# CHƯƠNG 4

Giám sát các hoạt động giao tiếp

# Nội dung

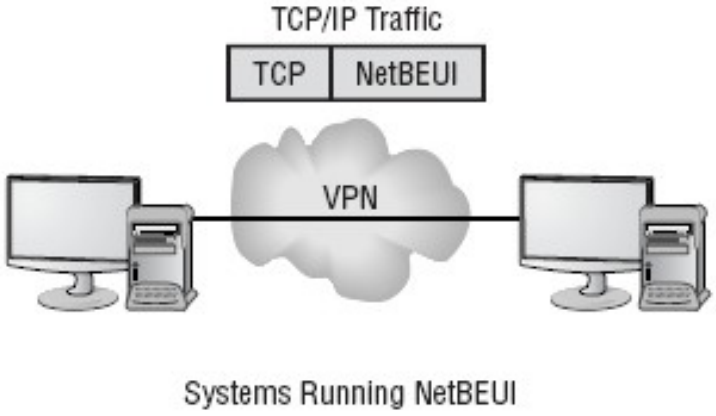
- Giám sát mạng
- Các hệ thống phát hiện xâm nhập
- Các hệ thống không dây
- Các đặc điểm của các phần mềm gửi nhận thông điệp
- Phát hiện gói

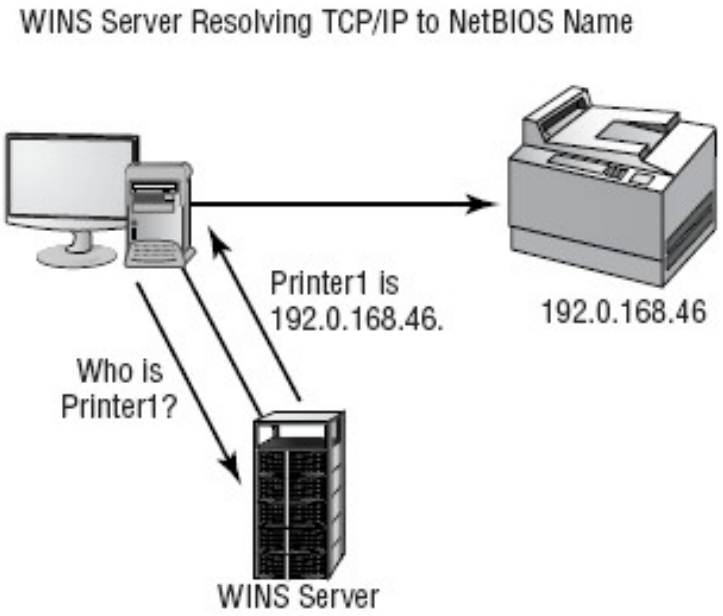
# 4.1 Giám sát mạng

- Mạng bị tấn công bởi nhiều hình thức
- Việc giám sát giúp ta theo dõi các sự kiện hoạt động của hệ thống mạng.
- Real-time (network snipper) hoặc ngay khi có sự kiện xảy ra (sử dụng IDS)
- Biện pháp:
  - Cài đặt các chương trình theo dõi giám sát hệ thống và báo cáo khi có sự kiện bất thường xảy ra
  - System log
  - Hệ thống IDS

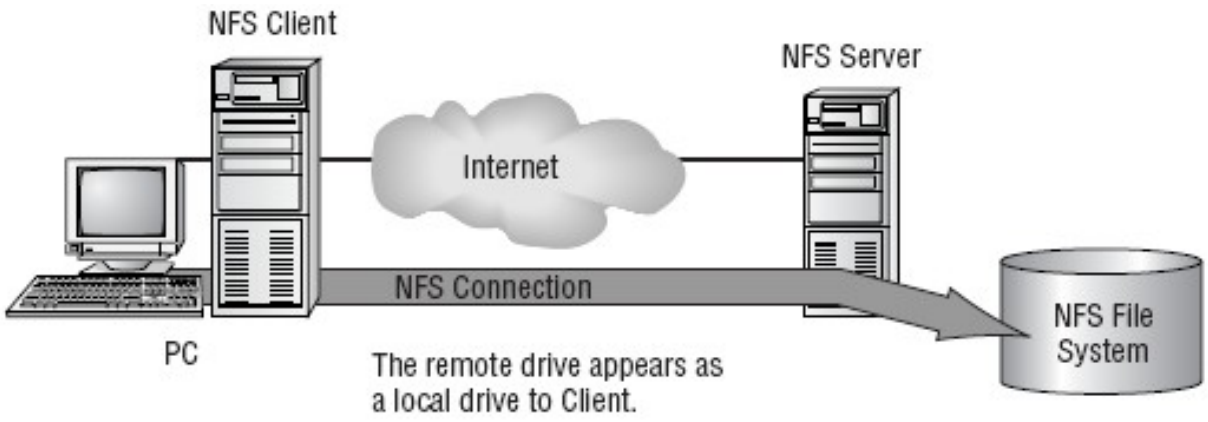
- Xác định các loại giao tiếp
  - TCP/IP
    - IP, TCP, UDP, ICMP, and IGMP
    - Sử dụng netstat
  - Các giao thức Novell
    - Novell Netware
    - IPX/SPX: giao thức cho mạng lớn và nhỏ
    - NDS và eDirectory: dịch vụ directory của Novell (Netware Directory Service)

- Giao thức Microsoft
  - NetBIOS:
    - sử dụng khái niệm tên tài nguyên 15-ký tự, có thể giao tiếp NetBEUI, TCP/IP, or IPX/SPX.
    - Mở port cho dịch vụ chia sẻ tập tin và in ấn
  - NetBEUI:
    - NetBIOS Extended User Interface
    - Sử dụng truyền NetBIOS qua LAN
    - Là giao thức không thể định tuyến -> không truyền được qua router
    - Dễ bị tấn công bởi sniffer
  - Dịch vụ WINS Service:
    - Chuyển địa chỉ NetBIOS sang địa chỉ TCP/IP, tương tự DNS
    - Chạy trên Windows Advanced Server
    - Nếu không có WINS thì Windows sử dụng LMHOSTS
    - Dễ bị tấn công ở dạng DoS

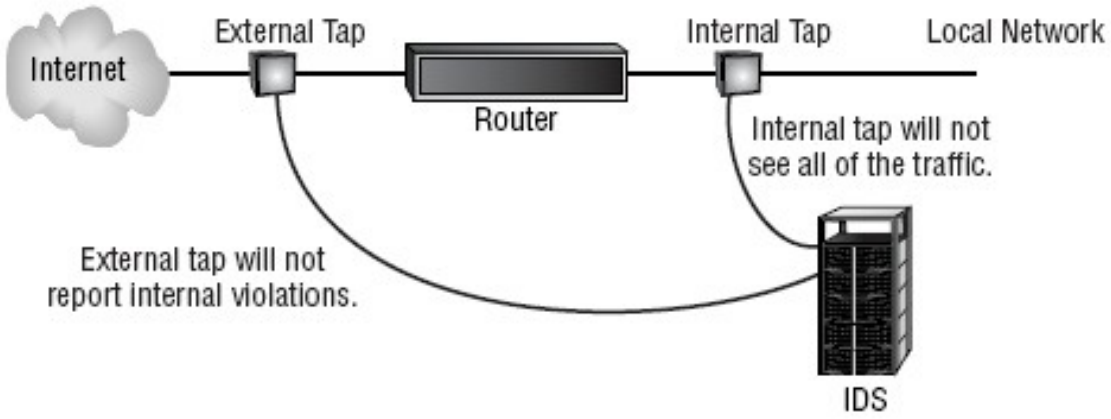

TCP/IP Traffic
TCP
NetBEUI
VPN
Systems Running NetBEUI


WINS Server Resolving TCP/IP to NetBIOS Name
Printer1 is
192.0.168.46.
192.0.168.46
Who is
Printer1?
WINS Server

- Giao thức NFS:
  - Giao thức chia sẻ tập tin trên hệ thống Unix
  - Cho phép user từ xa mount ổ đĩa trên mạng
- Giao thức Apple
  - AppleTalk
  - Giao thức khả định tuyến



- Các hệ thống giám sát mạng



# 4.2 Các hệ thống phát hiện xâm nhập

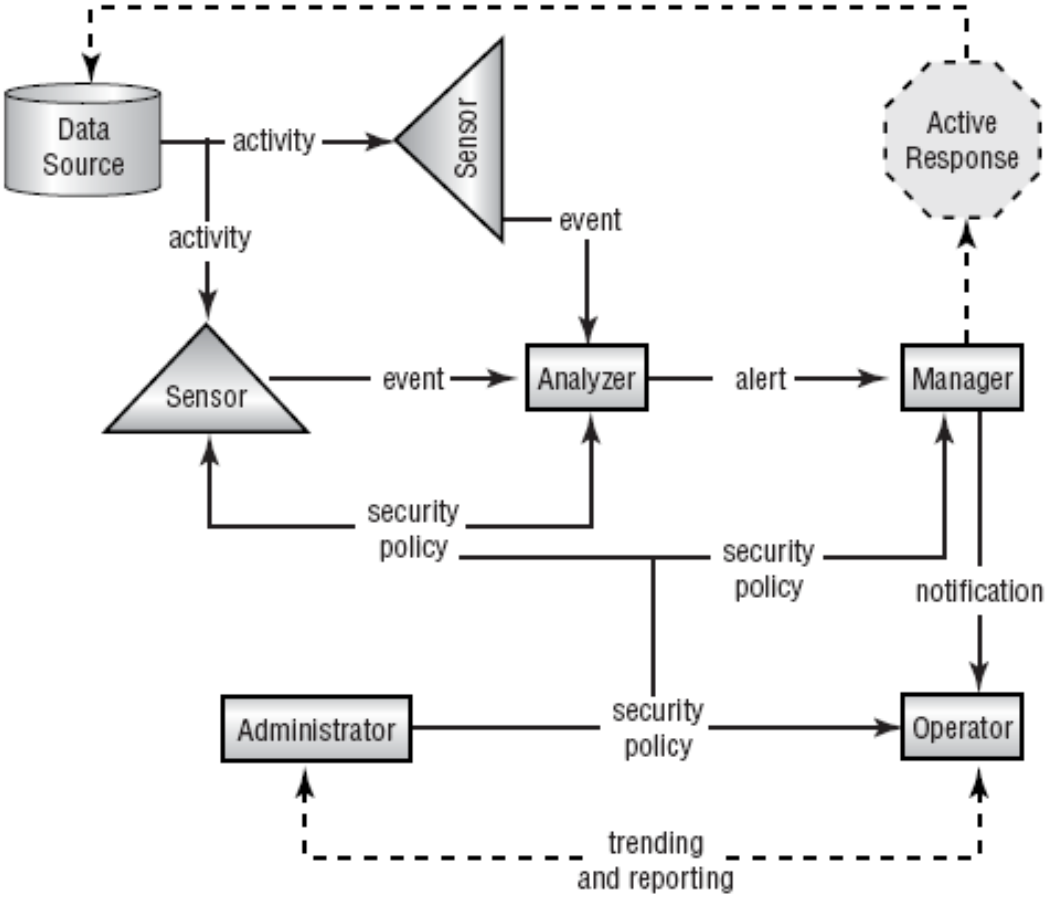
- IDS giúp phát hiện sự xâm nhập
- ID: quá trình giám sát theo dõi các sự kiện trong hệ thống phát hiện có sự xâm nhập hay không.
- Xâm nhập:
  - Hoạt động hay hành động đe dọa đến độ tin cậy, nhất quán hoặc tính có sẵn tài nguyên

# Một số thuật ngữ

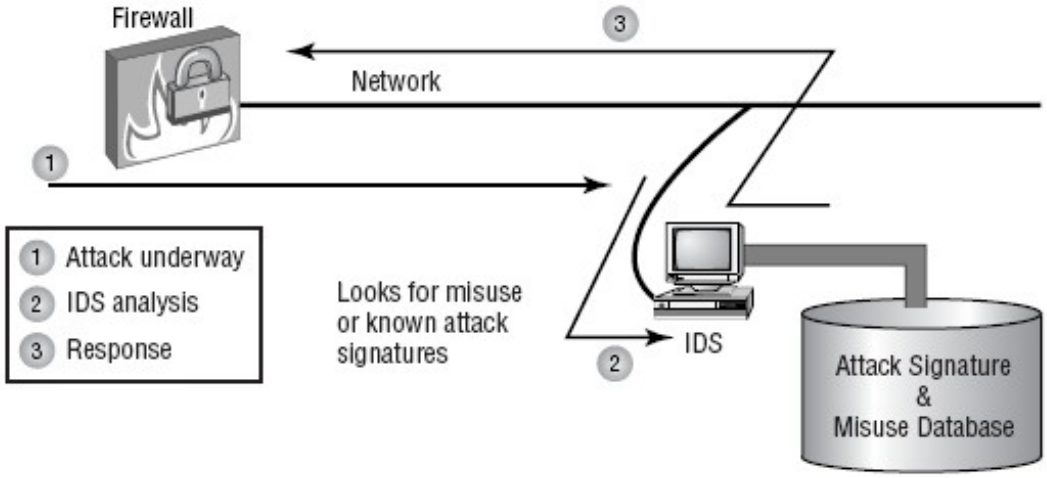
- Activity: là một thành phần của nguồn dữ liệu được người điều hành quan tâm
- Administrator: người chịu trách nhiệm thiết lập chính sách bảo mật (triển khai, cấu hình các IDS…)
- Operator: người chịu trách nhiệm chính IDS
- Alert: thông báo từ chương trình phân tích cho biết có sự kiện được quan tâm xảy ra (ICMP)
- Analyzer - chương trình phân tích: phân tích dữ liệu có được từ cảm biến. Tìm kiếm các hoạt động nghi ngờ.
- Data source: thông tin thô mà IDS sử dụng để phát hiện các hoạt động nghi ngờ (tập tin audit, system log, luồng thông tin trên mạng)

# Một số thuật ngữ (tt)

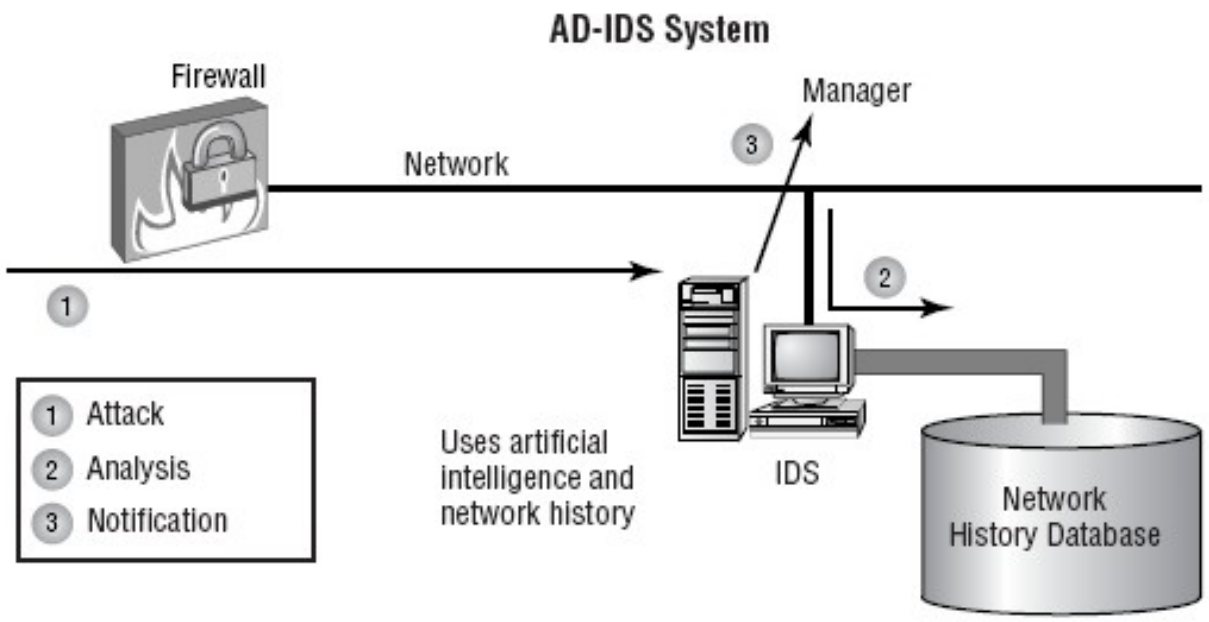
- Event: là sự kiện xảy ra trong nguồn dữ liệu cho biết có hoạt động nghi vấn xảy ra.
- Manager: là chương trình hoặc quá trình mà người điều hành sử dụng trong IDS. Ví dụ: IDS console
- Notification: là quá trình hoặc phương pháp mà manager đưa ra thông báo alert cho người điều hành.
- Sensor: là thành phần trong IDS, thu thập dữ liệu từ nguồn dữ liệu và chuyển nó cho analyzer (trình điều khiển thiết bị, hộp đen kết nối với mạng và truyền báo cáo với IDS). Là điểm thu thập dữ liệu nguồn chính của IDS


Data Source
activity
Sensor
Active Response
activity
event
Sensor
event
Analyzer
alert
Manager
security policy
security policy
notification
Administrator
security policy
Operator
trending and reporting

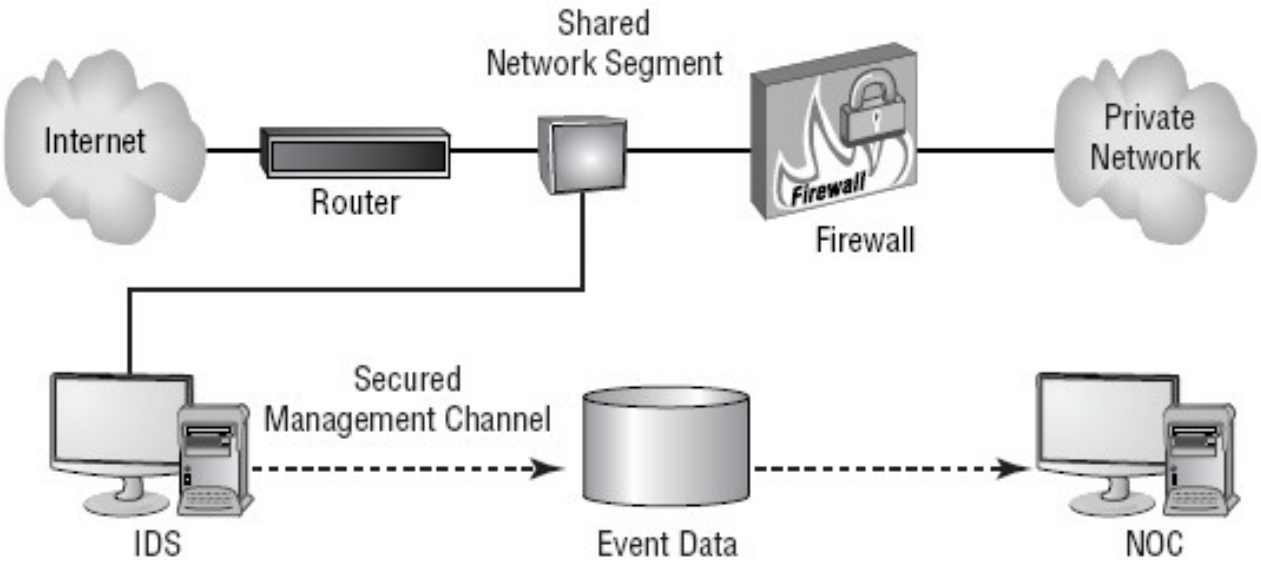
- Mô hình IDS (IDS # firewall):
  - Misuse Detection IDS: tập trung đánh giá các dấu hiệu tấn công và kiểm tra.
    - Dấu hiệu tấn công (attack signature): mô tả pp tấn công tổng quát
    - Tấn công TCP flood attack thực hiện các session TCP không hoàn tất. MD-IDS biết được hình thái tấn công TCP flood attack, nó tạo báo cáo hoặc đáp ứng tương ứng nhằm ngăn trở tấn công



- Mô hình IDS (tt)
  - Anomaly-Detection IDS: *AD-IDS* tìm kiếm sự bất thường.
  - Chương trình huấn luyện học các hoạt động bình thường, có AI



- Mô hình IDS (tt)
  - Network-based IDS (N-IDS): được thêm vào hệ thống qua giao tiếp mạng, quản lý, báo cáo tất cả các luồng thông tin trên mạng
  - Lắp đặt trước, hoặc sau firewall



- N-IDS (tt)
  - Trước firewall: quản lý tất cả các luồng thông tin đi vào mạng
  - Sau firewall: chỉ thấy đc các hoạt động đi qua firewall
  - Có thể kết nối với switch, hub hoặc kết nối với tap.
  - 2 loại đáp ứng:
    - Passive
    - Active

# N-IDS

- Passive: là loại đáp ứng phổ biến đối với các tấn công, dễ phát triển, hiện thực
  - Đăng nhập
  - Thông báo
  - Tránh
- Active: là đáp ứng dựa trên tấn công -> có thể ngăn chặn ảnh hưởng nhanh nhất.
  - Lập kế hoạch cho các event, các chính sách, và cả AI.
  - Hủy quá trình hoặc session: ie. flooding
  - Thay đổi cấu hình mạng: từ chối các yêu cầu trên 1 IP nào đó trong thời gian biết trước
  - Đánh lừa: đánh lừa kẻ tấn công việc tấn công đã thành công, kiểm soát toàn bộ thông tin gửi về hệ thống bị tấn công -> phân tích tình hình, cách thức tấn công -> đưa giải pháp

# H-IDS (Host-based IDS)

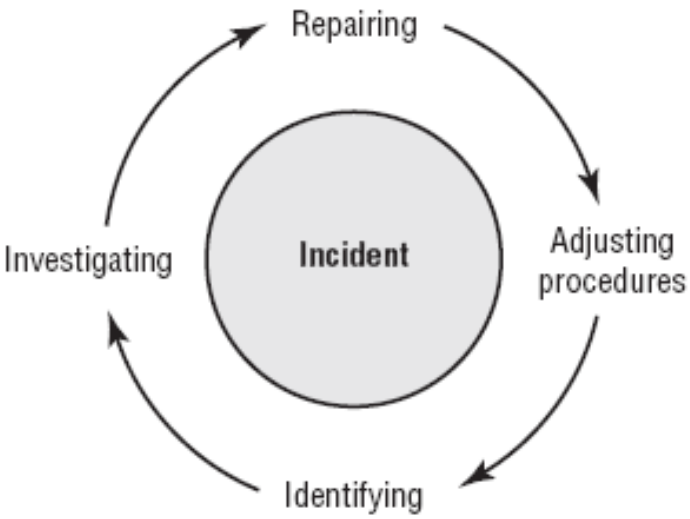
- Là phần mềm chạy trên host như 1 dịch vụ hoặc quá trình chạy nền
- Sử dụng các log, sự kiện hệ thống, các tương tác của phần mềm
- Không kiểm soát luồng thông tin truyền vào host.
- Cài đặt trên server sử dụng mã hóa
- Passive
- 2 khuyết điểm:
  - Có thể làm hư hại các file log
  - Phải triển khai trên mỗi host có nhu cầu
- 1 ưu điểm:
  - Giúp lưu giữ checksum trên file log -> dễ nhận biết tấn công

# Honey pot

- Là máy được thiết kế như “máy mồi”
- Mục đích là chịu đựng sự tấn công và chết -> hiểu cơ chế tấn công -> đưa ra giải pháp an toàn
- Được thiết kế tỉ mỉ để nhử tấn công
- Trong thực tế, máy được thiết kế cài đặt như là một hệ thống mạng tổng hợp, và giao tiếp với hệ thống mạng
  - Enticement: là quá trình đánh lừa người khác: quảng cáo phần mềm miễn phí, giả vờ khoe không có ai có thể tấn công được
  - Entrapment: đánh bẫy là quá trình mà pháp luật khuyến khích sử dụng để kết luận ai đó phạm tội.

# Đáp ứng rắc rối

- Là quá trình của nhận dạng, điều tra, sửa chữa, lập tài liệu, và điều chỉnh nhằm ngăn chặn rắc rối khác xảy ra.



- B1: Nhận diện rắc rối:
  - Tấn công bên trong hay từ bên ngoài?
  - Quá tải?

- B2: Điều tra rắc rối
  - Log, các file liên quan đến rắc rối
  - Xác định tấn công nào lớn: sự kiện ngẫu nhiên hay là tích cực nhầm (có thể xảy ra khi luồng thông tin qua mạng không bình thường)
  - Thay đổi chính sách để đối phó với các đe dọa mới
  - Cần ghi nhận lại tài liệu

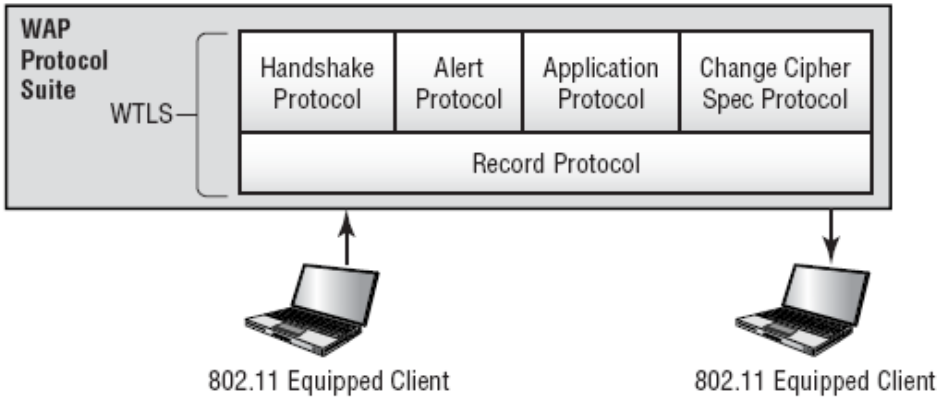
- B3: Sửa chữa hư hỏng
  - Tìm cách phục hồi truy xuất tài nguyên bị tổn hại
  - Thiết lập lại quyền kiểm soát hệ thống
  - DoS -> reset
  - Hư hỏng do worm -> anti-virus, ghost từ đầu
- B4: Lập tài liệu sự cố
  - Lập tài liệu các bước nhận diện, phát hiện, và sửa chữa
  - Chuyển thông tin cho các nhà viết phần mềm hoặc hệ thống
- B5: Điều chỉnh sau khi xử lý thành công sự cố
  - Các chính sách nào hoạt động tốt hay không hoạt động
  - Học được gì sau sự cố
  - Nên thực hiện thế nào vào lần sau

# 4.3 Các hệ thống không dây

- Wireless Transport Layer Security (WTLS)
- Các chuẩn không dây IEEE 802.11
- Các ứng dụng WEP/WAP

# WTLS

- Là lớp an toàn của giao thức ứng dụng không dây (WAP)
- Cung cấp xác thực, mã hóa và tính nhất quán dữ liệu của thiết bị không dây.
- Sử dụng băng thông hẹp
- Mức độ bảo mật vừa phải
- Ứng dụng cho các thiết bị điện thoại di động
- WTLS là một phần trong hệ thống WAP



# Các chuẩn không dây IEEE 802.11

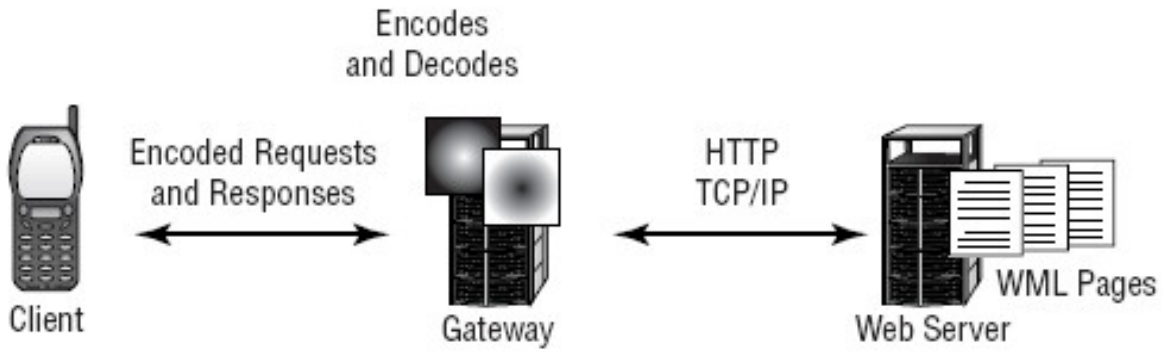
- Họ các giao thức IEEE 802.11x cung cấp giao tiếp không dây trên tần số radio
- Phổ tần số 2.4GHz và 5GHz
- **802.11**
  - băng thông 1Mbps hoặc 2Mbps
  - Phổ tần số 2.4GHz và sử dụng phổ tần mở rộng FHSS (frequency-hopping spread spectrum) hoặc DSSS (direct-sequence spread spectrum) để mã hóa dữ liệu.
- **802.11a**
  - Băng thông: upto 54Mbps
  - Phổ tần 5GHz.
  - Sử dụng OFDM (orthogonal frequency division multiplexing) để mã hóa dữ liệu
- **802.11b**
  - Băng thông: upto 11Mbps (scale 5.5, 2, và 1Mbps)
  - Phổ tần 2.4GHz.
  - Chỉ sử dụng DSSS.
- **802.11g**
  - Băng thông: 20Mbps+
  - Phổ tần 2.4GHz.

# Các chuẩn không dây IEEE 802.11 (tt)

- **Direct-Sequence Spread Spectrum (DSSS)** thêm dữ liệu cần được truyền vào đường truyền tốc độ cao hơn. Truyền tốc độ cao chứa thông tin dư thừa để đảm bảo tính chính xác của dữ liệu.
- **Frequency-Hopping Spread Spectrum (FHSS)** phân đoạn đường truyền trên một dãy các tần số xác định trước. Việc phân đoạn được đồng bộ ở 2 đầu cuối và được thấy như một kênh truyền đơn ở cả 2 đầu
- **Orthogonal Frequency Division Multiplexing (OFDM)** phân chia dữ liệu thành các tín hiệu con và truyền chúng đồng thời. Việc truyền này có thể diễn ra trên nhiều tần số hoặc phổ tần khác nhau

# WEP/WAP

- WAP: Wireless Access Protocol
- WEP: Wired Equivalent Privacy
- WAP:
  - Được phát triển bởi Motorola, Nokia và một số hãng khác
  - Chức năng tương tự như TCP/IP
  - Sử dụng phiên bản ngắn gọn của HTML (WML), WML script



- WAP:
  - Hệ thống gateway WAP
    - HTTP <-> WAP
    - Mã hóa, giải mã trên các giao thức bảo mật
    - WAP server và Internet không được mã hóa -> **gap** trong WAP
- WEP:
  - Là chuẩn an toàn bảo mật mới cho thiết bị không dây
  - Mã hóa dữ liệu
  - Có khả năng bị hack trong vòng 5g

# Các tấn công có thể trên hệ thống không dây

- Tất cả giao tiếp sử dụng tần số radio.
- Tần số radio đều có thể bị can thiệp dễ dàng
- Sử dụng PC + 802.11x card tương ứng + chương trình bắt gói dữ liệu
- Điều tra site (site survey): lắng nghe trên hệ thống mạng không dây, được sử dụng để xác định vùng không bị nhiễu (loại hệ thống, các protocol sử dụng, thông tin mật khác của hệ thống)

# 4.4 Phần mềm nhắn tin

- Trojan
- Mã code nguy hại
- DoS
- Link nguy hại

# 4.5 Phát hiện gói

- Là quá trình kiểm soát dữ liệu truyền qua hệ thống mạng
- Chương trình bắt gói gọi là sniffer

# 4.6 Phân tích tín hiệu

- Phân tích tín hiệu và tín hiệu thông minh liên quan đến việc bắt và phân tích các tín hiệu điện tử.
- Được sử dụng trong quân đội và các tổ chức văn phòng chính phủ
- Footprinting:
  - Là quá trình nhận diện mạng và đặc tính bảo mật một cách có hệ thống.
  - Sử dụng hiểu biết về hệ thống, các giao thức, loại server đang chạy, và các chương trình ứng dụng như web server, mail server...
  - Ví dụ: xem xét mã nguồn của website

- Scanning:
  - Thu thập thông tin cấu hình hệ thống
  - Quét và tìm kiếm đường xâm nhập hệ thống (ví dụ traceroute)
  - Khi biết hiện thực hệ thống, thì nó chuyển sang quá trình quét bằng cách ping địa chỉ gần với địa chỉ web server hay mail server.
  - Nếu có tín hiệu trả lời -> IMCP đang chạy (tức là TCP/IP hiện hữu)
  - Tìm port đang mở trên hệ thống đó
  - Khi tìm được port, tiến hành thăm dò thử nhằm tìm ra sơ hở của hệ thống để tấn công
  - Khi hoàn tất quá trình scan, kẻ tấn công có thể sử dụng enumerate.