HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI GIẢNG MÔN

An ninh mạng thông tin

TEL1401

Giảng viên: TS. Phạm Anh Thư

Điện thoại/E-mail: 0912528188

thupa80@yahoo.com, thupaptit@gmail.com

Bộ môn: Mạng viễn thông - KhoaViễn thông 1

Học kỳ/Năm biên soạn: I/ 2022-2023

CHƯƠNG 6 AN TOÀN HỆ THỐNG THÔNG TIN

6.1 Tổng quan an toàn hệ thống thông tin

6.2 Phần mềm độc hại

6.3 Tấn công từ chối dịch vụ DoS

6.4 Phát hiện xâm nhập

6.5 Tường lửa và ngăn chặn xâm nhập

Tổng quan an toàn hệ thống thông tin

- **An ninh máy tính** là thực hiện các biện pháp đảm bảo *tính bảo mật, tính toàn vẹn và tính sẵn sàng* của cơ sở hạ tầng CNTT và thông tin đang được xử lý, lưu trữ và trao đổi qua mạng lưới.
  - Tính bảo mật:
    - Bảo mật thông tin: đảm bảo thông tin cá nhân hoặc thông tin bảo mật không được cung cấp hoặc tiết lộ với những người không được phép.
    - Tính riêng tư: Đảm bảo các cá nhân kiểm soát được những thông tin liên quan đến mình sẽ được thu thập và lưu trữ bởi ai hoặc tiết lộ cho ai.

Tổng quan an toàn hệ thống thông tin

- **An ninh máy tính**
  - Tính toàn vẹn:
    - Toàn vẹn dữ liệu: đảm bảo thông tin và các chương trình chỉ được thay đổi theo cách được cấp phép.
    - Toàn vẹn hệ thống: hệ thống khỏi bị sửa đổi bởi những người không có thẩm quyền; đảm bảo dữ liệu chính xác và đáng tin cậy.
  - Tính sẵn sàng: đảm bảo những người được ủy quyền có thể truy cập thông tin khi cần thiết và tất cả phần cứng và phần mềm được duy trì đúng cách và cập nhật khi cần thiết

Phần mềm độc hại

- Phần mềm độc hại là một trong những mối đe dọa quan trọng nhất đối với hệ thống máy tính.
- Phần mềm độc hại: "Một chương trình được chèn vào hệ thống, thường là một cách bí mật, với mục đích làm tổn hại đến tính bảo mật, tính toàn vẹn hoặc tính khả dụng của dữ liệu, của ứng dụng, của hệ điều hành hoặc gây sự khó chịu, gián đoạn hoạt động của nạn nhân."
- Các phần mềm độc hại này cũng xâm nhập các trang web và các server, trong các email spam hoặc các tin nhắn, nhằm mục đích lừa người dùng tiết lộ thông tin cá nhân nhạy cảm.

Phần mềm độc hại

- Có rất nhiều các phần mềm độc hại: Marcro Virus, Spammer, Spyware, Virus, Worm, Zombie, bot,…
- Phân loại dựa trên hành động:
  - Loại cần có chương trình chủ, kí sinh như Virus;
  - Loại độc lập và có chương trình hoàn thiện như Trojan, Sâu và Bot.
- Đồng thời chúng có thể được phân biệt theo tính nhân bản
  - Không nhân bản như Trojan, Spam E-mail;
  - Nhân bản như Virus và Sâu.

Phần mềm độc hại

- Các hành động mà phần mềm độc hại thực hiện:
  - Phá hủy các tệp tin hệ thống hay tệp dữ liệu.
  - Trộm dịch vụ để khiến hệ thống biến thành một phần tử zombie trong một mạng lưới bot.
  - Trộm thông tin hệ thống như mã khóa, mật khẩu hay các thông tin quan trọng khác bằng phần mềm gián điệp.
  - Ẩn náu để hệ thống không tìm được sự hiện diện và cản nó.
- **Các bộ công cụ tấn công:** sau những năm 2000 thì nhiều bộ dụng cụ cho những cuộc tấn công khác nhau được hoàn thiện. Những bộ công cụ này được gọi là phần mềm tội phạm, chứa một lượng cách xâm nhập và hành động đa dạng, cho phép cả những người nghiệp dư nhất phát triển và triển khai phần mềm độc.

Phần mềm độc hại

- **Nguồn tấn công:**
  - Từ những cá nhân muốn chứng tỏ trình độ của bản thân
  - Từ tội phạm chính trị, tổ chức tội phạm,
  - Các tổ chức muốn bán dịch vụ cho công ty, quốc gia và các cơ quan nhà nước.
  - Nguồn cung như vậy thay đổi nguồn lực cho sự phát triển các phần mềm độc hại dẫn đến sự phát triển một nguồn kinh tế ngầm liên quan đến việc buôn bán các bộ công cụ tấn công, quyền truy cập các máy chủ đã bị xâm nhập và các thông tin bị ăn trộm.

Phần mềm độc hại

- **Nhiễm độc nội dung - Virus:**
  - Virus có thể là một đoạn mã máy sẽ lây nhiễm cho các ứng dụng đang tồn tại, phần mềm tiện ích, chương trình hệ thống, hoặc một đoạn mã dùng để khởi động máy tính.
  - Virus máy tính là một loại mã độc hại có khả năng tự nhân bản và lây nhiễm chính nó vào các file, chương trình hoặc máy tính.
  - Virus phải luôn bám vào vật chủ (có thể là file dữ liệu hoặc file ứng dụng) để lây lan.
  - Virus nhiễm độc sang các chương trình khác hay bất cứ nội dung nào bằng cách biến đổi chúng. Việc biến đổi có thể tiêm vào đoạn mã gốc một hành động sao chép đoạn code virus, thứ mà có thể tiếp tục đi lây nhiễm.

Phần mềm độc hại

- **Nhiễm độc nội dung - Virus:**
  - Cấu tạo của một con virus gồm 3 phần:
    - Cơ chế lây nhiễm: Cách virus lan truyền để nhân bản.
    - Điều kiện kích hoạt: Điều kiện hay hành động cần xảy ra để con virus hoạt động. Đây gọi là bom logic.
    - Payload: Hành động của con virus ngoại trừ phát tán. Payload có thể gây hại nhưng cũng có thể gồm những hành động vô hại dễ nhận thấy.

Phần mềm độc hại

- **Nhiễm độc nội dung - Virus:**
- Trong vòng đời, một con virus sẽ trải qua 4 giai đoạn:
  - Giai đoạn nằm im: virus không làm gì cho đến khi được kích hoạt bởi một ai hay một sự kiện nào đó. Không phải virus nào cũng trải qua giai đoạn này.
  - Giai đoạn lan truyền: Virus gắn một bản sao của nó vào chương trình khác hoặc phần mềm hệ thống. Bản sao của nó không nhất thiết phải giống y hệt vì virus phải biến đổi để tránh khỏi bị phát hiện.
  - Giải đoạn kích hoạt: virus được kích hoạt để thực thi chức năng của nó. Giống như giai đoạn nằm im, giai đoạn kích hoạt là kết quả của nhiều sự kiện của hệ thống bao gồm tổng số lượng bản sao của virus đã nhân bản.
  - Giai đoạn thực hiện: Hành động được thực hiện. Hành động có thể vô hại như hiện tin nhắn lên màn hình hoặc gây hại như phá hủy chương trình hoặc tệp tin.

Phần mềm độc hại

- **Sâu-worm:**
  - Là phần mềm độc lan truyền bằng cách lợi dụng điểm yếu của phần mềm.
  - Là phần mềm có khả năng chủ động tìm thiết bị để lây nhiễm và mỗi thiết bị đã lây nhiễm trở thành bàn đạp để tấn công các thiết bị khác.
  - Sâu tận dụng điểm yếu của người dùng hoặc chương trình máy chủ để tiếp cận hệ thống mới. Nó có thể dùng kết nối mạng để lan truyền từ hệ thống này sang hệ thống khác. Nó cũng có thể lan truyền qua các kênh như ổ USB, đĩa CD, DVD,…
  - Sâu email có thể lan truyền trong macro hoặc script gắn tài liệu đính kèm email. Sau khi kích hoạt sâu sẽ nhân bản và tiếp tục phát tán.

Tấn công từ chối dịch vụ DoS

- Từ chối dịch vụ là một dạng tấn công vào tính khả dụng của dịch vụ
- DoS là một hành động ngăn cản hoặc làm suy yếu việc sử dụng hợp pháp các hệ thống, các mạng, hoặc các ứng dụng bằng cách làm cạn kiệt tài nguyên như CPU, bộ nhớ, băng tần, và ổ đĩa.
- Các tài nguyên có thể bị tấn công:
  - Băng thông mạng: liên quan tới khả năng của các liên kết mạng kết nối máy chủ tới mạng Internet
  - Tài nguyên hệ thống: làm quá tải hoặc làm hỏng phần mềm xử lý mạng. Các gói tin được gửi đi tiêu thụ tài nguyên hạn chế có sẵn trên hệ thống.
  - Tài nguyên ứng dụng: Tấn công vào một ứng dụng cụ thể, như máy chủ Web, thường liên quan đến một số yêu cầu hợp lệ, mỗi yêu cầu trong số đó tiêu thụ tài nguyên đáng kể.

Tấn công từ chối dịch vụ DoS

- **Tấn công từ chối dịch vụ cổ điển:**
  - Là tấn công tràn lụt vào một tổ chức: gây quá tải dung lượng của kết nối mạng đến tổ chức mục tiêu.
  - Cuộc tấn công có thể đơn giản như sử dụng một lệnh ping tràn lụt được hướng đến máy chủ Web trong công ty mục tiêu
  - Nguồn gốc của cuộc tấn công được xác định rõ ràng vì địa chỉ của nó được sử dụng làm địa chỉ nguồn trong các gói tin yêu cầu ICMP echo
    - nguồn gốc của cuộc tấn công được xác định rõ ràng, tăng cơ hội xác định được kẻ tấn công và họ sẽ bị xử lý bởi pháp luật.
    - hệ thống mục tiêu sẽ cố gắng phản hồi cho các gói được gửi đến => gây ra cuộc tấn công ngược trở lại hệ thống nguồn

Tấn công từ chối dịch vụ DoS

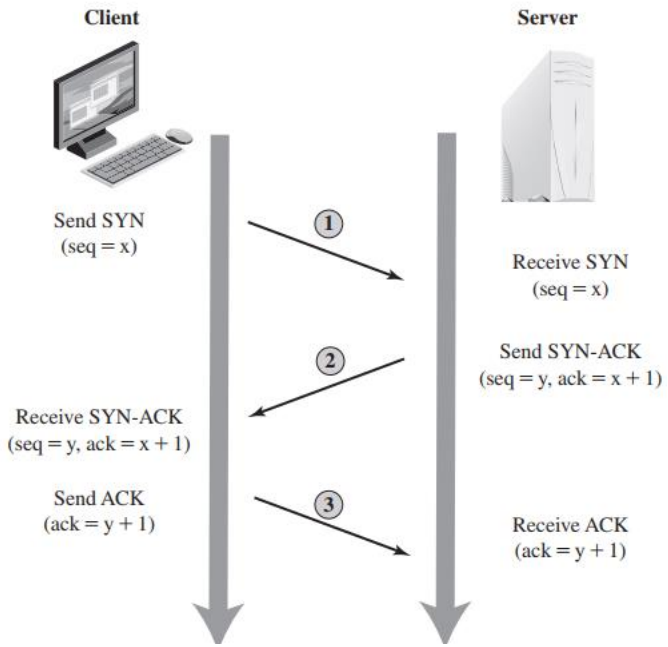
- **Tấn công giả mạo địa chỉ nguồn:**
  - Sử dụng các địa chỉ nguồn giả mạo.
  - Kẻ tấn công có thể tạo ra khối lượng lớn các gói tin. Tất cả các gói tin này có hệ thống đích là địa chỉ đích nhưng sẽ sử dụng các địa chỉ nguồn được chọn ngẫu nhiên, thường là khác nhau, cho mỗi gói
    - Tắc nghẽn tương tự sẽ xảy ra trong bộ định tuyến được kết nối với liên kết dung lượng thấp hơn.
    - Các gói phản hồi ICMP echo sẽ không còn được phản hồi trở lại hệ thống nguồn
    - Bất kỳ gói phản hồi nào được trả về chỉ làm tăng thêm tràn lụt lưu lượng hướng vào hệ thống mục tiêu
  - Khó xác định hệ thống tấn công. Kiểm tra tiêu đề của mỗi gói không đủ để xác định nguồn của nó.
  - Cần phải xác định luồng các gói tin thông qua các bộ định tuyến dọc theo đường truyền dẫn từ nguồn đến hệ thống đích.

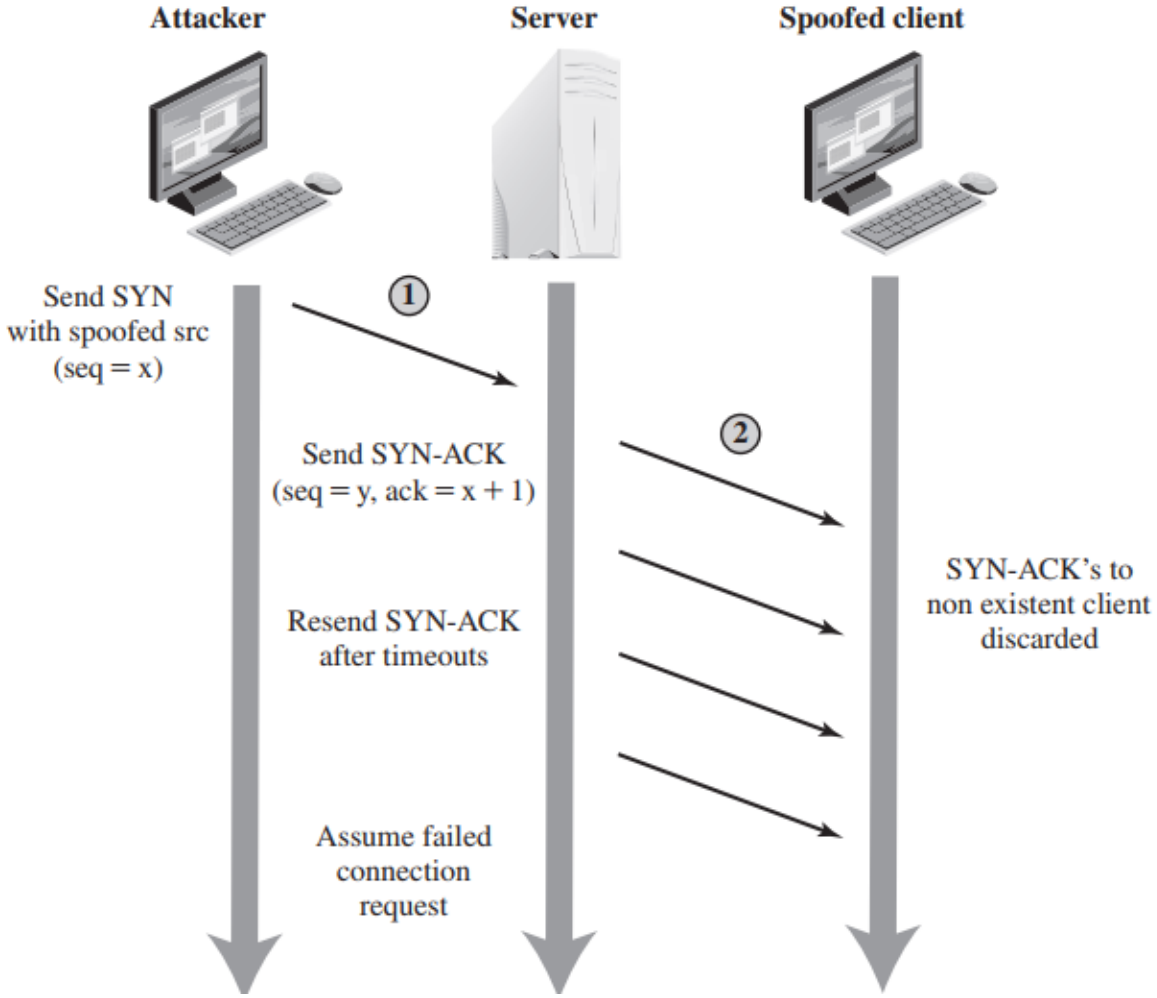
Tấn công từ chối dịch vụ DoS

- **Tấn công giả mạo SYN :**
  - Gửi liên tục các gói tin yêu cầu kết nối TCP ban đầu (SYN), kẻ tấn công làm tràn ngập tất cả các cổng có sẵn trên Server mục tiêu, khiến server mục tiêu đáp ứng lưu lượng hợp pháp một cách rất chậm chạp hoặc không đáp ứng kịp thời.
  - Kẻ tấn công tạo ra một số gói tin yêu cầu kết nối SYN với các địa chỉ nguồn giả mạo.
    - máy chủ ghi lại các chi tiết của kết nối TCP yêu cầu và gửi gói SYN-ACK đến địa chỉ nguồn.
    - Nếu có một hệ thống hợp lệ tại địa chỉ nguồn này, nó sẽ phản hồi bằng một gói tin với cờ RST được thiết lập để hủy bỏ yêu cầu kết nối không xác định này.

Tấn công từ chối dịch vụ DoS

- **Tấn công giả mạo SYN :**





Tấn công từ chối dịch vụ DoS

- **Tấn công tràn ngập:**
  - Mục đích chung là làm quá tải dung lượng mạng trên một số liên kết đến máy chủ, hay làm quá tải khả năng xử lý và phản hồi của máy chủ đối với lưu lượng truy cập này.
  - Những cuộc tấn công này làm tràn lụt liên kết mạng tới máy chủ với một loạt các gói dữ liệu độc hại áp đảo lưu lượng truy cập hợp lệ đến máy chủ.
  - Để đối phó với sự tắc nghẽn, xảy ra trong một số bộ định tuyến trên đường truyền đến máy chủ mục tiêu, nhiều gói tin sẽ bị loại bỏ.
  - Do đó, lưu lượng truy cập hợp lệ có xác suất tồn tại thấp. Điều này dẫn đến khả năng máy chủ phản hồi các yêu cầu kết nối mạng bị suy giảm nghiêm trọng hoặc bị lỗi hoàn toàn.
  - Bất kỳ loại gói tin nào cũng có thể được sử dụng trong một cuộc tấn công tràn ngập: gói ICMP, UDP hoặc TCP SYN

Tấn công từ chối dịch vụ DoS

- **Tràn ngập ICMP:**
  - Sử dụng gói tin yêu cầu ICMP echo.
  - Loại gói ICMP này được chọn do các quản trị viên mạng cho phép các gói tin này đi vào mạng của họ, vì ping là một công cụ chẩn đoán mạng hữu ích
  - Gần đây, nhiều tổ chức đã hạn chế khả năng vượt qua tường lửa của các gói tin này. Đáp lại, những kẻ tấn công bắt đầu sử dụng các loại gói ICMP khác.
  - Một số gói tin IMCP được sử dụng để khắc phục lỗi của hệ thống mạng TCP/IP, nên các gói tin ICMP này có nhiều khả năng được cho phép thông qua tường lửa của các tổ chức hơn.
  - Việc lọc một số loại gói ICMP quan trọng sẽ làm suy giảm hoặc phá vỡ hành vi mạng TCP/IP bình thường, ví dụ có thể làm cho các gói tin ICMP không đến được đích hoặc các gói vượt quá thời gian truyền.

Tấn công từ chối dịch vụ DoS

- **Tràn ngập UDP:**
  - Một giải pháp thay thế cho việc sử dụng các gói ICMP là sử dụng các gói UDP hướng đến một cổng nào đó và do đó đây là giải pháp tiềm năng để làm tràn ngập hệ thống mục tiêu với một lượng lớn dữ liệu đến.
  - Một cuộc tấn công gây tràn ngập UDP có thể được bắt đầu bằng cách gửi một số lượng lớn các gói tin UDP tới cổng ngẫu nhiên trên một máy chủ từ xa và kết quả là các máy chủ sẽ kiểm tra các ứng dụng tương ứng với cổng.
    - Nếu máy chủ thấy rằng không có ứng dụng đang lắng nghe ở cổng đó thì nó sẽ trả lời với một bản tin ICMP không thể đến đích được.
    - Khi số lượng yêu cầu vượt ngưỡng sẽ dẫn đến mất khả năng xử lý các yêu cầu của khách hàng thông thường dẫn đến tình trạng từ chối dịch vụ.
    - Đến lúc đó cuộc tấn công đã đạt được mục tiêu là chiếm dung lượng trên liên kết tới máy chủ.

Tấn công từ chối dịch vụ DoS

- **Tràn ngập TCP SYN:**
  - Gửi các gói TCP tới hệ thống đích, các gói tin này có địa chỉ nguồn là thật hoặc giả mạo.
  - Chúng sẽ có tác động tương tự như cuộc tấn công giả mạo SYN như đã đề cập đến ở trên.
  - Tuy nhiên, trong trường hợp này, tổng khối lượng các gói là mục đích của tấn công.

Tấn công từ chối dịch vụ DoS

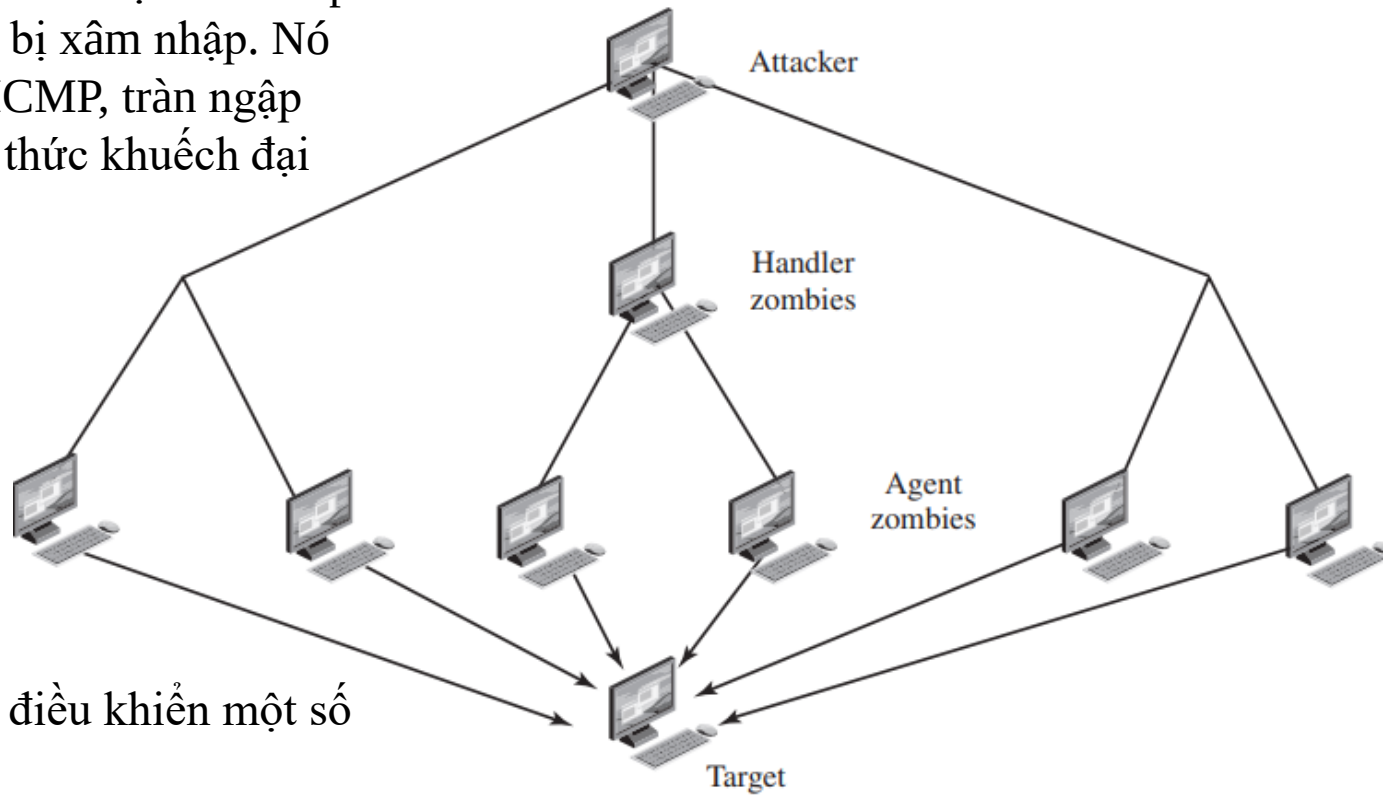
- **Tấn công từ chối dịch vụ phân tán DDOS:**
  - Sử dụng nhiều hệ thống, máy trạm hoặc PC của người dùng bị xâm phạm, để tạo ra các cuộc tấn công
  - Kẻ tấn công sử dụng phần mềm độc hại để phá hoại hệ thống và cài đặt Agent tấn công mà chúng có thể kiểm soát (zombie)
  - Một tập lớn các hệ thống như vậy dưới sự kiểm soát của một kẻ tấn công có thể được tạo ra, tạo thành một mạng botnet

Tấn công từ chối dịch vụ DoS

- **Tấn công từ chối dịch vụ phân tán DDOS:**

Kiến trúc tấn công DDoS

Agent là một chương trình Trojan đã được sao chép và chạy trên các hệ thống zombie bị xâm nhập. Nó có khả năng triển khai tràn ngập ICMP, tràn ngập SYN, tràn ngập UDP và các hình thức khuếch đại ICMP của các cuộc tấn công DoS



Trình xử lý (handler) thực hiện điều khiển một số lượng lớn hệ thống Agent

Tấn công từ chối dịch vụ DoS

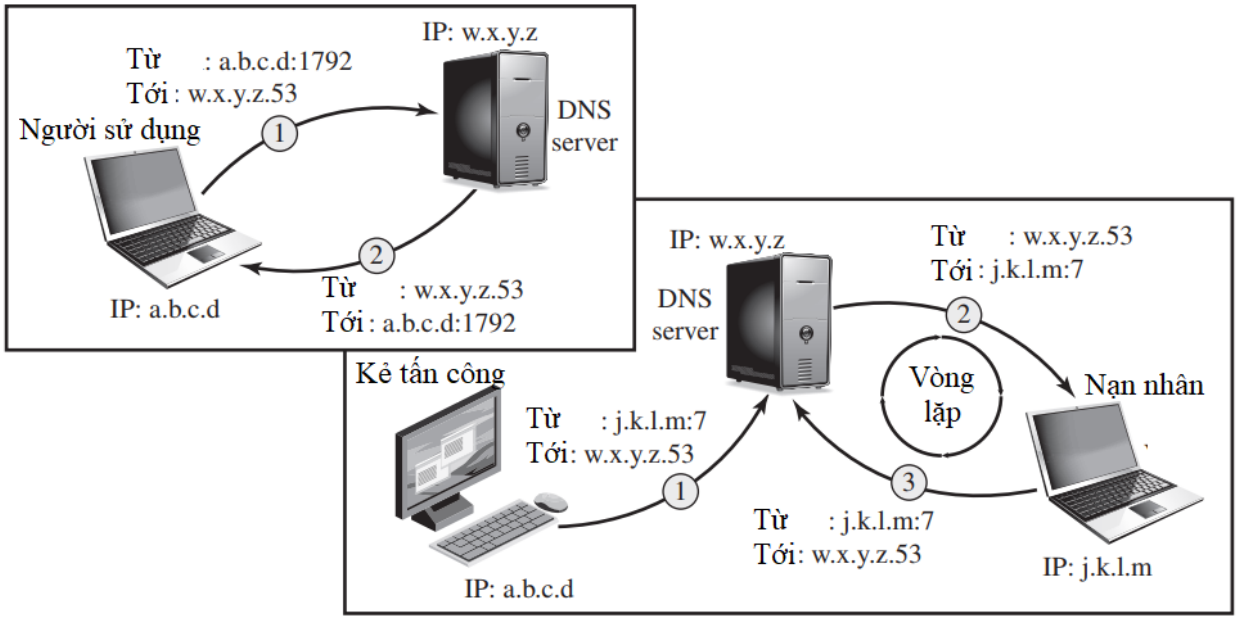
- **Tấn công băng thông dựa trên ứng dụng:**
  - Các cuộc tấn công băng thông dựa trên ứng dụng cố gắng tận dụng việc tiêu thụ tài nguyên lớn không cân xứng tại một máy chủ
  - **Tràn ngập SIP:** khai thác thực tế rằng một yêu cầu SIP INVITE duy nhất kích hoạt mức tiêu thụ tài nguyên đáng kể
  - **Tấn công dựa trên HTTP:** tràn ngập HTTP và Slowloris.
    - Tràn ngập HTTP đề cập đến một kiểu tấn công bắn phá các máy chủ Web bằng các yêu cầu HTTP. Thông thường, đây là một cuộc tấn công DDoS, với các yêu cầu HTTP đến từ nhiều bot khác nhau.
    - Slowloris là một chương trình tấn công từ chối dịch vụ cho phép kẻ tấn công áp đảo máy chủ mục tiêu bằng cách mở và duy trì nhiều kết nối HTTP đồng thời giữa kẻ tấn công và mục tiêu.

Tấn công từ chối dịch vụ DoS

- **Tấn công phản xạ và khuếch đại:**
  - Ngược lại với DDoS, bên trung gian là các hệ thống bị xâm nhập đang chạy các chương trình của kẻ tấn công, các cuộc tấn công phản xạ và khuếch đại sử dụng hệ thống mạng hoạt động bình thường.
  - Kẻ tấn công gửi một gói tin có địa chỉ nguồn giả mạo đến một dịch vụ đang chạy trên một máy chủ. Máy chủ sau đó phản hồi gói tin này bằng cách gửi bản tin phản hồi đến địa chỉ nguồn giả mạo thuộc về mục tiêu tấn công thực sự.
  - Nếu kẻ tấn công gửi một số yêu cầu đến một số máy chủ, tất cả đều có cùng một địa chỉ nguồn giả mạo, kết quả là tràn ngập các bản tin phản hồi và gây ra tràn ngập liên kết mạng mục tiêu.
  - Thực tế là các hệ thống máy chủ bình thường đang được sử dụng làm trung gian và việc xử lý các gói tin của chúng hoàn toàn thông thường, có nghĩa là các cuộc tấn công này có thể dễ triển khai hơn và khó truy tìm lại kẻ tấn công thực sự hơn.

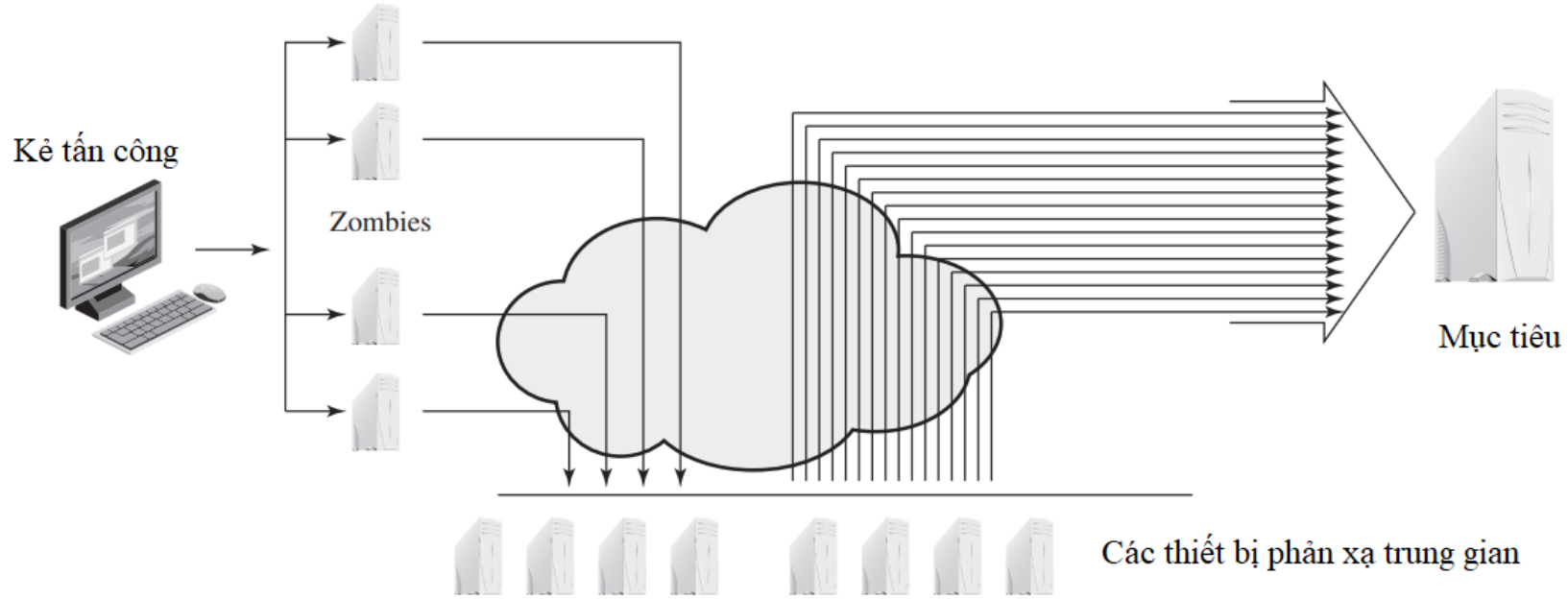
Tấn công từ chối dịch vụ DoS

- **Tấn công phản xạ và khuếch đại:**
  - **Tấn công phản xạ:** Kẻ tấn công gửi các gói tin đến một dịch vụ đã biết tại hệ thống trung gian với địa chỉ nguồn giả mạo là địa chỉ của hệ thống mục tiêu thực tế. Khi hệ thống trung gian phản hồi, phản hồi sẽ được gửi đến hệ thống mục tiêu. Về mặt hiệu quả, điều này phản ánh cuộc tấn công từ bên trung gian, được gọi là phản xạ.



Tấn công từ chối dịch vụ DoS

- **Tấn công phản xạ và khuếch đại:**
  - **Tấn công khuếch đại:** Các cuộc tấn công khuếch đại là một biến thể của các cuộc tấn công phản xạ và cũng liên quan đến việc gửi một gói tin có địa chỉ nguồn giả mạo là địa chỉ của hệ thống đích đến các hệ thống trung gian. Hai kiểu tấn công này khác nhau ở việc tạo ra nhiều gói phản hồi cho mỗi gói ban đầu được gửi đi.



Tấn công từ chối dịch vụ DoS

- **Bảo vệ chống lại tấn công DoS:**
  - Phòng ngừa và ngăn chặn tấn công (trước cuộc tấn công): thực thi các chính sách tiêu thụ tài nguyên và cung cấp các tài nguyên dự phòng có sẵn theo yêu cầu.
  - Lọc và Phát hiện cuộc tấn công (trong cuộc tấn công): cố gắng phát hiện cuộc tấn công khi nó bắt đầu và phản hồi ngay lập tức
  - Nhận dạng và truy xuất nguồn tấn công (trong và sau cuộc tấn công): nỗ lực để xác định nguồn gốc của cuộc tấn công
  - Phản ứng tấn công (sau cuộc tấn công): Đây là một nỗ lực để loại bỏ hoặc giảm bớt tác động của một cuộc tấn công.

Phát hiện xâm nhập

- Xâm nhập mạng là những hoạt động có chủ đích, lợi dụng các tổn thương của hệ thống thông tin nhằm phá vỡ tính sẵn sàng, tính toàn vẹn và tính bảo mật của hệ thống.
- Xâm nhập còn được hiểu là hành động trái phép vượt qua các cơ chế bảo mật của một hệ thống.
- Có rất nhiều kiểu xâm nhập mạng khác nhau và thường được phân thành các loại chính: tấn công từ chối dịch vụ, kiểu thăm dò, tấn công chiếm quyền "root", tấn công điều khiển từ xa.
- Ví dụ xâm nhập như đoán và bẻ khóa, sao chép dữ liệu, xem trộm dữ liệu mật, đăng nhập mà không được phép

Phát hiện xâm nhập

Có một số loại kẻ xâm nhập sau:

- Tội phạm mạng: Là các cá nhân hoặc thành viên của một nhóm tội phạm có tổ chức có mục tiêu là phần thưởng tài chính
- Kẻ hoạt động xã hội: Là những cá nhân hoặc thành viên của một nhóm lớn hơn những kẻ tấn công bên ngoài, họ được thúc đẩy bởi các nguyên nhân xã hội hoặc chính trị.
- Các tổ chức do nhà nước bảo trợ: Là các nhóm tin tặc được các chính phủ bảo trợ để tiến hành các hoạt động gián điệp hoặc phá hoại
- Các loại khác: Là những tin tặc có động cơ khác với những động cơ được liệt kê ở trên, bao gồm những tin tặc cổ điển hoặc những kẻ bẻ khóa được thúc đẩy bởi thách thức kỹ thuật hoặc bởi lòng tôn trọng và danh tiếng của nhóm cộng đồng

Phát hiện xâm nhập

Phát hiện xâm nhập:

- Là một chức năng phần cứng hoặc phần mềm thu thập và phân tích thông tin từ các khu vực khác nhau trong máy tính hoặc mạng để xác định các hành vi xâm nhập an ninh có thể xảy ra.
- Hệ thống phát hiện xâm nhập IDS là hệ thống phát hiện các dấu hiệu của tấn công xâm nhập, đồng thời có thể khởi tạo các hành động trên thiết bị khác để ngăn chặn tấn công.
- IDS không thực hiện các thao tác ngăn chặn truy nhập mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo cho người quản trị mạng.

Phát hiện xâm nhập

Một hệ thống IDS bao gồm ba thành phần logic chính:

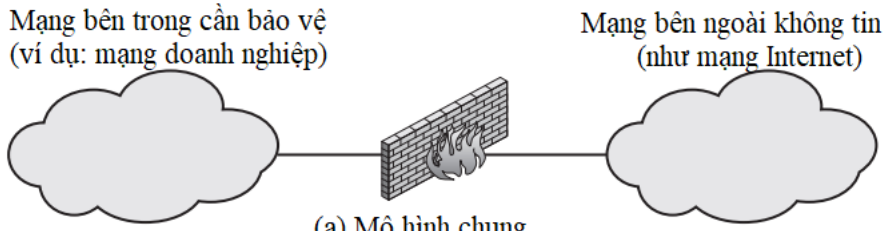
- **Bộ cảm biến (Sensor):** có nhiệm vụ thu thập dữ liệu. Đầu vào của bộ cảm biến có thể là bất kỳ phần nào của hệ thống có thể chứa bằng chứng về sự xâm nhập.
- **Bộ phân tích:** bộ phân tích nhận đầu vào từ một hoặc nhiều bộ cảm biến hoặc từ bộ phân tích khác. Bộ phân tích có trách nhiệm xác định xem có sự xâm nhập xảy ra hay không.
- **Giao diện người dùng:** Giao diện người dùng tới hệ thống IDS cho phép người dùng xem đầu ra từ hệ thống hoặc điều khiển hành vi của hệ thống.

Tường lửa và ngăn chặn xâm nhập

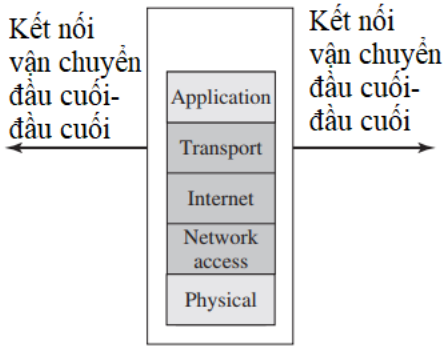
- Tường lửa có thể là biện pháp hiệu quả để bảo vệ hệ thống nội bộ hoặc mạng các hệ thống khỏi các nguy cơ an ninh trong khi vẫn cung cấp quyền truy cập vào thế giới bên ngoài thông qua mạng diện rộng và Internet.
- Tường lửa được đặt giữa mạng nội bộ và Internet để thiết lập một liên kết được kiểm soát và để dựng lên một bức tường hoặc vành đai an ninh bên ngoài.
- Mục đích của bức tường này là bảo vệ mạng nội bộ khỏi các cuộc tấn công trên Internet.
- Tường lửa có thể là một hệ thống máy tính đơn lẻ hoặc một tập hợp của hai hoặc nhiều hệ thống hợp tác để thực hiện chức năng tường lửa.
- Tường lửa cung cấp một lớp bảo vệ bổ sung, cách ly các hệ thống bên trong khỏi các mạng bên ngoài.

Tường lửa và ngăn chặn xâm nhập

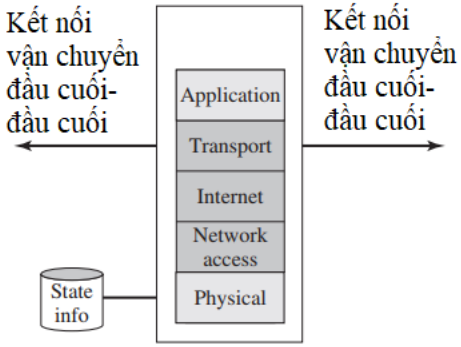
Một số loại tường lửa cơ bản



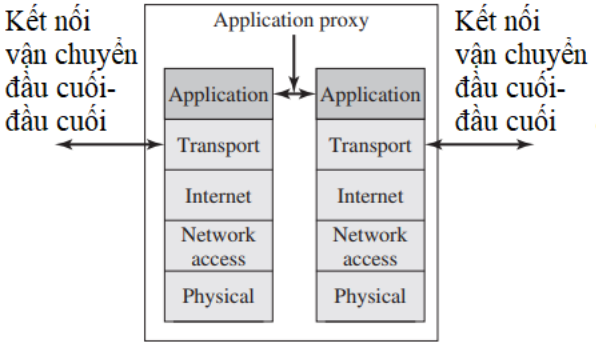
(a) Mô hình chung



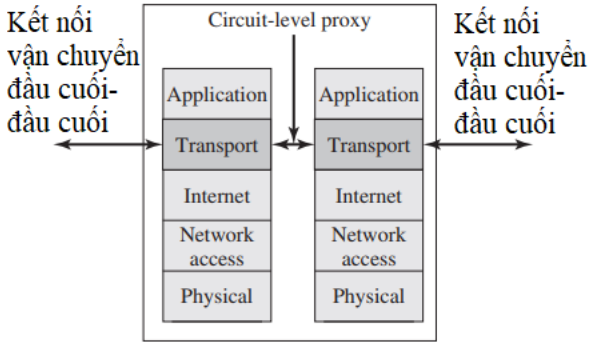
(b) Tường lửa lọc gói



(c) Tường lửa kiểm soát trạng thái



(d) Tường lửa proxy ứng dụng



(e) Tường lửa proxy mức kênh

Tường lửa và ngăn chặn xâm nhập

Vị trí và cấu hình tường lửa