Security Bootcamp 2013

GIẢI PHÁP PHÁT HIỆN THÂM NHẬP MẠNG KHÔNG DÂY

Trình bày

TS. Ngô Bá Hùng

nbhung@cit.ctu.edu.vn

KS. Ngô Trung Hiếu

ngotrunghieu@live.com

Khoa CNTT&TT-ĐH Cần Thơ

Đơn vị tổ chức:

Đơn vị tài trợ:

NỘI DUNG TRÌNH BÀY

- Các hình thức tấn công mạng không dây
- Một số giải pháp hiện tại và hạn chế
- Giải pháp DIDS cho mạng không dây
- Kết quả đạt được

Các hình thức tấn công

Mạng không dây
Tiện lợi & nguy cơ

Các hình thức tấn công thông dụng

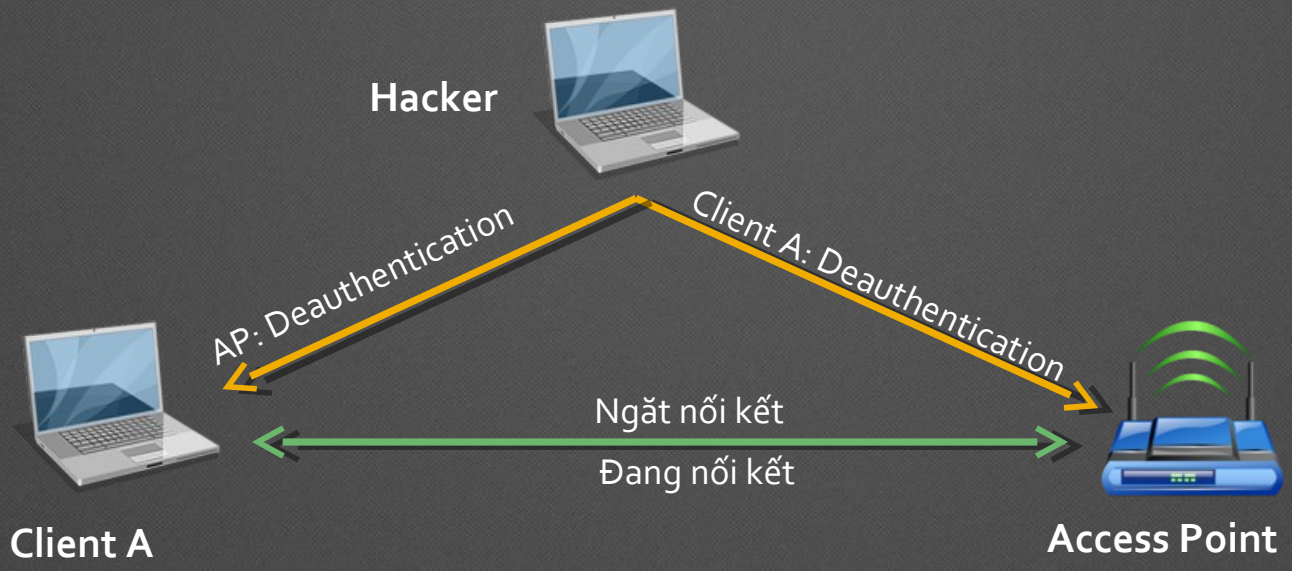
- Tấn công từ chối chứng thực (Deauthentification Attack)
- Tạo Access Point giả mạo
- Tấn công bên trong mạng wireless

Tấn công từ chối chứng thực

- Deauthentication là một kiểu khung con thuộc kiểu Management.
- Khi nhận được khung này, máy thiết bị đang nối kết không dây sẽ ngắt kết nối để sau đó kết nối và chứng thực lại
- Khung Deauthentication hoàn toàn không được bảo vệ bởi chứng thực và mã hóa
- Hacker gởi Khung Deauthentication giả mạo đến máy Client và Access Point

Tấn công từ chối chứng thực

- Nếu gởi Khung Deauthentication liên tục sẽ làm tê liệt Access Point
- Hoặc lừa máy Client kết nối vào Access Point giả mạo



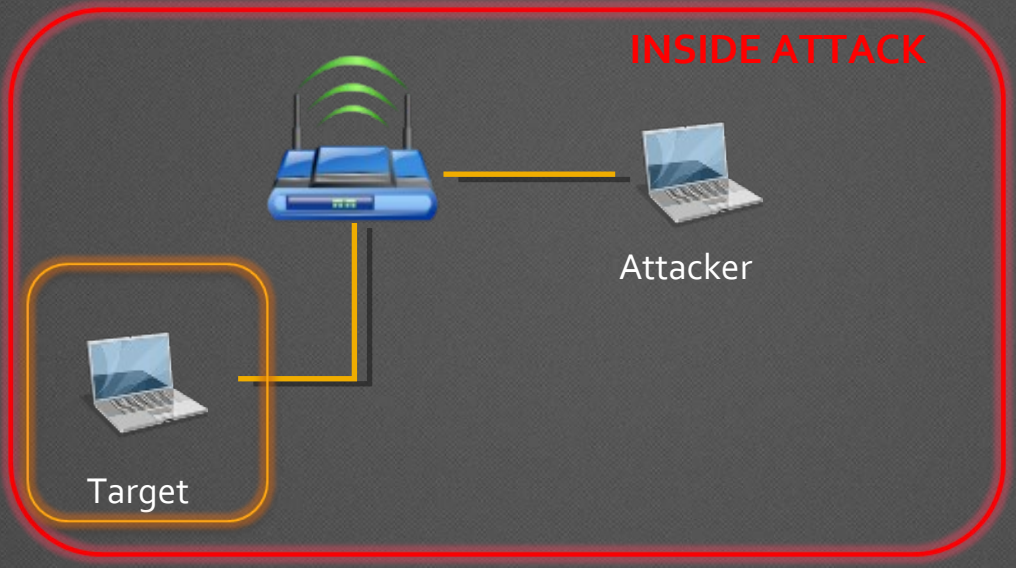
Tạo Access Point giả mạo

- Với một USB Wireless Card và một laptop, Hacker sẽ dựng một Access Point mới ví dụ UBND-VL$_{n+1}$ để lừa người dùng nối kết vào
- Từ đó triển khai các hình thức tấn công khác trên máy đã nối kết
  - Lừa đảo chiếm tài khoản, khóa WPA…
  - Dò khóa WEP từ client
  - Bắt các thông số của 4ways handshake WPA → AP-less WPA Cracking Attack
  - Man-In-The-Middle: đánh cấp, thêm, sửa thông tin nhạy cảm đã mã hóa bằng SSL

Đánh cắp tài khoản với Access Point giả mạo

Access Point giả mạo tạo các trang chứng thực giả và chuyển về cho khách hàng để lấy mật khẩu người dùng

Tấn công bên trong mạng Wireless



Tấn công bên trong mạng Wireless

192.168.1.69/24

samba

root

Xác định được mục tiêu

Xác định được dịch vụ

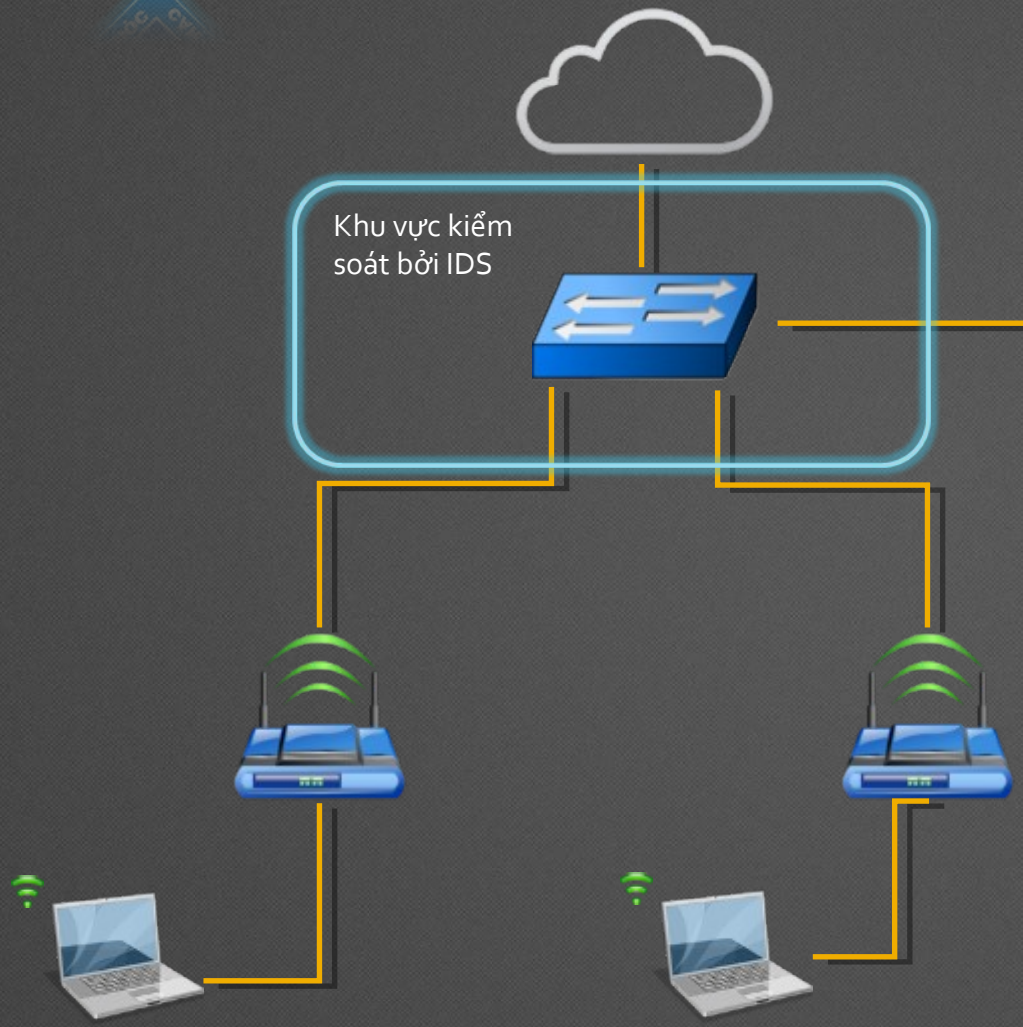
Tiến hành tấn công

- Vô hiệu hóa tường lửa, trình diệt virus… -> Làm mất đi lớp bảo vệ máy tính victim
- Cài đặt virus, backdoor…
- Lợi dụng máy tính victim tấn công mục tiêu khác
- Kích hoạt webcam, microphone tiến hành ghi hình, thu âm victim nhằm "theo dõi"

Một số giải pháp hiện tại và hạn chế

Các giải pháp truyền thống

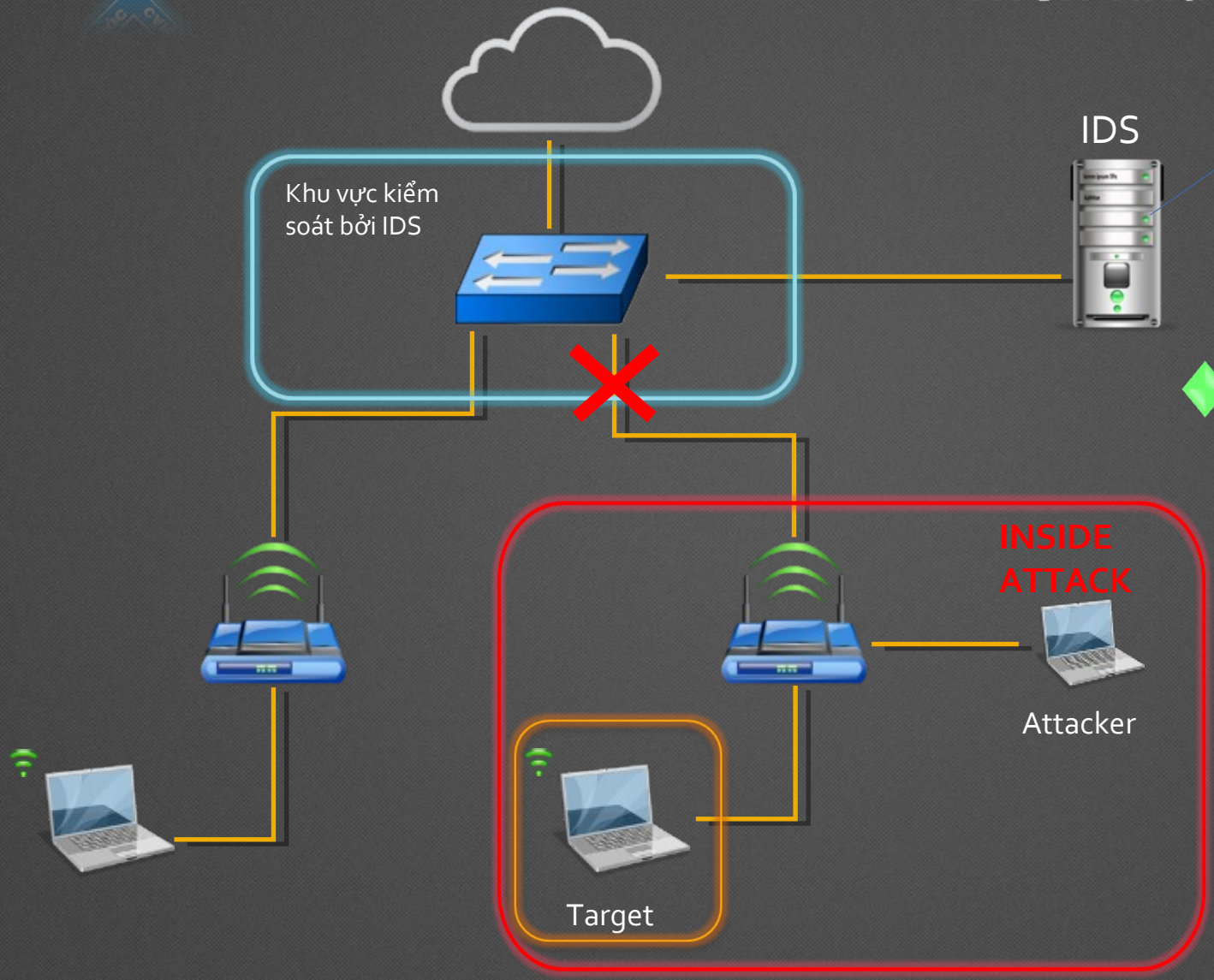
Triển khai IDS



- Kiểm soát lưu thông trên nhiều AP
- Kiểm soát toàn bộ lưu thông vào và ra của mạng không dây

Các giải pháp truyền thống

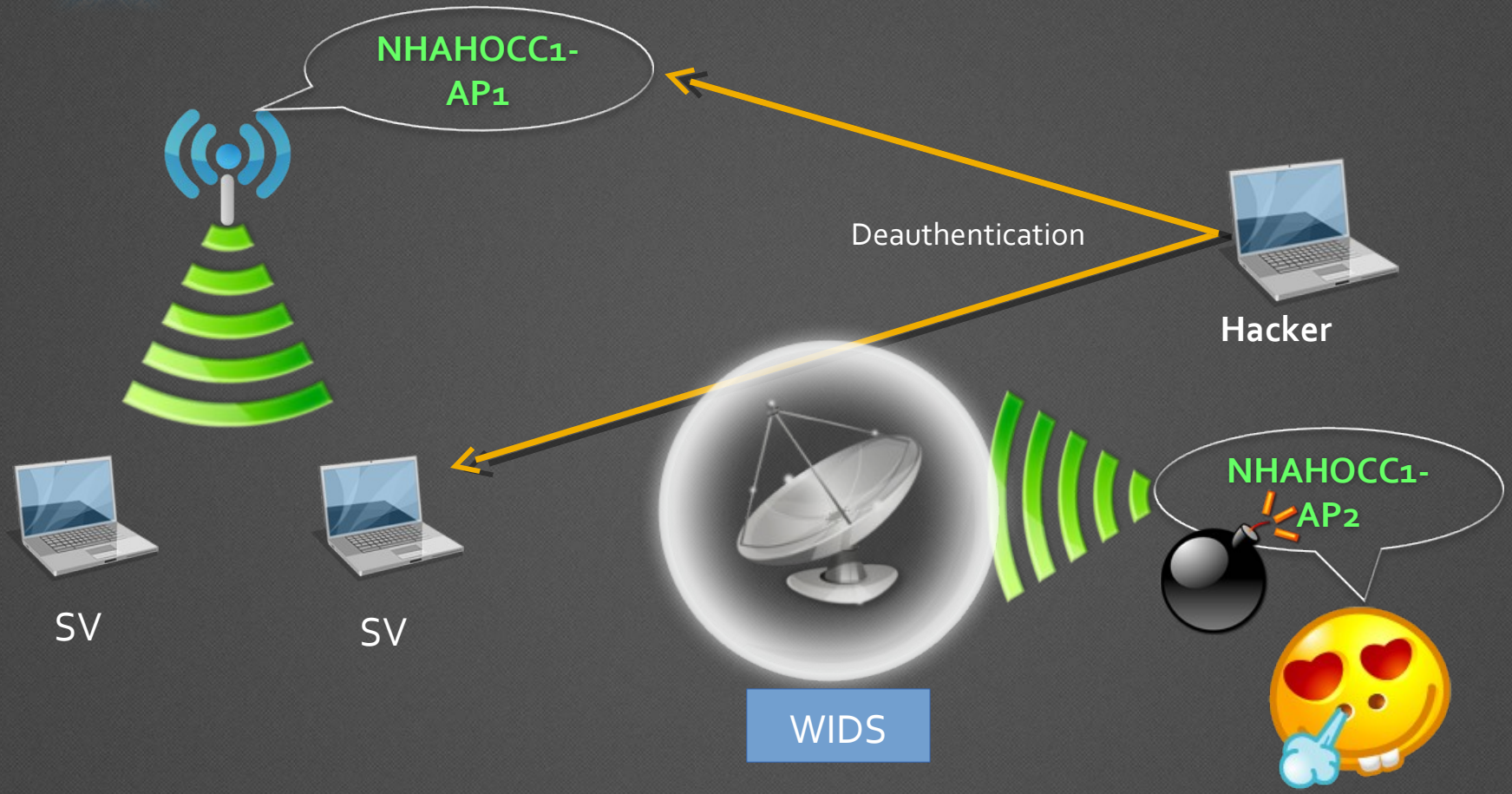
Triển khai IDS



Hệ thống phát hiện thâm nhập -IDS

- Không thể kiểm soát lưu thông nội bộ trong mạng WLAN

Giải pháp WIDS



- Phát hiện được các hình thức tấn công ngoài

Các giải pháp truyền thống

Triển khai WIDS

- Không phát hiện được các cuộc tấn công bên trong mạng không dây
- Đắc tiền
- Không tùy biến được

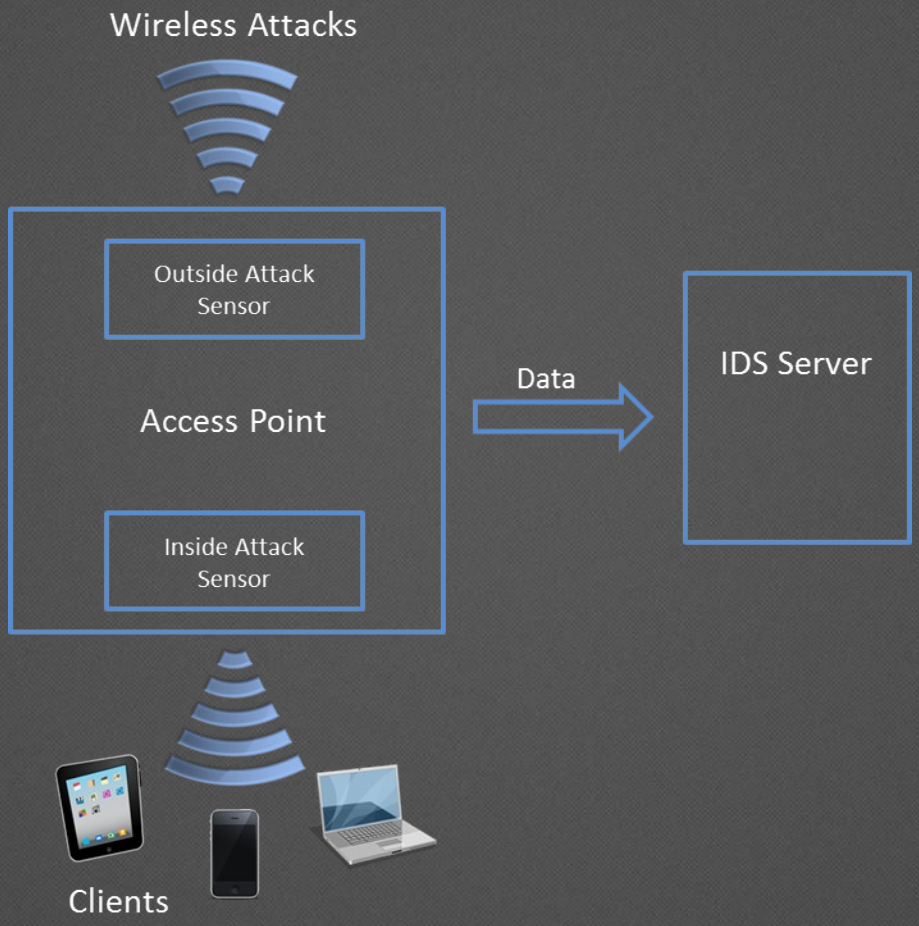
YÊU CẦU ĐẶT RA

- Xây dựng giải pháp phát hiện thâm nhập mạng cục bộ không dây với các mục tiêu
  - Có thể phát hiện được các hình thức tấn công từ bên ngoài và từ bên trong mạng không dây
  - Chi phí thấp
  - Dựa trên phần mềm nguồn mở để dễ dàng tùy biến, phát triển
  - Cảnh báo tức thì khi phát hiện xâm nhập

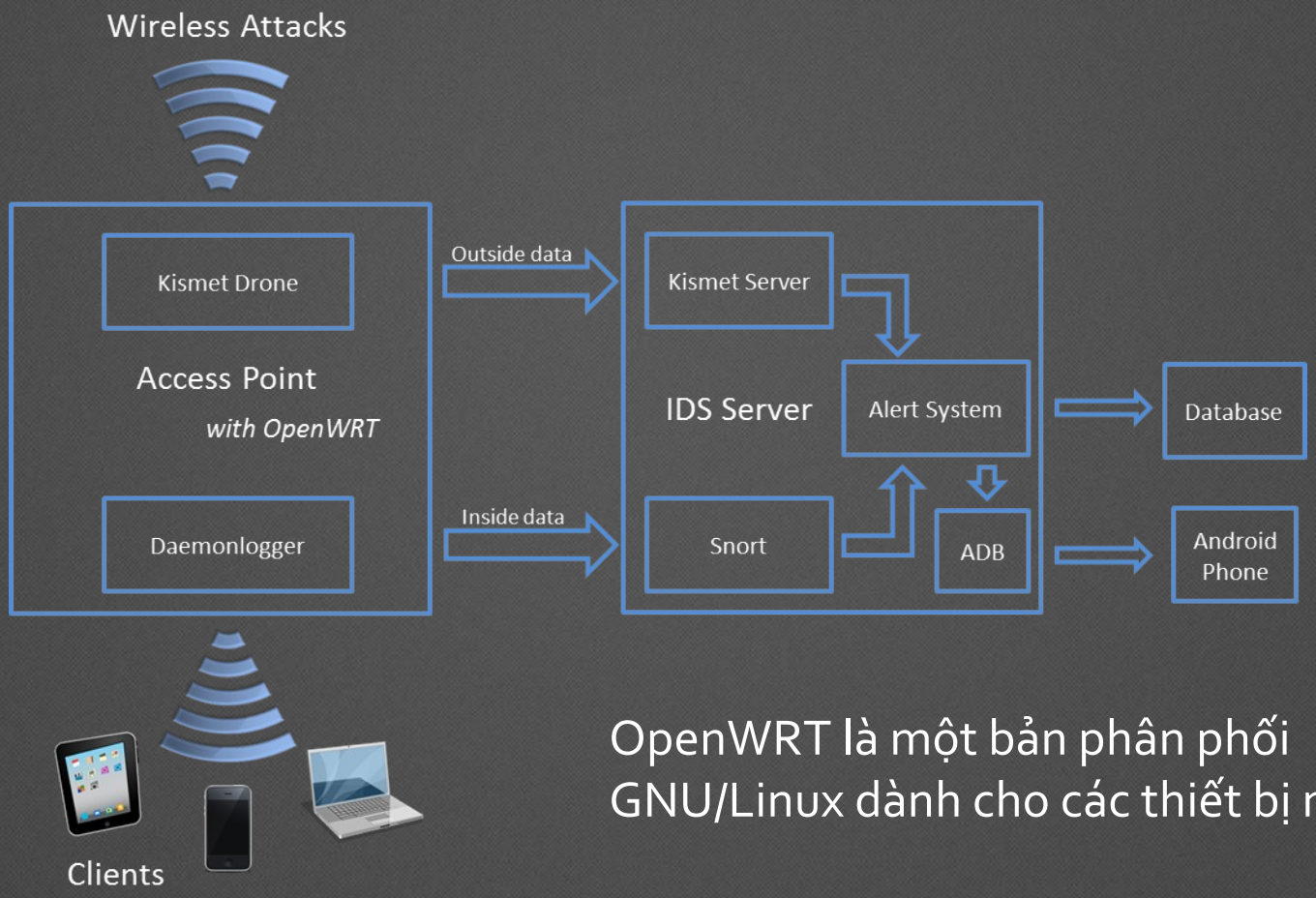
Giải pháp DIDS

Distributed Intrusion Detection System

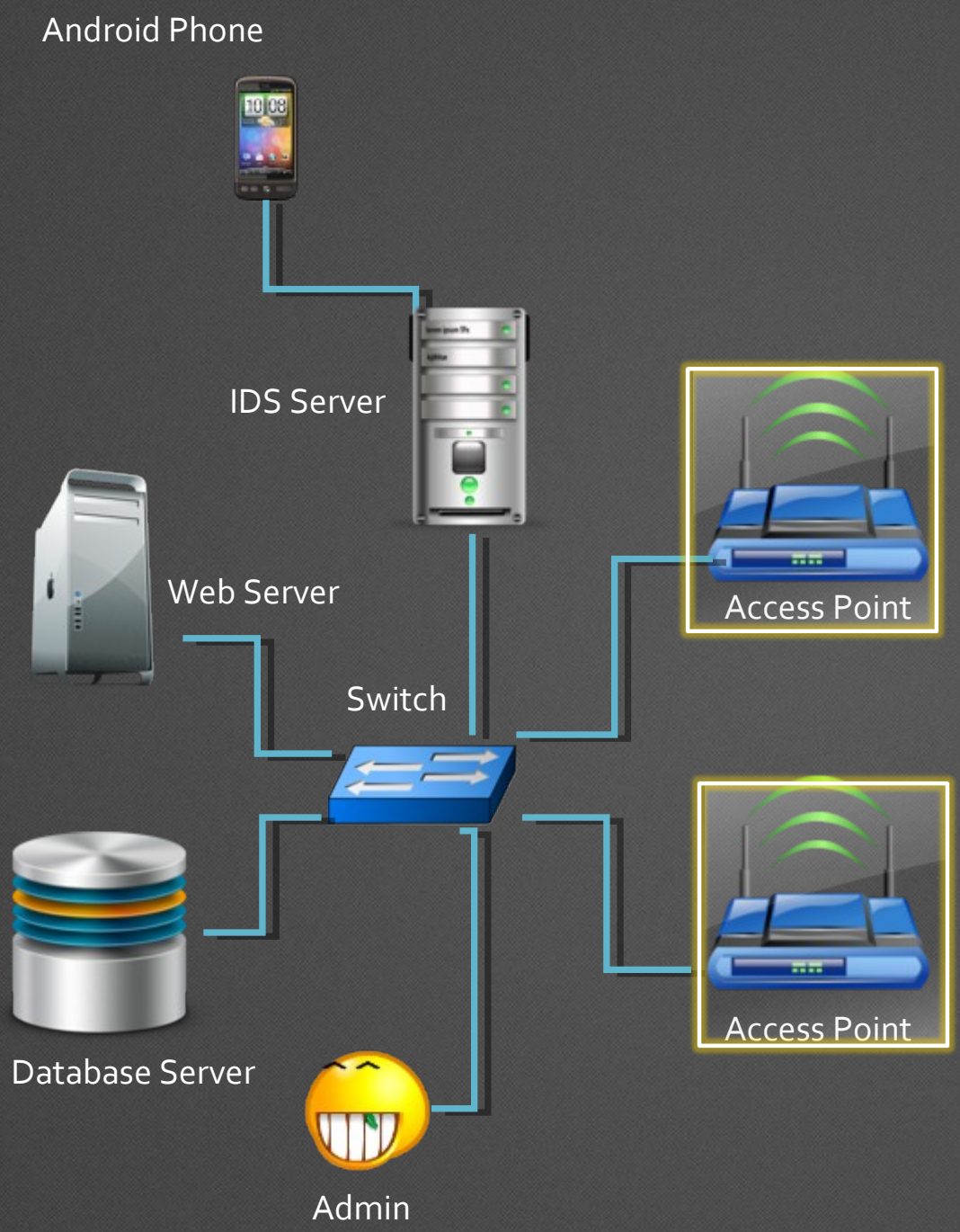
Mô hình DIDS


Wireless Attacks
Outside Attack Sensor
Access Point
Inside Attack Sensor
Data
IDS Server
Clients

Cài đặt mô hình DIDS bằng giải pháp PMNM



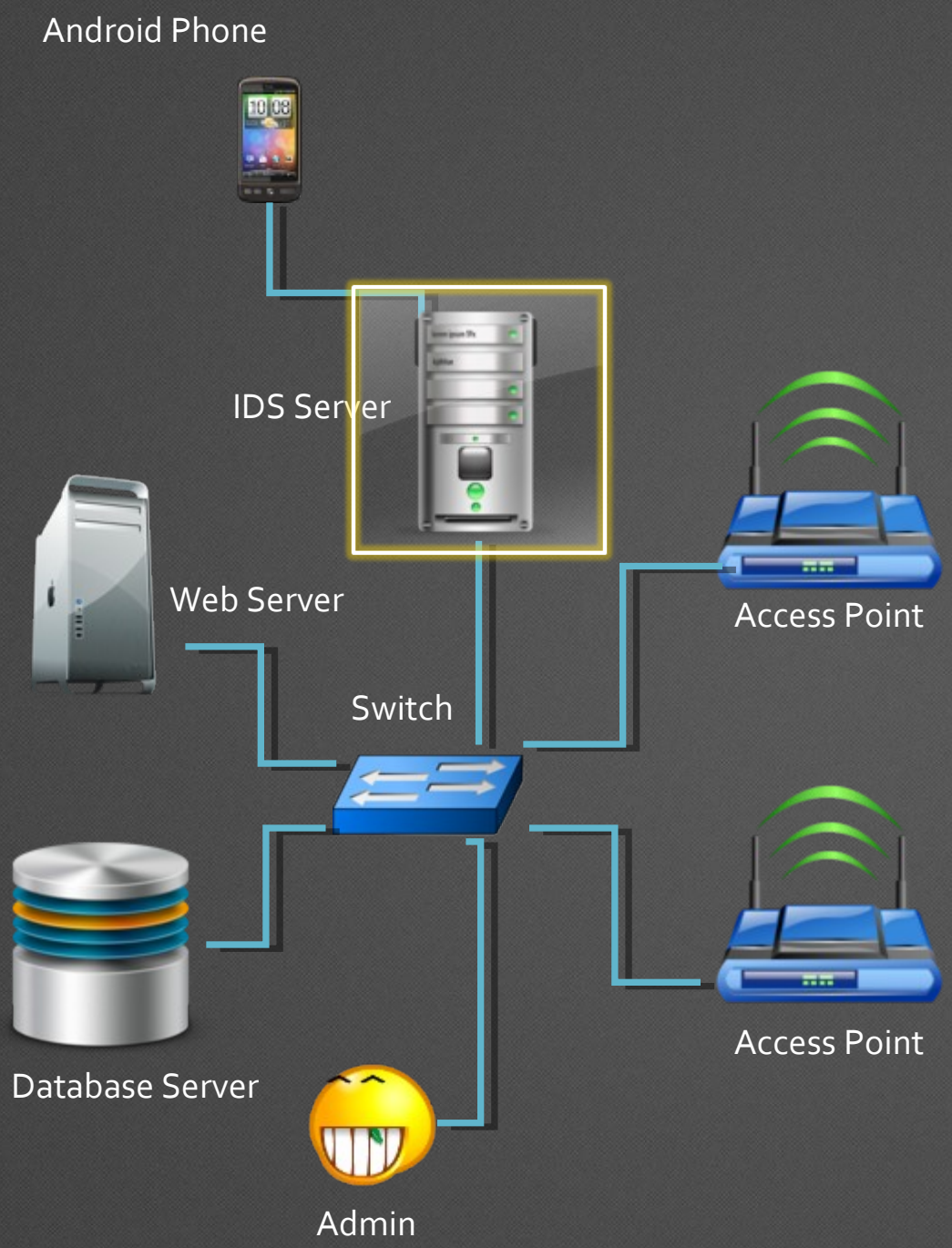
OpenWRT là một bản phân phối GNU/Linux dành cho các thiết bị nhúng



Access Point

OpenWRT

- Cung cấp kết nối
- Thu thập dữ liệu bên ngoài mạng WLAN và chuyển về IDS Server
- Gửi bản sao của các gói tin bên trong mạng WLAN về IDS Server

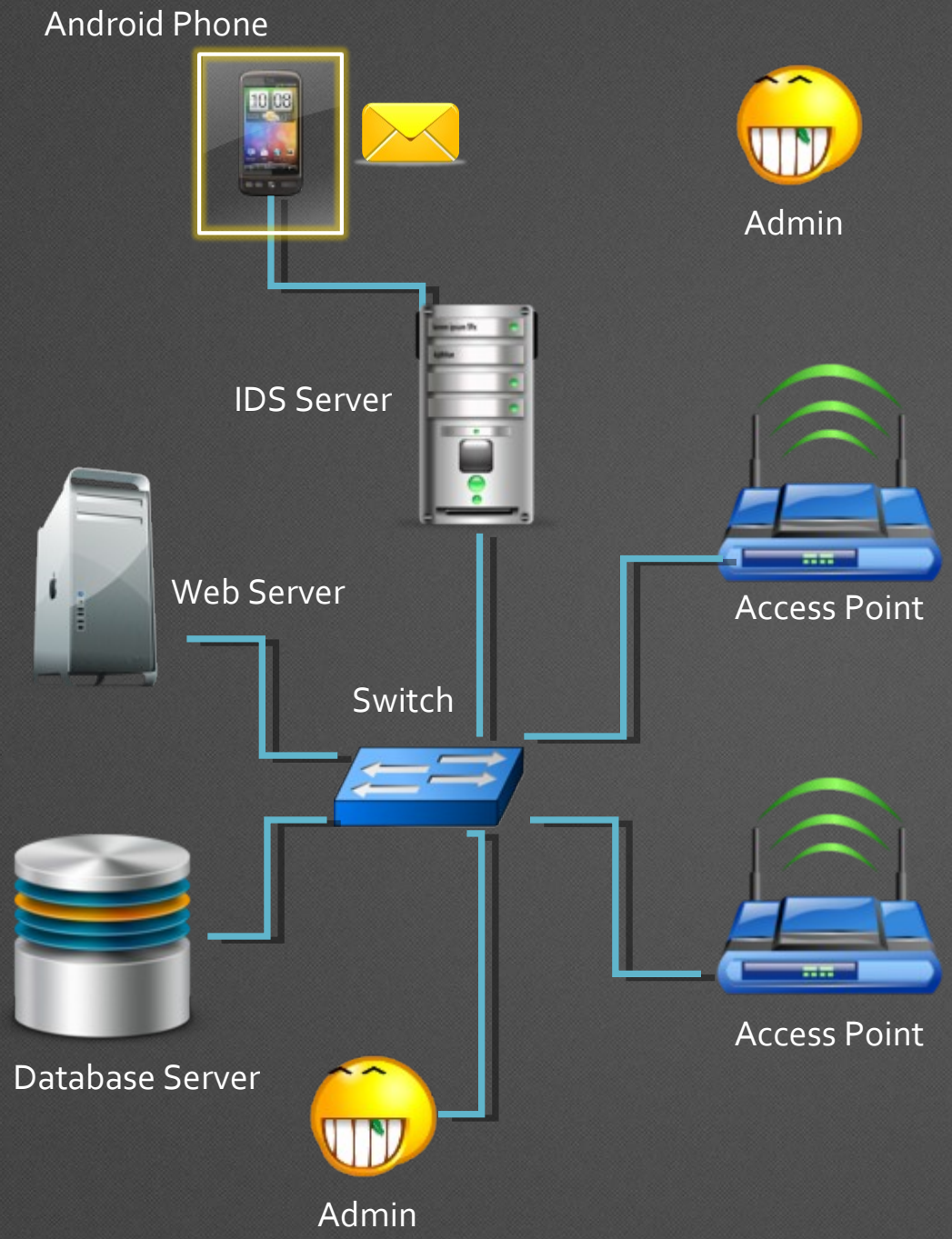


IDS Server

Ubuntu

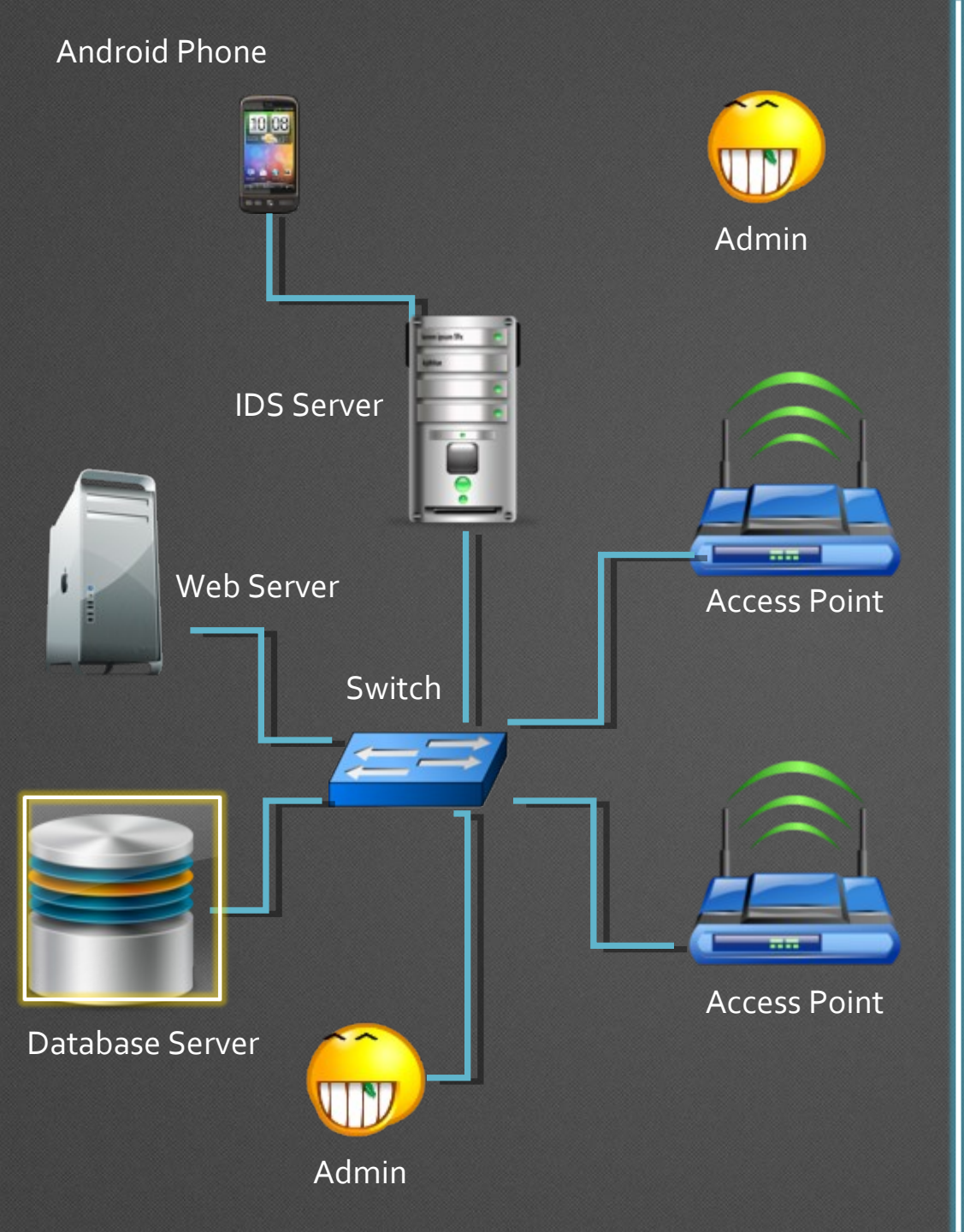
Snort Kismet

- Là thành phần xử lý chính
- Nếu phát hiện sự kiện xấu
- Yêu cầu Android Phone gửi tin nhắn cảnh báo
- Lưu thông tin vào Database Server



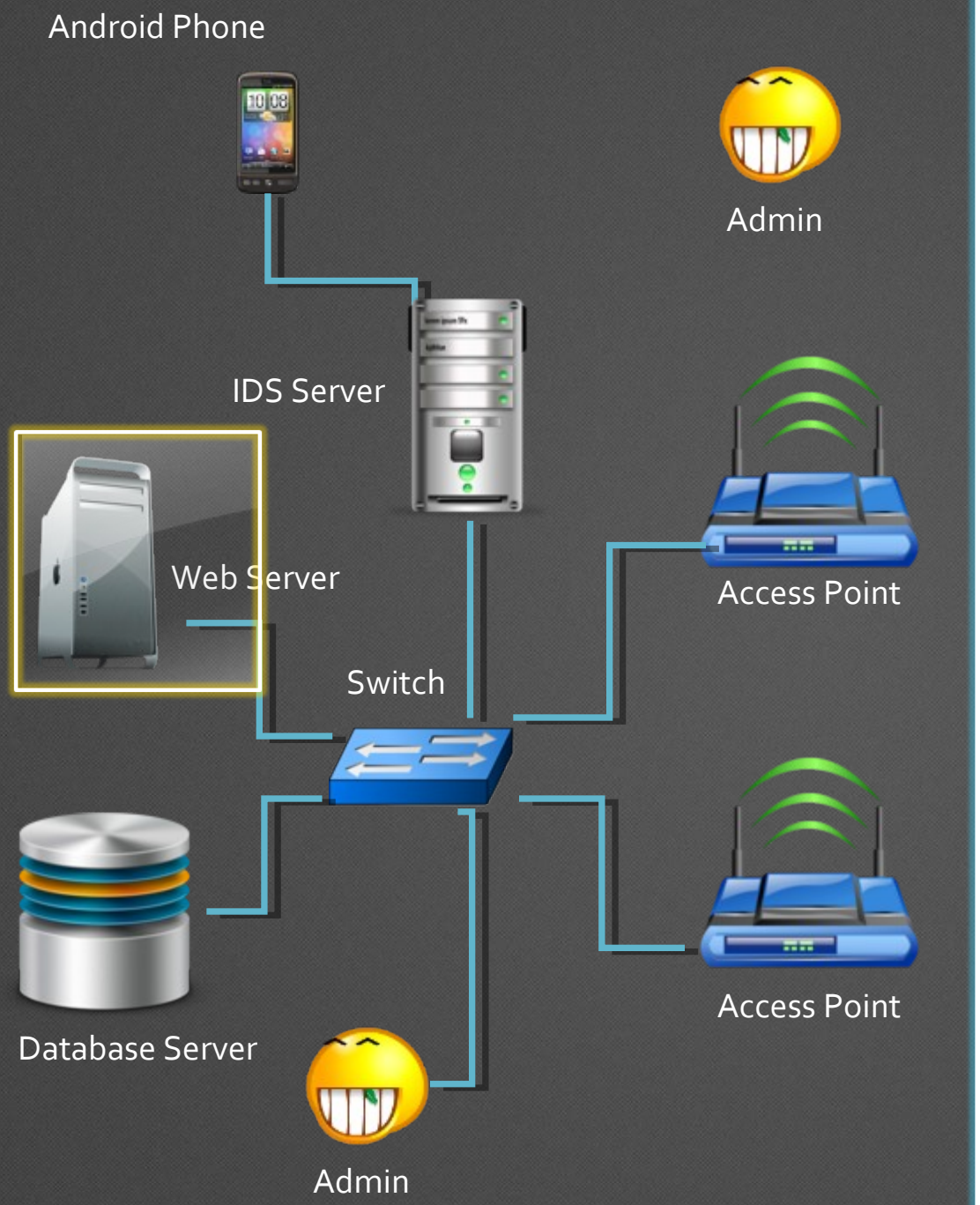
Android Phone

- Nhận yêu cầu từ IDS Server
- Gửi tin nhắn cảnh báo đến nhà quản trị



Database Server

- Lưu trữ thông tin về các sự kiện xấu
- Phục vụ cho Web Server và IDS Server



Web Server

- Cung cấp ứng dụng Web phục vụ nhà quản trị

Kết quả đạt được

Giải quyết hoàn toàn yêu cầu đặt ra

- Khắc phục hạn chế của giải pháp IDS/WIDS truyền thống
- Có thể triển khai trên các thiết bị mạng thông thường
- Dựa trên các sản phẩm phần mềm mở nguồn mở
- Chi phí triển khai thấp nhất có thể

So sánh với các giải pháp khác

Dựa trên Kismet, hỗ trợ phát hiện 21 kiểu tấn công bên ngoài khác nhau

Tên tấn công	DIDS	CUWN
AIRJACKSSID	✔	✔
APSPOOF	✔	✔
BSSTIMESTAMP	✔	✔
CRYPTODROP	✔	✔
DEAUTHFLOOD	✔	✔
BCASTDISCON	✔	✔
DHCPCLIENTID	✔	✔
DHCPCONFLICT	✔	✔
DISASSOCTRAFFIC	✔	✔
DISCONCODEINVALID	✔	✔
DEAUTHCODEINVALID	✔	✔
DHCPNAMECHANGE	✔	✔
DHCPOSCHANGE	✔	✔
LONGSSID	✔	✔
LUCENTTEST	✔	✔
MSFBCOMSSID	✔	✔
MSFDLINKRATE	✔	✔
MSFNETGEARBEACON	✔	✔
NETSTUMBLER	✔	✔
NULLPROBERESP	✔	✔
PROBENOJOIN	✔	✔

CUWN-Cisco Unified Wireless Network

So sánh với các giải pháp khác

Tên chức năng	DIDS	CUWN	Quadrant Information Security	Jason Murray
Phát hiện tấn công từ bên ngoài	Có, dựa trên Kismet	Có, tương tự Kismet	Có, dựa trên Kismet	Có, dựa trên Kismet
Phát hiện tấn công từ bên trong	Có, dựa trên Snort	Có	Có, dựa trên Snort	Không
Hỗ trợ rules để nhận diện thêm tấn công từ bên trong	Có, Snort rules	Có	Có, Snort rules	Không
Hỗ trợ cảnh báo tức thì bằng tin nhắn SMS	Có	Không	Không	Không
Hỗ trợ quản lý sự kiện với cơ sở dữ liệu	Có	Có	Có	Không
Chặn đứng gói tin xấu (IPS)	Không	Có	Không	Không
Khả năng mở rộng	Có, không ràng bởi buộc phần cứng	Không, ràng buộc phần cứng CISCO	Có, không ràng bởi buộc phần cứng	Có, không ràng bởi buộc phần cứng
Giá thành triển khai	Rất thấp	Rất cao	Rất thấp	Rất thấp

Các tính năng nổi bật DIDS

- Giám sát và phát hiện những rủi ro từ bên trong lẫn bên ngoài
- Có khả năng phản ứng chủ động với sự kiện xấu
- Tự động cảnh báo cho một hoặc nhiều nhà quản trị thông qua SMS
- Tích hợp sẵn ứng dụng Web giúp thực hiện các tác vụ cơ bản, hỗ trợ đa nền tảng hệ thống và trình duyệt.

End

Chân thành cảm ơn đã theo dõi