Lab 1: Thực nghiệm tấn công MAC flooding

Chuẩn bị môi trường: dùng GNS3 để mô phỏng switch, tiếp theo dùng máy ảo kết nối với switch trên GNS3. Máy tấn công dùng Kali Linux và cài phần mềm macof để làm ngập bảng CAM của switch

Ví dụ lệnh macof:

macof –i [interface] –n [npacks] -s[size]

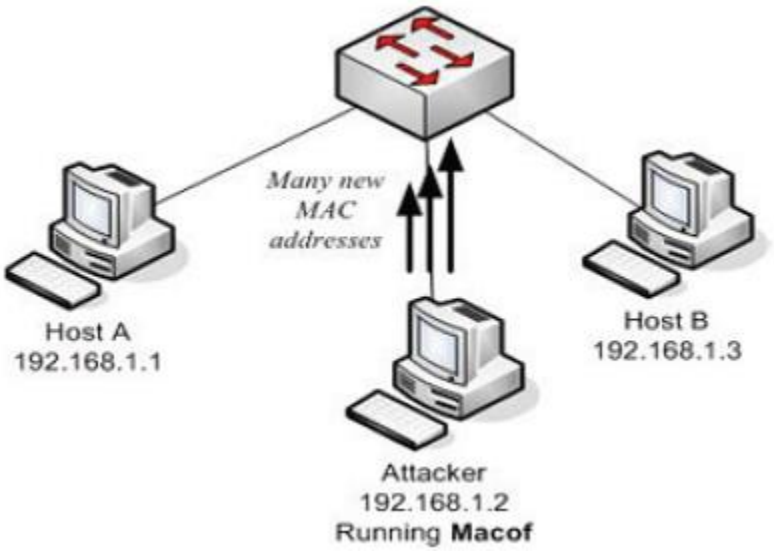
Trong đó

I là giao diện để gửi gói tin ra

N: số gói tin được gửi đi

S: kích thước gói tin (60-1514 byte)

Ví dụ sơ đồ mạng



Có 3 máy kết nối với switch với 3 địa chỉ MAC tương ứng Et0/0, Et0/1 và Et0/2

Bước 1: Máy tấn công: dùng macof gửi 100 địa chỉ giả mạo từ giao diện Et0 (dùng lệnh: macof -i eth0 -n 100)

Bước 2: Kiểm tra bảng CAM tại switch thấy có nhiều MAC giả mạo đi vào trên giao diện Et0/2 (từ máy hacker) được cập nhật trên bảng CAM

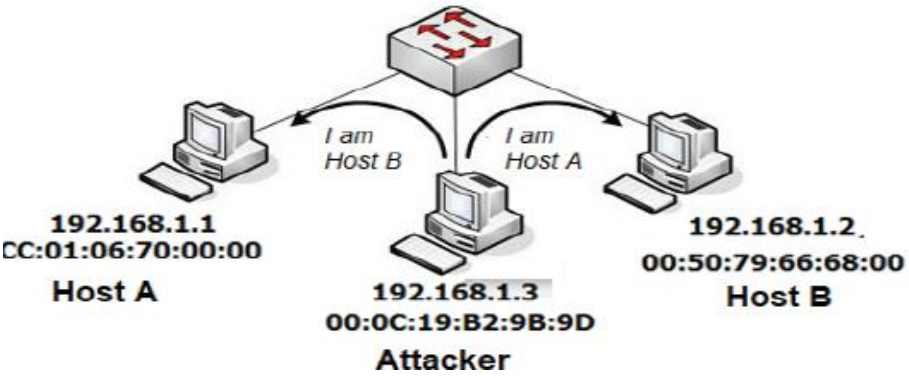
Bước 3: Ngăn chặn: bật chế độ bảo vệ port Et0/2 để giới hạn số lượng địa chỉ MAC (ví dụ tối đa =5), dùng lệnh:

```
SW#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW(config)#int e1/1
SW(config-if)#switchport mode access
SW(config-if)#switchport port-security
SW(config-if)#switchport port-security maximum 5
SW(config-if)#switchport port-security violation ?
  protect   Security violation protect mode
  restrict  Security violation restrict mode
  shutdown  Security violation shutdown mode

SW(config-if)#switchport port-security violation sh
SW(config-if)#switchport port-security violation shutdown
```

Lab 2. Tấn công ARP poisoning

Ví dụ hacker tấn công để lấy tất cả lưu lượng giữa Host A và Host B



Bước 1: Kiểm tra địa chỉ các máy đang kết nối với máy tấn công

Máy kali: arp -a

Bước 2: Cấu hình forward gói tin đến các địa chỉ IP để cho kết nối luôn được thực hiện

```
┌──(root💀kali)-[/home/kali]
└─# echo 1 > /proc/sys/net/ipv4/ip_forward

┌──(root💀kali)-[/home/kali]
└─# more /proc/sys/net/ipv4/ip_forward
1
```

Bước 3: Đầu độc bộ nhớ đệm ARP của victim để bộ nhớ đệm chứa các mục giả tạo sau

Trong cache ARP của Host A: IP_B -> MAC_Attacker

Trong cache ARP của Host B: IP_A-> MAC_Attacker

(Có thể dùng arpspoof hoặc dsniff

arpspoof [-i interface] [-t target]

Trong đó i là giao diện và t chỉ định một máy cụ thể để đầu độc ARP)

Bước 4: Tại máy tấn công sẽ gửi đến Host A và Host B các phản hồi ARP giả mạo với ánh xạ sai

IP-A-> MAC-Attacker và IP-B -> MAC-Attacker

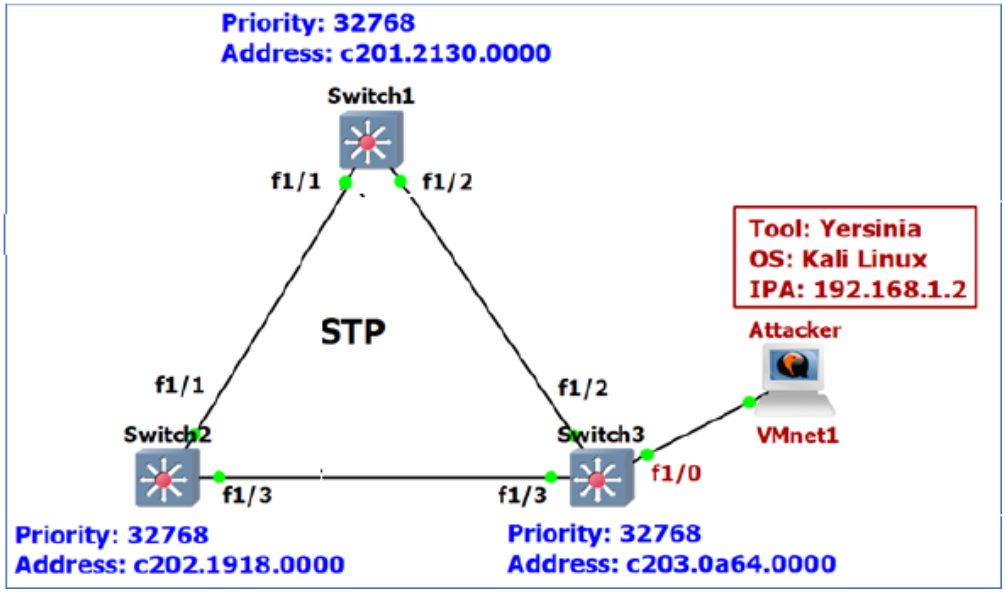
Bước 5: Dùng wireshark bắt gói tin tại máy tấn công sẽ thấy IP của Host A và Host B có MAC của máy tấn công

Bước 6: Ping từ Host A sang Host B sẽ thấy traffic đi về phía máy tấn công (bắt bằng wireshark)

Lab 3: Tấn công STP Spoofing để chiếm quyền Root Bridge

Chuẩn bị môi trường: dùng GNS3 để mô phỏng các thiết bị switch kết nối với nhau

Máy tấn công chạy Kali linux kết nối với port f1/0 trên Switch 3, cài phần mềm Yersinia



Bước 1: Máy tấn công gửi thông điệp BPDU để bầu cử lại Root Bridge với Bridge ID nhỏ hơn Root Bridge hiện tại và nó chiếm Rood Bridge.

Trước tấn công, switch 1 là Root Bridge, dùng lệnh *sh spaning-tree vlan 1 br* để kiểm tra

switch 2 (cổng f1/1 và f1/3) ở trạng thái forwarding (hoạt động bình thường), switch 3 (cổng f1/3) ở trạng thái blocked, cổng f1/0 kết nối với máy tấn công (kali linux).

Bước 2: Máy tấn công sử dụng Yersinia, chọn STP, "Claiming Root Role" để tấn công

Sau đó máy tấn công trở thành Root Bridge với Root ID chuyển từ địa chỉ switch 1 sang địa chỉ máy tấn công

Bước 3: Kiểm tra bằng lệnh *sh spaning-tree vlan 1 br*

Tại switch 1 có cảnh báo STP Root mới của VLAN 1 (địa chỉ của máy tấn công) on port Fa1/2, cost 57, như vậy switch 1 mất quyền Root Bridge

Bước 4: Khắc phục bằng cách cấu hình BPDU Guard kết hợp với PortFast cho cổng f1/0 trên switch 3. Khi có dấu hiệu tấn công, cổng f1/0 sẽ bị đóng.

Lab 4. Tấn công STP DoS

Tấn công bằng cách sử dụng BPDU giả mạo để tiêu tốn tài nguyên của switch, ví dụ tấn công vào switch 3. Kiểm tra dung lượng tại switch 3 bằng lệnh *sh proc cpu | incl seconds*

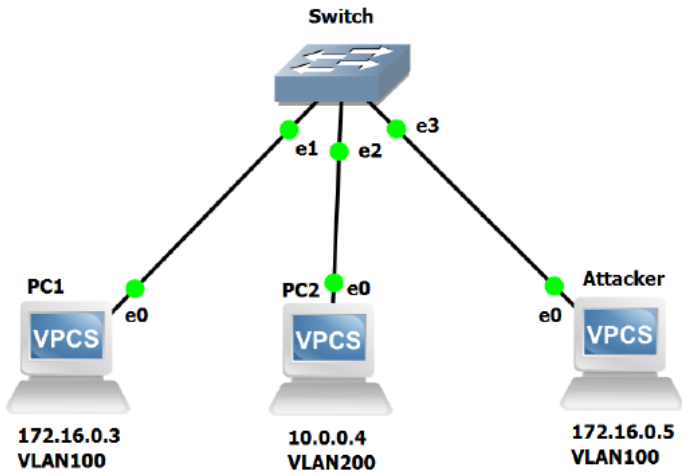
Dùng lệnh *sh spanning-tree interface FastEthernet 1/0* để thấy Số lượng BPDU nhận được là 0

Bước 1: tấn công dùng Yersinia từ máy tấn công, chọn STP, "sending conf BPDUs", khi đó một lượng lớn BPDU được gửi liên tục đến switch3 qua cổng f1/0

Bước 2: dùng 2 lệnh trên để kiểm tra dung lượng và BPDU

Lab 5. Tấn công VLAN

Giả mạo switch và bật trunking. Sơ đồ thực nghiệm



Chuẩn bị môi trường: Dùng GNS3 để mô phỏng các thiết bị Switch và máy tính kết nối với nhau. Trên Switch chia 2 VLAN, dùng 2 PC để gắn vào 2 VLAN.

- Máy tấn công kết nối với Switch, chạy trên Kali Linux, cài phần mềm Yersinia. Trong kịch bản này, hacker sẽ truy cập vào mạng VLAN 100 - cùng VLAN với PC1 và tấn công có thể ping được PC2 với VLAN200. Sau tấn công, kẻ tấn công sẽ ping được tới PC2 ở VLAN200.

- Kiểm tra trên Switch có 2 VLAN và trạng thái của VLAN trên Switch: lệnh show vlan

- Cấu hình Dynamic Desirable trên switch

- Bật dtp để xem các gói tin DTP - Dynamic Trunking Protocol gửi tới dùng lệnh: #debug dtp events

- Tại máy tấn công: dùng Yersinia để thực hiện tấn công. Bật Trunking

- Tại Switch: thấy trạng thái cổng Gi0/0 đã bị thay đổi thành “trunk”

- Các VLAN trên Switch được di chuyển trên cổng Gi0/0

- Trên máy tấn công, thực hiên thêm một giao diện VLAN mới và đặt ID = 200, sau đó gán một IP mới cùng IP với PC2 trong VLAN200 cho giao diện VLAN mới