

QUÉT HỆ THỐNG VÀ NGHE LÉN

Khoa Công nghệ thông tin và Truyền thông
Trường Đại học Cần Thơ

Phần B

NGHE LÉN

NGHE LÉN

- Khái niệm về nghe lén.
- Hoạt động nghe lén.
- Phân loại các hình thức tấn công nghe lén.
- Các biện pháp phòng chống.

KHÁI NIỆM VỀ NGHE LÉN

- Nghe lén là hành động bắt gói tin (packet) hay bắt khung tin (frame) lan truyền trong mạng nội bộ.
- Thông tin người dùng có thể bị đánh cắp và được sử dụng bất hợp pháp khi hệ thống bị nghe lén.

HOẠT ĐỘNG NGHE LÉN

- Kẻ tấn công sử dụng công cụ chuyên biệt để đón bắt gói tin lan truyền trong mạng thông qua switch hay hub. Các gói tin này do người dùng trong mạng truyền-nhận với nhau

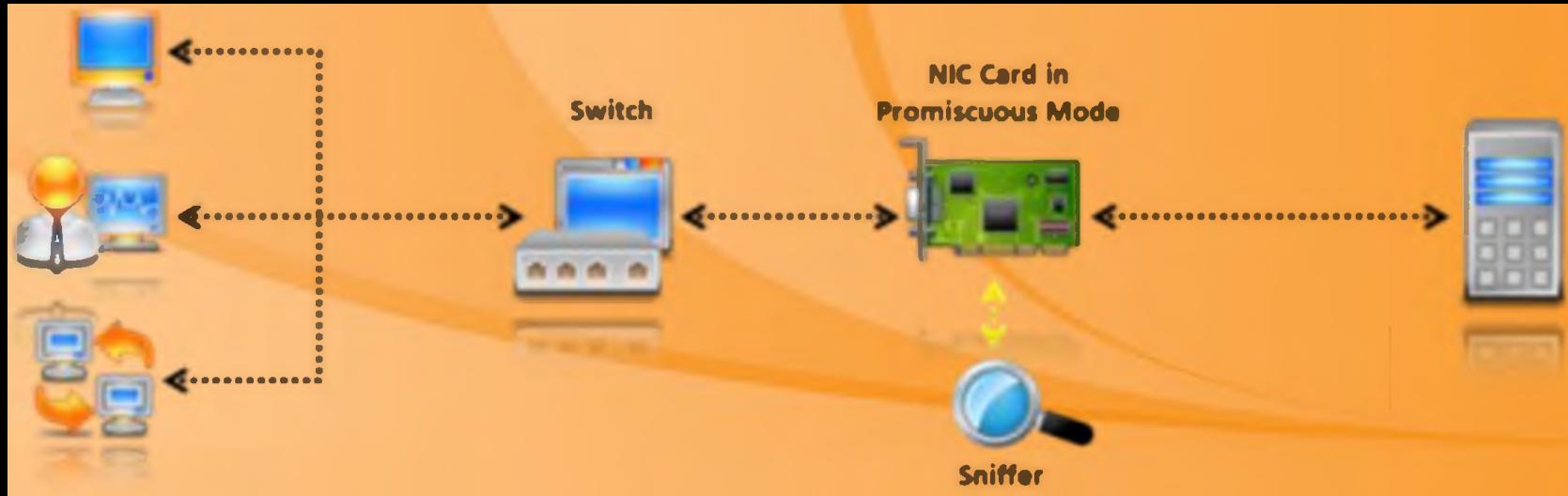


NGUY CƠ DẪN ĐẾN BỊ NGHE

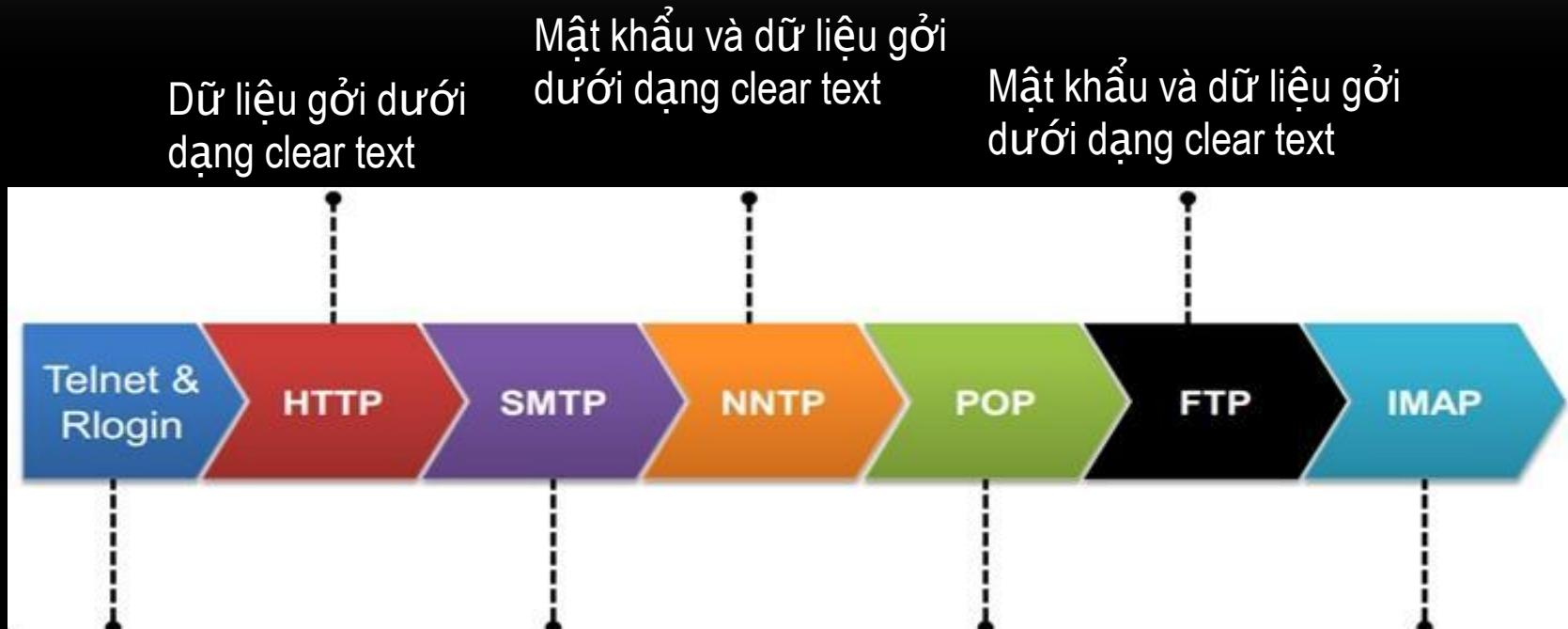
- Cơ chế bảo mật lỏng lẻo như mở cổng không cần thiết trên các thiết bị chuyển mạch như switch.
- Không tiến hành phân chia mạng con (subnet) cho hệ thống.
- Nhân viên không được phổ biến về các mối nguy hại.
- Dữ liệu truyền đi không được mã hoá.

CƠ CHẾ CỦA HOẠT ĐỘNG NGHE LÉN

- Kẻ nghe lén sẽ kích hoạt chế độ hỗn tạp (promiscuous) trên card mạng (NIC) của máy tính để có thể nhận tất cả các gói tin/khung thông tin vận chuyển qua segment mạng mà NIC kết nối tới.
- Nội dung của gói/khung thông tin có thể được giải mã dựa vào phân tích hình thái của gói/khung thông tin này.



CÁC THÔNG TIN CÓ THỂ BỊ NGHE LÉN



Thăm dò tên người dùng và mật khẩu

Mật khẩu và dữ liệu gửi dưới dạng clear text

Mật khẩu và dữ liệu gửi dưới dạng clear text

Mật khẩu và dữ liệu gửi dưới dạng clear text

CÁC CÔNG CỤ NGHE LÉN

- **Cain & Abel** là một công cụ tấn công đa năng trên windows. Nó cho phép dễ dàng khôi phục các loại mật khẩu khác nhau bằng cách nghe lén trên mạng.
- **Wireshark** có thể bắt được hầu hết các gói tin trong mạng hiện nay như Ethernet, 802.11, PPP/HDLC, ATM, Bluetooth, Token Ring, Frame Relay, FDDI

CÁC CÔNG CỤ NGHE LÉN

- **Ethereal** là một phần mềm nghe lén miễn phí có thể bắt các gói tin từ các kết nối LAN có dây và không dây.
- **Etherpeek** là một công cụ sniffer tuyệt vời cho mạng có dây với bộ lọc mở rộng và khả năng theo dõi các cuộc hội thoại TCP/IP. Phiên bản mới nhất của Etherpeek được đổi tên thành OmniPeek

BIỆN PHÁP PHÒNG CHỐNG NGHE LÉN

- Cách bảo mật tốt nhất để chống lại nghe lén trong mạng là sự mã hóa. Mặc dù sự mã hóa cũng không ngăn chặn được việc gói tin bị chặn bắt, nhưng nó làm cho bất kỳ dữ liệu nào bị nghe lén cũng trở nên vô dụng bởi vì hacker không thể hiểu được thông tin đó.