn công một mạng LAN. Nó làm việc trên nhiều nền tảng như Microsoft Windows, Linux, Mac OS X, BSD và Solaris

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Các công cụ quét lỗ hổng:

Các công cụ quét lỗ hổng được sử dụng để tìm các lỗ hổng trên mạng máy tính, hệ thống máy tính, hoặc các ứng dụng máy tính. Những công cụ này được sử dụng bởi Hacker để tìm thấy lỗ hổng và khai thác chúng. Mặt khác, các quản trị viên cũng sử dụng nó để tìm lỗ hổng bảo mật trên hệ thống của họ để khắc phục ngăn chặn các cuộc tấn công. Sau đây là một số công cụ thường được sử dụng.

Nessus: là một công cụ quét lỗ hổng mã nguồn mở và miễn phí cho đến năm 2005. Sau đó, nó được chuyển đổi thành một sản phẩm thương mại. Nessus hoạt động bằng cách phân tích mạng để tìm lỗ trong mạng. Nó là một công cụ đa nền tảng chạy trên các hệ điều hành như Linux, Mac OS X và Microsoft Windows. Nó sử dụng giao diện đồ họa, thân thiện với người sử dụng.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Các công cụ quét lỗ hổng:

OpenVAS: OpenVAS là một công cụ quét lỗ hổng bảo mật mạnh mẽ được tích hợp trên hệ điều hành Backtrack dành cho các nhà quản trị. Hiện nay OpenVAS đã quét hơn 25.000 lỗ hổng. Công cụ này được tạo ra như một nhánh của Nessus khi Nessus trở nên thương mại hóa.

Core Impact: là một công cụ để khai thác các lỗ hổng hơn là tìm kiếm các lỗ hổng. Nó có khả năng tự động cập nhật những cách khai thác lỗ hổng bảo mật (Exploits), cùng với một đội ngũ các nhà bảo mật chuyên nghiệp viết lên các đoạn Exploit, nó là một sản phẩm thương mại.

Retina: là một công cụ quét lỗ hổng được sử dụng để tra cứu các lỗ hổng trên hệ thống mạng, sử dụng giao diện đồ họa. Nhược điểm của công cụ này là nó chỉ hoạt động trên Microsoft Windows và là một công cụ thương mại.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Công cụ phát hiện tấn công:

Một số công cụ được sử dụng để phát hiện các cuộc tấn công nhưng chúng không thể ngăn chặn các cuộc tấn công. Loại công cụ này được gọi là hệ thống phát hiện xâm nhập Intrusion Detaction System (IDS) và một thể loại cụ thể của IDS chỉ hoạt động ở lớp mạng và được gọi là Network Intrusion Detection System (NIDS). Một số IDS đáng chú ý được liệt kê dưới đây:

Firestorm: Hệ thống pháthiện xâm nhập mạng này có hiệu suất cao và có đầy đủ khả năng để phát hiện các cuộc tấn công khác nhau. Nó có thể phân tích nhiều giao thức để phát hiện bất kỳ các mẫu độc hại trong lưu lượng mạng. Nó sử dụng phương pháp phát hiện bất thường và hỗ trợ đầy đủ quy tắc Snort. Firestorm chạy trên các nền tảng Linux 2.x, FreeBSD 4.x, OpenBSD, và Solaris.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Công cụ phát hiện tấn công:

Prelude: là một IDS lai, trong đó sử dụng các quy tắc Snort và có khả năng sử dụng các quy tắc IDS khác. Nó sử dụng một số cảm biến trong mạng để nắm bắt và phát hiện bất kỳ gói tin độc hại. Nó có thể làm việc trên Linux, BSD, và hệ điều hành khác.

Dragon: là hệ thống phát hiện xâm nhập mạng và máy trạm. Nó là một công cụ thương mại và đi kèm với thư viện phong phú, nó cho phép nó phát hiện một loạt các cuộc tấn công độc hại. Nó có giao diện đồ họa thân thiện với người dùng và cả giao diện dòng lệnh.

Bro: là một hệ thống phát hiện xâm nhập mã nguồn mở và miễn phí trên Unix. Nó làm việc trên lớp mạng và lớp ứng dụng, nó có thể phát hiện các cuộc tấn công ẩn sử dụng lưu lượng được mã hóa hoặc những cố gắng né tránh phân tích và phát hiện.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Các công cụ phòng thủ:

Chúng khác hơn so với IDS, chúng cũng sử dụng các kỹ thuật khác nhau để ngăn chặn các cuộc tấn công. Cơ chế và phương pháp khác nhau được sử dụng để phát hiện các mã độc hại và sau đó ngăn chặn các cuộc tấn công. Một số ví dụ về các hệ thống phòng chống xâm nhập (IPS) được liệt kê dưới đây:

Intrusion Prevention System (IPS): là hệ thống ngăn ngừa xâm nhập, có chức năng theo dõi, ngăn ngừa kịp thời các hoạt động xâm nhập không mong muốn. Chức năng chính của IPS là xác định các hoạt động nguy hại, lưu giữ các thông tin này. Sau đó kết hợp với firewall để dừng ngay các hoạt động này, và cuối cùng đưa ra các báo cáo chi tiết về các hoạt động xâm nhập trái phép trên. Hệ thống IPS được xem là trường hợp mở rộng của hệ thống IDS, cách thức hoạt động cũng như đặc điểm của 2 hệ thống này tương tự nhau. Điểm khác nhau duy nhất là hệ thống IPS ngoài khả năng theo dõi, giám sát thì còn có chức năng ngăn chặn kịp thời các hoạt động nguy hại đối với hệ thống. Hệ thống IPS sử dụng tập luật giống như hệ thống IDS.

Snort: là IDPS nổi tiếng và mạnh mẽ nhất, hoạt động trên lớp mạng và cũng có thể làm việc trên lớp ứng dụng. Nó có thể phát hiện và ngăn chặn các cuộc tấn công khác nhau như lỗi tràn bộ đệm, tấn công từ chối dịch vụ, tàng hình cổng quét, tấn công CGI, thăm dò SMB và các cuộc tấn công khác. Snort là công cụ mã nguồn mở được sử dụng rộng rãi và có nhiều nghiên cứu, phát triển cho nó.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Các công cụ phòng thủ:

Suricata: là một hệ thống phát hiện và phòng chống xâm nhập mã nguồn mở và miễn phí. Nó hoạt động trên lớp ứng dụng để phát hiện và ngăn chặn các cuộc tấn công. Suricata chạy đa luồng làm cho nó nhanh hơn so với IPS và IDS khác. Các kỹ thuật phát hiện sử dụng bởi công cụ này được sử dụng dựa trên nguyên tắc bất thường.

Firewall: là thiết bị phần cứng và/hoặc phần mềm giúp ngăn chặn một số liên lạc bị cấm bởi chính sách an ninh, dựa trên các bộ quy tắc. Một số loại tường lửa có thể hoạt động trên các lớp ứng dụng.

Netfilter: là mã nguồn mở, được viết bằng ngôn ngữ C, và tường lửa miễn phí nhưng chỉ hoạt động trên Linux. Tường lửa này có thể được sử dụng với giao diện dòng lệnh. Nó hỗ trợ các giao thức khác nhau trên IPv4 và bao gồm các mô-đun khác nhau để xử lý các giao thức khác nhau.

IPFilter hoặc "IPF" là một mã nguồn mở và tường lửa miễn phí. Nó hỗ trợ IPv4 và IPv6 và có thể làm việc trên các hệ điều hành như AIX, BSD/OS, DragonFlyBSD, FreeBSD, IRIX, HP-UX, Linux kernel, NetBSD, OpenBSD, OpenSolaris, QNX, Solarix, SunOS, và Tru46.

BIỆN PHÁP PHÒNG CHỐNG TẤN CÔNG

CÔNG CỤ BẢO MẬT TCP/IP

Công cụ kiểm tra:

Đây là những công cụ được sử dụng bởi cả Hacker và các chuyên gia kiểm thử xâm nhập. Sau đây là một số các công cụ kiểm tra thâm nhập quan trọng cho bộ giao thức TCP/IP.

Nmap: là một công cụ quét, theo dõi và đánh giá bảo mật một hệ thống mạng được phát triển bởi Gordon Lyon. Nmap là phần mềm mã nguồn mở miễn phí, ban đầu chỉ được phát triển trên nền tảng Linux sau đó được phát triển trên nhiều nền tảng khác nhau như Windows, Solari, Mac OS... và phát triển thêm phiên bản giao diện người dùng (zenmap).

Netcat: là công cụ nhỏ và dễ sử dụng. Nó giúp thay đổi các gói tin để thử nghiệm các phản ứng giao thức.

hping: là một công cụ mã nguồn mở và miễn phí dùng để phân tích các gói tin TCP/IP. Nó không có một giao diện người dùng đồ họa và chỉ có thể được truy cập bằng cách sử dụng giao diện dòng lệnh. Nó hỗ trợ nhiều giao thức bao gồm ICMP, TCP, UDP và các giao thức RAW-IP.