**Đề tài: Bảo vệ switch layer 2**

Phân chia công việc

1. **Trương Văn Trọng: (Tuần 9 )**

**Nội dung 2:** Tìm hiểu, viết tài liệu, demo tấn công, bảo vệ MAC address table overflows: làm tràn bảng MAC trên switch.

**Một phần nội dung 5:** Tìm hiểu, viết tài liệu, demo tấn công, bảo vệ DHCP attacks: tấn công DHCP bằng cách Flood Request DHCP lên DHCP Server.

1. **Nguyễn Tấn Phát: (Tuần 12)**

**Nội dung 3:** Tìm hiểu, viết tài liệu, demo tấn công, bảo vệ STP manipulation giao thức STP

**Một phần nội dung 5:** Tìm hiểu, viết tài liệu, demo tấn công, bảo vệ dựng lên một DHCP Server giả để tấn công DHCP chính.

Tổng hợp tài liệu, viết tài liệu báo cáo đồ án file word.

1. **Nguyễn Nhã Tuấn: (Tuần 10)**
2. **Lê Chí Nguyện: (Tuần 11)**
3. **Nguyễn Hữu Quốc:**

Tìm hiểu phân chia công việc phù hợp cho từng thành viên. Giám sát, quản lý nhóm, phân chia nhiệm vụ nhóm, tìm hiểu toàn bộ nội dung đề tài, tìm tài liệu phù hợp cho nhóm, hỗ trợ giải thích, demo tấn công, bảo vệ tất cả các nội dung.

Chỉnh sửa tài liệu báo cáo đồ án file word.

**Nội dung tìm hiểm cụ thể:**

# Nội dung 1. MAC address spoofing attacks: tấn công giả mạo địa chỉ MAC

==>Phương thức tấn công: Dựa trên cơ chế gửi ARP tìm kiếm khi không thấy đích.

==> Cách bảo vê: ARP Spoofing: Phần mềm phát hiện tấn công ARP

# Nội dung 2. MAC address table overflows: làm tràn bảng MAC trên switch

==> Phương thức tấn công: Tạo MAC ảo làm đầy bảng CAM của Switch

==> Cách bảo vê : Thực hiện tính năng port security trên Switch

# Nội dung 3. STP manipulation:tấn công giao thức STP

* Phương thức tấn công : Chiếm quyền trong STP
* Cách bảo vê: Thực hiện Port Fast, BPDU Guard

# Nội dung 4. VLAN attacks: tấn công VLAN

==>Tấn công bằng VLAN Hopping, VLAN Double-Tagging

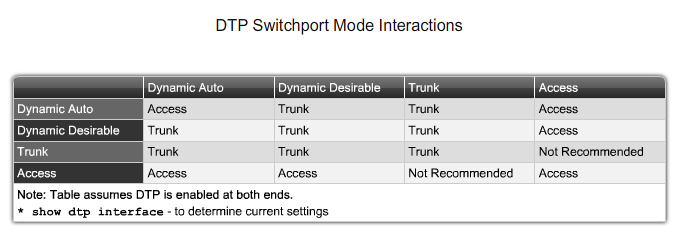
🡺 Cách bảo vệ: Vlan Trunk phải sử dụng vlan riêng với User, không sử dụng Default Vlan 1, tắt tính năng DTP (Tắt, cho port thành access), tắt tất cả các cổng không sử dụng. Chỉ cho 1 số Vlan nhất định đi qua đường Trunk, không nên cho ALL.

Đặt những interface non-trunking ở mode non-trunking vĩnh viễn mà không có sự thương lượng

Switch(config)# interface fastethernet 0/1

Switch(config-if)# switchport mode access

Switch(config-if)# switchport nonegotiate



# Nội dung 5. DHCP attacks: tấn công DHCP

==> Phương thức tấn công: Flood Request DHCP lên DHCP Server và dựng lên một DHCP Server giả.

==> Cách bảo vê :

Flood Request DHCP lên DHCP Server : Bật Port Security trên Switch access để 1 cổng chỉ được xin 1 - 2 địa chỉ IP tùy vào nhu cầu

DHCP Server giả.:Dùng Tính năng DHCP snooping, bật trust (cho offer, reply) cho DHCP, tắt trust (chỉ cho discover, request) cho các cổng khác không phải DHCP,.

# Nội dung 6. sử dụng SSH

Khi cài đặt cấu hình thiết bị từ xa: Nếu sử dụng telnet thì đổi port mặc định để giảm thiểu rủi ro, nên sử dụng SSH để cấu hình thiết bị từ xa hơn là telnet.

Slide Cisco anh đã làm gọn lại rồi, có delete vài slide không cần thiết các bạn xem lại slide nhé

1.Trọng (Tuần sau - tuần 9) Văn Trọng Slide 6->18 (Topic 2, 3, demo cấu hình bảo vệ nội dung liên quan)

2. Tuấn (Tuần 10) Nguyễn Nhã Tuấn Slide 19 -> 32 (Topic 4, 5, demo cấu hình bảo vệ nội dung liên quan)

3: Nguyện (Tuần 11) Lê Chí Nguyện Slide 26->32 và 33->37 (Topic 5, 6 + Lời khuyên bảo mật + đổi port mặc định telnet + demo cấu hình bảo vệ nội dung liên quan)

4: Phát (Tuần 12): Slide 26->32 và 38 -> 44 (Topic 5, 7, demo cấu hình bảo vệ nội dung liên quan).