1. Tấn công từ chối dịch vụ và từ chối dịch vụ phân tán

1.1 Tấn công từ chối dịch vụ

1.1.1 Giới thiệu

Tấn công từ chối dịch vụ (Denial of Service - DoS) là dạng tấn công nhằm ngăn chặn người dùng hợp pháp truy nhập các tài nguyên mạng. Tấn công DoS có thể được chia thành 2 loại: (1) tấn công logic (Logic attacks) và (2) tấn công gây ngập lụt (Flooding attacks). Tấn công logic là dạng tấn công khai thác các lỗi phần mềm làm dịch vụ ngừng hoạt động, hoặc làm giảm hiệu năng hệ thống. Tấn công DoS sử dụng sâu Slammer đề cập ở Mục 2.3.2.2 là dạng tấn công khai thác lỗi tràn bộ đệm trong phần mềm. Ngược lại, trong tấn công gây ngập lụt, kẻ tấn công gửi một lượng lớn yêu cầu gây cạn kiệt tài nguyên hệ thống hoặc băng thông đường truyền mạng.

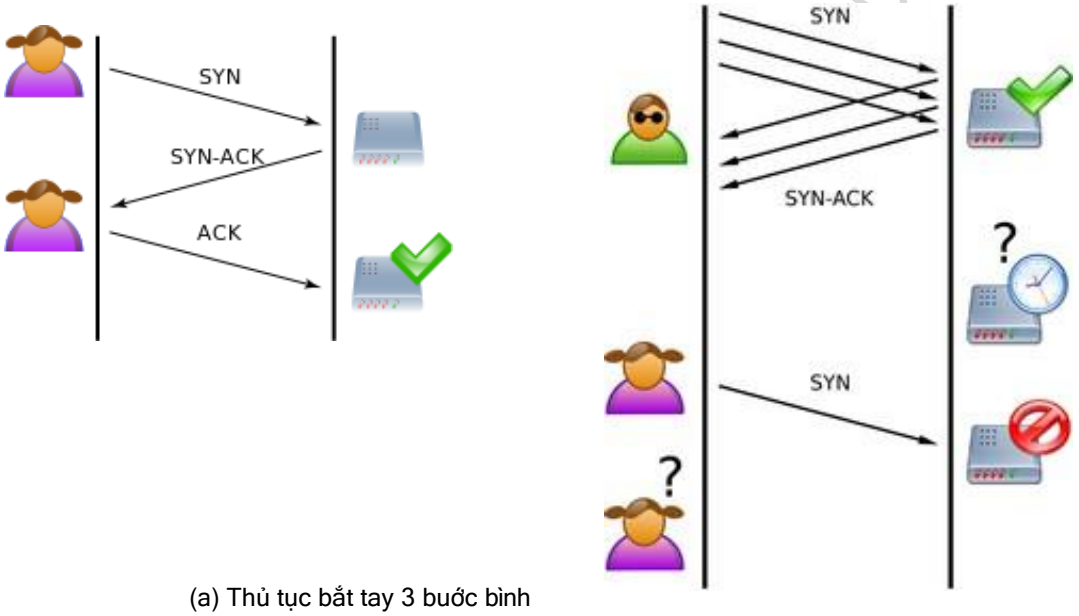
Có nhiều kỹ thuật tấn công DoS đã được phát hiện trên thực tế. Các kỹ thuật tấn công DoS thường gặp bao gồm: SYN Flood, Smurf, Teardrop, Ping of Death, Land Attacks, ICMP Flood, HTTP Flood, UDP Flood,… Trong phạm vi của môn học này, chúng ta chỉ đề cập đến 2 kỹ thuật phổ biến nhất là SYN Flood và Smurf.

1.1.2 Tấn công SYN flood

** Giới thiệu*

Tấn công SYN Flood là kỹ thuật tấn công DoS khai thác điểm yếu trong thủ tục bắt tay 3 bước (3-way handshake) khi hai bên tham gia truyền thông thiết lập kết nối TCP để bắt đầu phiên trao đổi dữ liệu. SYN là bit cờ điều khiển của giao thức TCP dùng để đồng bộ số trình tự gói tin. Thủ tục bắt tay khi một người dùng hợp pháp thiết lập một kết nối TCP đến máy chủ, như minh họa trên hình Hình 2.21 (a) gồm 3 bước như sau:

- Người dùng thông qua máy khách gửi yêu cầu mở kết nối (SYN hay SYN-REQ) đến máy chủ;
- Máy chủ nhận được lưu yêu cầu kết nối vào Bảng kết nối (Backlog) và gửi lại xác nhận kết nối SYN-ACK cho máy khách;
- Khi nhận được SYN-ACK từ máy chủ, máy khách gửi lại xác nhận kết nối ACK đến máy chủ. Khi máy chủ nhận được xác nhận kết nối ACK từ máy khách, nó xác nhận kết nối mở thành công, máy chủ và máy khách bắt đầu phiên truyền thông TCP. Bản ghi mở kết nối được xóa khỏi Bảng kết nối.



(a) Thủ tục bắt tay 3 bước bình thường của giao thức TCP

(b) Tấn công SYN Flood

Hình 2.21. (a) Thủ tục bắt tay 3 bước của TCP và (b) Tấn công SYN Flood

** Kịch bản tấn công*

Kịch bản tấn công SYN Flood, như minh họa trên Hình 2.21 (b) gồm các bước sau:

- Kẻ tấn công gửi một lượng lớn yêu cầu mở kết nối (SYN-REQ) đến máy nạn nhân;
- Nhận được yêu cầu mở kết nối, máy nạn nhân lưu yêu cầu kết nối vào Bảng kết nối trong bộ nhớ;
- Máy nạn nhân sau đó gửi xác nhận kết nối (SYN-ACK) đến kẻ tấn công;
- Do kẻ tấn công không gửi lại xác nhận kết nối ACK, nên máy nạn nhân vẫn phải lưu tất cả các yêu cầu kết nối chưa được xác nhận trong Bảng kết nối. Khi Bảng kết nối bị điền đầy thì các yêu cầu mở kết nối của người dùng hợp pháp sẽ bị từ chối;
- Máy nạn nhân chỉ có thể xóa một yêu cầu kết nối đang mở khi nó hết hạn (timed- out).

Do kẻ tấn công thường sử dụng địa chỉ IP giả mạo, hoặc địa chỉ không có thực làm địa chỉ nguồn (Source IP) trong gói tin IP yêu cầu mở kết nối, nên xác nhận kết nối SYN- ACK của máy nạn nhân không thể đến đích. Đồng thời, kẻ tấn công cố tình tạo một lượng rất lớn yêu cầu mở kết nối dở dang để chúng điền đầy bảng kết nối. Hậu quả là máy nạn nhân không thể chấp nhận yêu cầu mở kết nối của những người dùng khác. Tấn công SYN Flood làm cạn kiệt tài nguyên bộ nhớ (cụ thể là bộ nhớ Bảng kết nối) của máy nạn nhân, có thể làm máy nạn nhân ngừng hoạt động và gây nghẽn đường truyền mạng.

** Phòng chống*

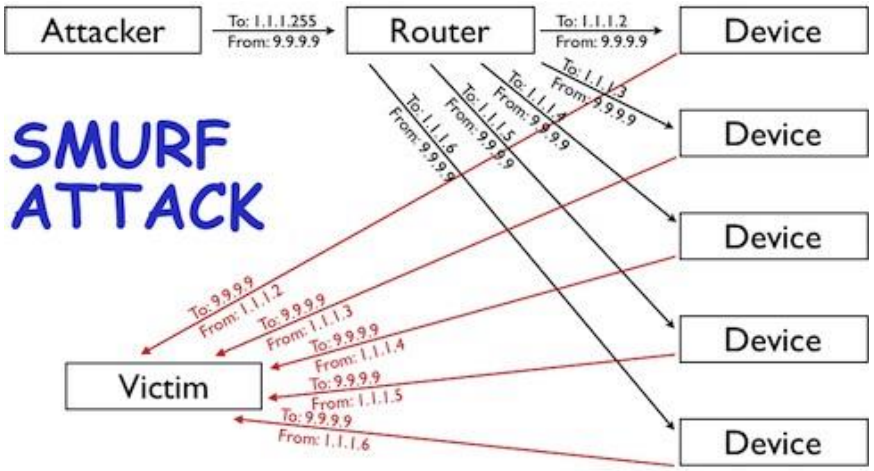
Nhiều biện pháp phòng chống tấn công SYN Flood được đề xuất, nhưng chưa có giải pháp nào có khả năng ngăn chặn triệt để dạng tấn công này. Do vậy, để phòng chống tấn công SYN Flood hiệu quả, cần kết hợp các biện pháp sau:

- Sử dụng kỹ thuật lọc địa chỉ giả mạo (Spoofed IP Filtering): Kỹ thuật này đòi hỏi chỉnh sửa giao thức TCP/IP không cho phép kẻ tấn công giả mạo địa chỉ;
- Tăng kích thước Bảng kết nối: Tăng kích thước Bảng kết nối cho phép tăng khả năng chấp nhận các yêu cầu mở kết nối;
- Giảm thời gian chờ (SYN-RECEIVED Timer): Các yêu cầu mở kết nối chưa được xác nhận sẽ bị xóa sớm hơn khi thời gian chờ ngắn hơn;
- SYN cache: Một yêu cầu mở kết nối chỉ được cấp phát không gian nhớ đầy đủ khi nó được xác nhận;
- Sử dụng tường lửa (Firewall) và Proxy: Tường lửa và proxy có khả năng nhận dạng các địa chỉ IP nguồn là địa chỉ không có thực, đồng thời chúng có khả năng tiếp nhận yêu cầu mở kết nối, chờ đến khi có xác nhận mới chuyển cho máy chủ đích.

1.1.3 Tấn công Smurf

** Giới thiệu*

Tấn công Smurf là dạng tấn công DoS sử dụng giao thức điều khiển truyền ICMP và kiểu phát quảng bá có định hướng để gây ngập lụt đường truyền mạng của máy nạn nhân. Trên mỗi phân vùng mạng IP thường có 1 địa chỉ quảng bá, theo đó khi có một gói tin gửi tới địa chỉ này, nó sẽ được router của mạng chuyển đến tất cả các máy trong mạng đó.



Hình 2.22. Mô hình tấn công Smurf

** Kịch bản tấn công*

Hình 2.22 minh họa mô hình tấn công DoS Smurf. Theo đó, kịch bản tấn công Smurf gồm các bước:

- Kẻ tấn công gửi một lượng lớn gói tin chứa yêu cầu ICMP (Ping) với địa chỉ IP nguồn là địa chỉ của máy nạn nhân đến một địa chỉ quảng bá (IP Broadcast address) của một mạng;
- Router của mạng nhận được yêu cầu ICMP gửi đến địa chỉ quảng bá sẽ tự động chuyển yêu cầu này đến tất cả các máy trong mạng;
- Các máy trong mạng nhận được yêu cầu ICMP sẽ gửi trả lời (reply) đến máy có địa chỉ IP là địa nguồn trong yêu cầu ICMP (là máy nạn nhân). Nếu số lượng máy trong mạng rất lớn thì máy nạn nhân sẽ bị ngập lụt đường truyền, hoặc ngừng hoạt động.

** Phòng chống*

Có thể sử dụng các biện pháp sau để phòng chống tấn công Smurf:

- Cấu hình các máy trong mạng và router không trả lời các yêu cầu ICMP, hoặc các yêu cầu phát quảng bá;
- Cấu hình các router không chuyển tiếp yêu cầu ICMP gửi đến các địa chỉ quảng bá;
- Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo địa chỉ trong mạng.

Việc cấu hình các router không chuyển tiếp yêu cầu ICMP, hoặc các máy trong mạng không trả lời các yêu cầu ICMP có thể gây khó khăn cho các ứng dụng dựa trên phát quảng bá và giao thức ICMP, như ứng dụng giám sát trạng thái hoạt động của các máy trong mạng dựa trên ICMP/Ping.

1.2 Tấn công từ chối dịch vụ phân tán

1.2.1 Giới thiệu

Tấn công DDoS (Distributed Denial of Service) là một loại tấn công DoS đặc biệt, liên quan đến việc gây ngập lụt các máy nạn nhân với một lượng rất lớn các yêu cầu kết nối giả mạo. Điểm khác biệt chính giữa DDoS và DoS là phạm vi (scope) tấn công: trong khi số lượng máy tham gia tấn công DoS thường tương đối nhỏ, chỉ gồm một số ít máy tại một, hoặc một số ít địa điểm, thì số lượng máy tham gia tấn công DDoS thường rất lớn, có thể lên đến hàng ngàn, hoặc hàng trăm ngàn máy, và các máy tham gia tấn công DDoS có thể đến từ rất nhiều vị trí địa lý khác nhau trên toàn cầu. Do vậy, việc phòng chống tấn công DDoS gặp nhiều khó khăn hơn so với việc phòng chống tấn công DoS.

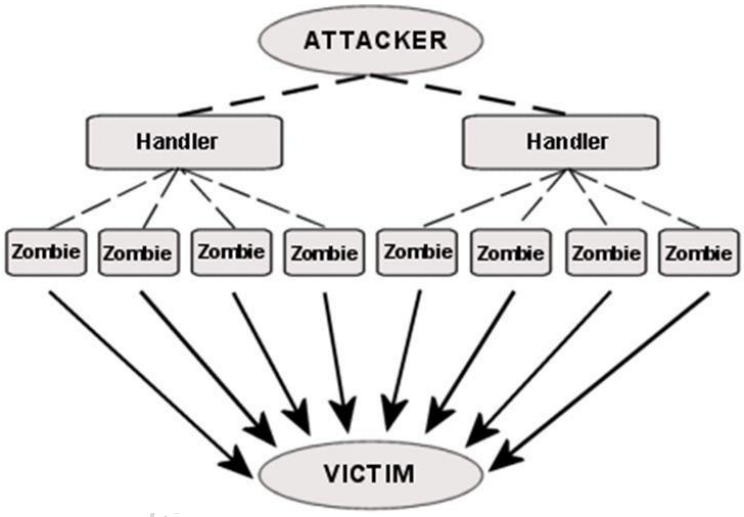
Có thể chia tấn công DDoS thành 2 dạng chính theo mô hình kiến trúc: tấn công DDoS trực tiếp (Direct DDoS) và tấn công DDoS gián tiếp, hay phản xạ (Indirect/Reflective DDoS). Trong tấn công DDoS trực tiếp, các yêu cầu tấn công

được các máy tấn công gửi trực tiếp đến máy nạn nhân. Ngược lại, trong tấn công DDoS gián tiếp, các yêu cầu tấn công được gửi đến các máy phản xạ (Reflectors) và sau đó gián tiếp chuyển đến máy nạn nhân.

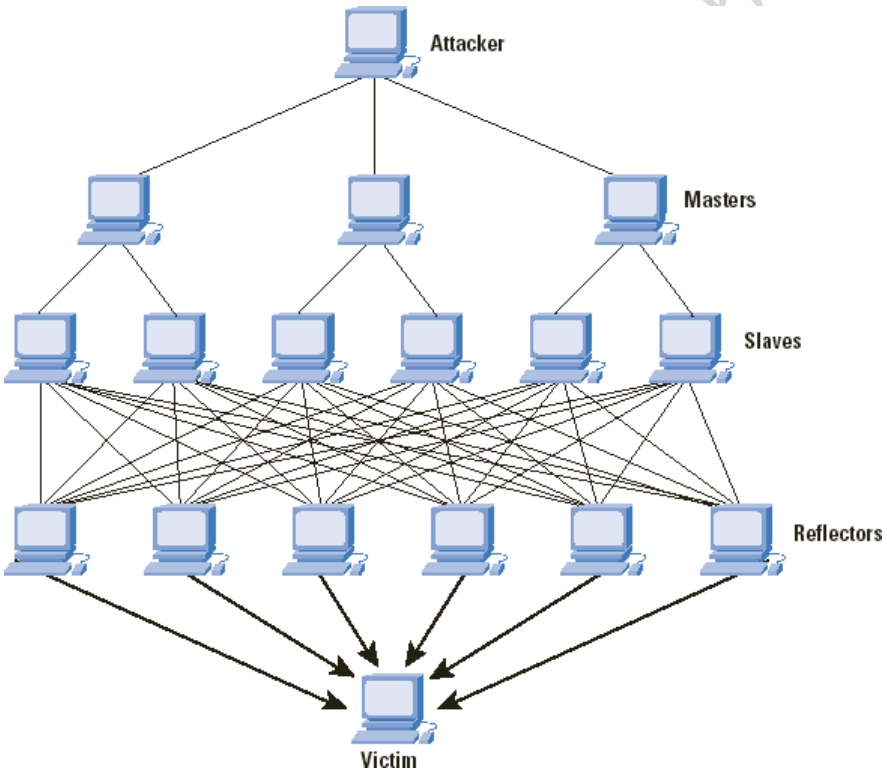
1.2.2 Tấn công DDoS trực tiếp

Hình 2.23 minh họa kiến trúc điển hình của dạng tấn công DDoS trực tiếp. Tấn công DDoS trực tiếp được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- Kẻ tấn công (Attacker) chiếm quyền điều khiển hàng ngàn, thậm chí hàng chục ngàn máy tính trên mạng Internet, sau đó bí mật cài các chương trình tấn công tự động (Automated agents) lên các máy này. Các automated agents còn được gọi là các Bot hoặc Zombie (Máy tính ma);
- Các máy bị chiếm quyền điều khiển hình thành mạng máy tính ma, gọi là botnet hay zombie network. Các botnet, hay zombie network không bị giới hạn bởi chủng loại thiết bị và tô pô mạng vật lý;
- Kẻ tấn công có thể giao tiếp với các máy botnet, zombie thông qua một mạng lưới các máy trung gian (handler) gồm nhiều tầng. Phương thức giao tiếp có thể là IRC (Internet Relay Chat), P2P (Peer to Peer), HTTP,...
- Tiếp theo, kẻ tấn công ra lệnh cho các automated agents đồng loạt tạo các yêu cầu giả mạo gửi đến các máy nạn nhân tạo thành cuộc tấn công DDoS;
- Lượng yêu cầu giả mạo có thể rất lớn và đến từ rất nhiều nguồn, vị trí địa lý khác nhau nên rất khó đối phó và lần vết để tìm ra kẻ tấn công thực sự.



Hình 2.23. Kiến trúc tấn công DDoS trực tiếp



Hình 2.24. Kiến trúc tấn công DDoS gián tiếp hay phản xạ

1.2.3 Tấn công DDoS gián tiếp

Hình 2.24 minh họa kiến trúc tấn công DDoS gián tiếp, hay phản xạ. Tấn công DDoS gián tiếp cũng được thực hiện theo nhiều giai đoạn theo kịch bản như sau:

- Kẻ tấn công chiếm quyền điều khiển của một lượng lớn máy tính trên mạng Internet, cài đặt phần mềm tấn công tự động bot/zombie (còn gọi là slave), hình thành nên mạng botnet;
- Theo lệnh của kẻ tấn công điều khiển các Slave/Zombie gửi một lượng lớn yêu cầu giả mạo với địa chỉ nguồn là địa chỉ máy nạn nhân đến một số lớn các máy khác (Reflectors) trên mạng Internet;
- Các Reflectors gửi các phản hồi (Reply) đến máy nạn nhân do địa chỉ của máy nạn nhân được đặt vào địa chỉ nguồn của yêu cầu giả mạo;
- Khi các Reflectors có số lượng lớn, số phản hồi sẽ rất lớn và gây ngập lụt đường truyền mạng hoặc làm cạn kiệt tài nguyên của máy nạn nhân, dẫn đến ngắt quãng hoặc ngừng dịch vụ cung cấp cho người dùng. Các Reflectors bị lợi dụng để tham gia tấn công thường là các hệ thống máy chủ có công suất lớn trên mạng Internet và không chịu sự điều khiển của tin tặc.

1.2.4 Phòng chống tấn công DDoS

Nhìn chung, để phòng chống tấn công DDoS hiệu quả, cần kết hợp nhiều biện

pháp và sự phối hợp của nhiều bên do tấn công DDoS có tính phân tán cao và hệ thống mạng máy tính ma (botnet) được hình thành và điều khiển theo nhiều tầng, lớp. Một số biện pháp có thể xem xét áp dụng:

- Sử dụng các phần mềm rà quét vi rút và các phần mềm độc hại khác nhằm loại bỏ các loại bot, zombie, slaves khỏi các hệ thống máy tính;
- Sử dụng các hệ thống lọc đặt trên các router, tường lửa của các nhà cung cấp dịch vụ Internet (ISP) để lọc các yêu cầu điều khiển (C&C – Command and Control) gửi từ kẻ tấn công đến các bot;
- Sử dụng các hệ thống giám sát, phát hiện bất thường, nhằm phát hiện sớm các dấu hiệu của tấn công DDoS.
- Sử dụng tường lửa để chặn (block) tạm thời các cổng dịch vụ bị tấn công.

1.3 Tấn công giả mạo địa chỉ

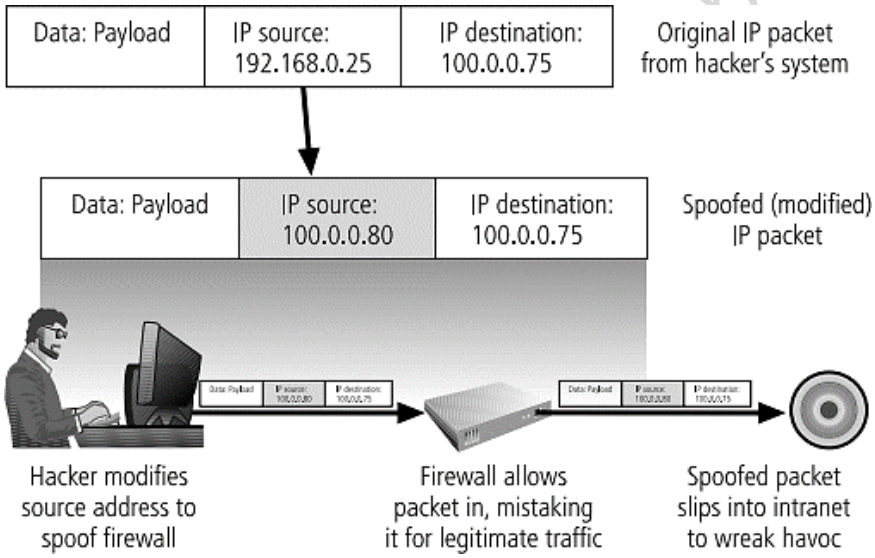
1.3.1 Giới thiệu

Dạng tấn công giả mạo địa chỉ thường gặp nhất là tấn công giả mạo địa chỉ IP, trong đó kẻ tấn công sử dụng địa chỉ IP giả làm địa chỉ nguồn (Source IP) của các gói tin IP, thường để đánh lừa máy nạn nhân nhằm vượt qua các hàng rào kiểm soát an ninh thông thường. Chẳng hạn, nếu kẻ tấn công giả địa chỉ IP là địa chỉ cục bộ của mạng LAN, hắn có thể có nhiều cơ hội xâm nhập vào các máy khác trong mạng LAN đó do chính sách kiểm soát an ninh với các máy trong cùng mạng LAN thường được giảm nhẹ.

1.3.2 Kịch bản

Hình 2.25 minh họa một cuộc tấn công giả mạo địa chỉ IP vào một máy nạn nhân trong mạng cục bộ. Các bước thực hiện như sau:

- Giả sử máy của kẻ tấn công có địa chỉ IP là 192.168.0.25 và hắn muốn gửi gói tin tấn công đến máy nạn nhân có địa chỉ IP là 100.0.0.75;
- Kẻ tấn công tạo và gửi yêu cầu giả mạo với địa chỉ IP nguồn của các gói tin IP của yêu cầu là 100.0.0.80 đến máy nạn nhân. Địa chỉ 100.0.0.80 là địa chỉ cùng mạng LAN với máy nạn nhân 100.0.0.75;
- Nếu tường lửa của mạng LAN không lọc được các gói tin với địa chỉ nguồn giả mạo, yêu cầu giả mạo của kẻ tấn công có thể đến được và gây tác hại cho máy nạn nhân.



Hình 2.25. Minh họa tấn công giả mạo địa chỉ IP

1.3.3 Phòng chống

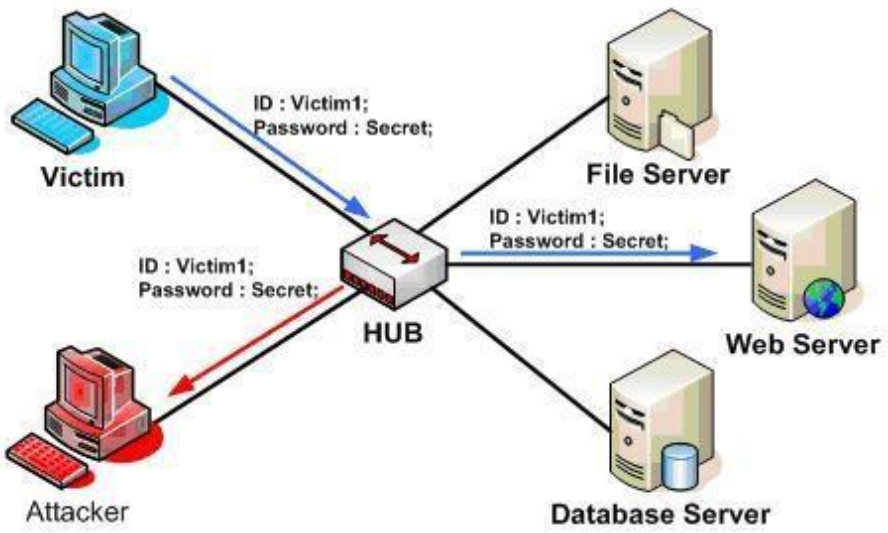
Biện pháp phòng chống tấn công giả mạo địa chỉ IP hiệu quả nhất là sử dụng kỹ thuật lọc trên tường lửa, hoặc các router với nguyên tắc lọc: các gói tin từ mạng ngoài đi vào mạng LAN mà có địa chỉ nguồn là địa chỉ nội bộ của mạng LAN đó thì chúng là các gói tin giả mạo và phải bị chặn.

1.4 Tấn công nghe lén

Tấn công nghe lén (Sniffing/Eavesdropping), như minh họa trên Hình 2.26 là dạng tấn công sử dụng thiết bị phần cứng hoặc phần mềm, lắng nghe trên card mạng, hub, switch, router, hoặc môi trường truyền dẫn để bắt các gói tin dùng cho phân tích, hoặc lạm dụng về sau. Đây là kiểu tấn công thụ động nhằm thu thập các thông tin nhạy cảm, hoặc giám sát lưu lượng mạng. Các thông tin nhạy cảm như tên người dùng, mật khẩu, thông tin thanh toán nếu không được mã hóa có thể bị nghe lén và lạm dụng. Các thông tin truyền trong mạng WiFi, hoặc các mạng không dây cũng có thể bị nghe lén dễ dàng do môi trường truyền dẫn vô tuyến và nếu không sử dụng các cơ chế bảo mật đủ mạnh.

Để phòng chống tấn công nghe lén, có thể áp dụng các biện pháp sau:

- Có cơ chế bảo vệ các thiết bị mạng và hệ thống truyền dẫn ở mức vật lý;
- Sử dụng các biện pháp, cơ chế xác thực người dùng đủ mạnh;
- Sử dụng các biện pháp bảo mật thông tin truyền dựa trên các kỹ thuật mã hóa.



Hình 2.26. Tấn công nghe lén