Bài: 8.2 Nghe trộm - ARP Poisoning, Tấn công Spoofing,Thiết lập địa chỉ MAC, DNS Poisoning,Wireshark

Xem bài học trên website để ủng hộ Kteam: 8.2 Nghe trộm - ARP Poisoning, Tấn công Spoofing,Thiết lập địa chỉ MAC, DNS Poisoning,Wireshark

Mọi vấn đề về lỗi website làm ảnh hưởng đến bạn hoặc thắc mắc, mong muốn khóa học mới, nhằm hỗ trợ cải thiện Website. Các bạn vui lòng phản hồi đến Fanpage How Kteam nhé!

ARP Poisoning

Giao thức phân giải địa chỉ (ARP)

ARP là một giao thức không quốc tịch sử dụng trong miền truyền tin để đảm bảo truyền thông bằng cách phân giải địa chỉ IP thành ánh xạ địa chỉ MAC. Nó hỗ trợ ánh xạ địa chỉ **L2** và **L3**.

ARP bảo đảm kết nối giữa địa chỉ MAC và địa chỉ IP. Bằng cách truyền đi ARP yêu cầu cùng với địa chỉ IP, switch sẽ biết được thông tin về địa chỉ MAC kết nối từ phản hồi của host. Trong trường hợp không có hoặc không tìm được ánh xạ, nguồn sẽ gửi bản tin đến tất cả các nodes. Chỉ có node với địa chỉ MAC kết hợp với IP đó phản hồi yêu cầu, chuyển tiếp gói tin chứa ánh xạ địa chỉ MAC. Switch sẽ ghi nhớ địa chỉ MAC và thông tin về port kết nối vào bảng CAM cố định độ dài.

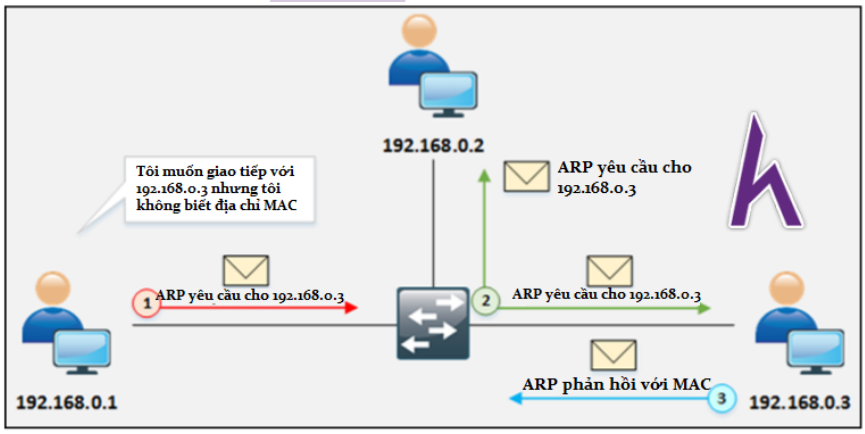

Figure 8-10 ARP Operation

Như đã thấy ở hình trên, nguồn tạo ra **ARP** yêu cầu bằng cách gửi một gói tin ARP. Một node có địa chỉ MAC nhận được yêu cầu sẽ phản hồi lại gói tin. Frame sẽ tràn ra tất cả các port (trừ port nhận frame) nếu đầu vào bảng CAM quá tải. Điều này cũng xảy ra khi địa chỉ MAC đích trong frame là địa chỉ truyền tin.

Kĩ thuật **MAC flooding** được dùng để chuyển switch thành một hub, trong đó switch bắt đầu truyền gói tin. Trong trường hợp này, user có thể lấy gói tin không dành cho mình.

Tấn công ARP Spoofing

Trong tấn công này, kẻ tấn công gửi gói tin ARP giả qua mạng LAN. Swicth sẽ cập nhật địa chỉ MAC của kẻ tấn công với địa chỉ IP của user hoặc server chính thống. Sau đó, switch sẽ chuyển tiếp gói tin đến kẻ tấn công do nhận định đó là MAC của user. Tấn công **ARP Spoofing** giúp kẻ tấn công lấy thông tin trích rút từ gói tin. Bên cạnh đó, tấn công này còn được dùng để:

- Session Hijacking
- Tấn công từ chối dịch vụ
- Tấn công man-in-the-middle
- Nghe trộm gói tin
- Chặn bắt thông tin

- Connection Hijacking
- VoIP tapping
- Đặt lại kết nối
- Đánh cắp mật khẩu

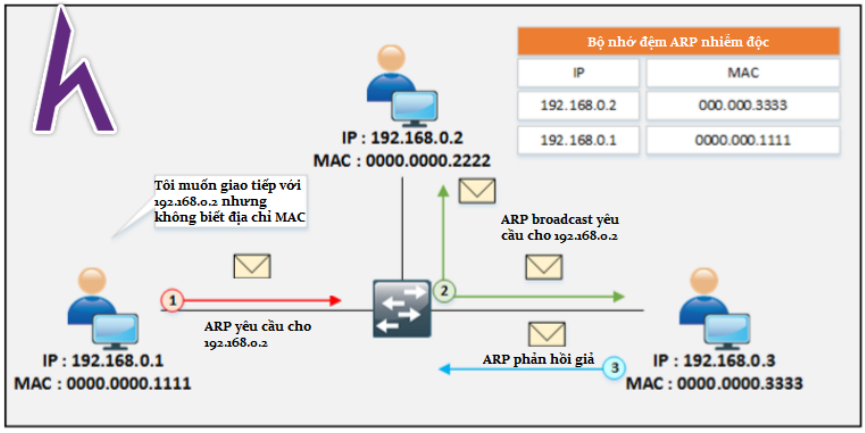

Figure 8-11 ARP Spoofing Attack

Chống lại tấn công ARP Poisoning

Thăm dò ARP động (DAI)

DAI được thực hiện với **DHCP Snooping**. Kết nối IP và MAC là một rãnh ghi từ **DHCP** giao tác để đề phòng **ARP Poisoning**. Để xây dựng kết nối IP và MAC cho xác thực DAI cần **DHCP Snooping**.

Thiết lập **DHCP Snooping** và thăm dò ARP động trên **Cisco Switches**

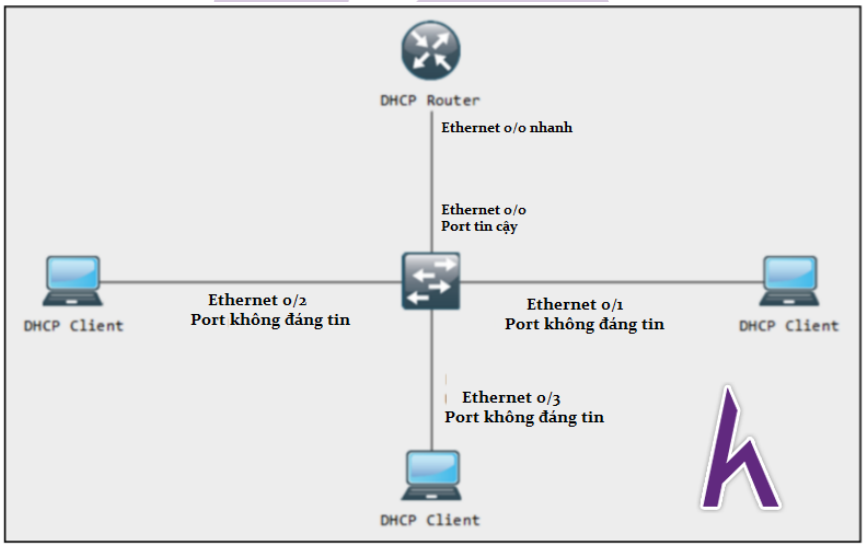

Figure 8-12 Configuring DHCP Snooping

Thiết lập

:

```
Switch>en
Switch#config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#ip dhcp snooping
Switch(config)#ip dhcp snooping vlan 1

Switch(config)#int eth 0/0
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#ex
Switch(config)#

Switch(config)#int eth 0/1
Switch(config-if)#ip dhcp snooping information option  allow-untrusted

Switch(config)#int eth 0/2
Switch(config-if)#ip dhcp snooping information option  allow-untrusted

Switch(config)#int eth 0/3
Switch(config-if)#ip dhcp snooping information option  allow-untrusted
```

Xác thực

:

```
Switch# show ip dhcp snooping
```

Bảng trên cho thấy giao diện đáng tin và không đáng tin cùng với những lựa chọn.

Thiết lập thăm dò ARP động

:

```
Switch(config)# ip arp inspection vlan <vlan number>
```

Lệnh xác thực

:

```
Switch(config)# do show ip arp inspection
```

Tấn công Spoofing

MAC Spoofing/Duplicating (sao chép MAC)

MAC Spoofing là kĩ thuật điều chỉnh địa chỉ MAC để giả dạng người dùng chính thống hoặc tạo tấn công như từ chối dịch vụ. Như chúng ta đã biết, địa chỉ MAC được thiết lập cố định trên bộ kiểm soát giao diện người dùng, tuy nhiên một số driver cho phép thay đổi địa chỉ MAC. Quy trình giả mạo địa chỉ MAC được gọi là **MAC Spoofing**. Kẻ tấn công nghe trộm địa chỉ MAC kích hoạt trên **switch port** của người dùng và sao lại. Sao lại địa chỉ MAC hướng giao thông mạng đến kẻ tấn công thay vì địa điểm ban đầu.

Lab 8-1: Thiết lập địa chỉ MAC được quản lí cục bộ

Quy trình

1. Đến **Command Prompt** và nhập dòng lệnh

> **C:\> ipconfig/all**

Quan sát địa chỉ MAC hiện hành được bộ điều hợp mạng sử dụng.

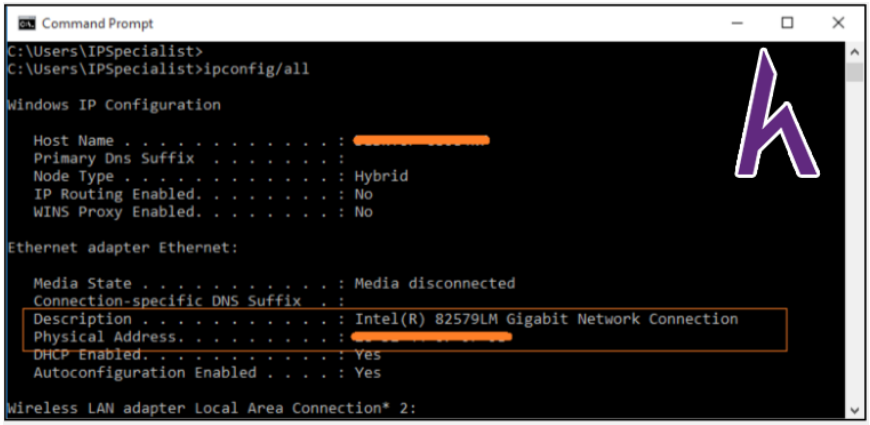

Figure 8-14 Finding MAC Address

2. Đến **Control Panel** và click vào **Hardware and Sounds**.

3. Click vào **Device Manager**.

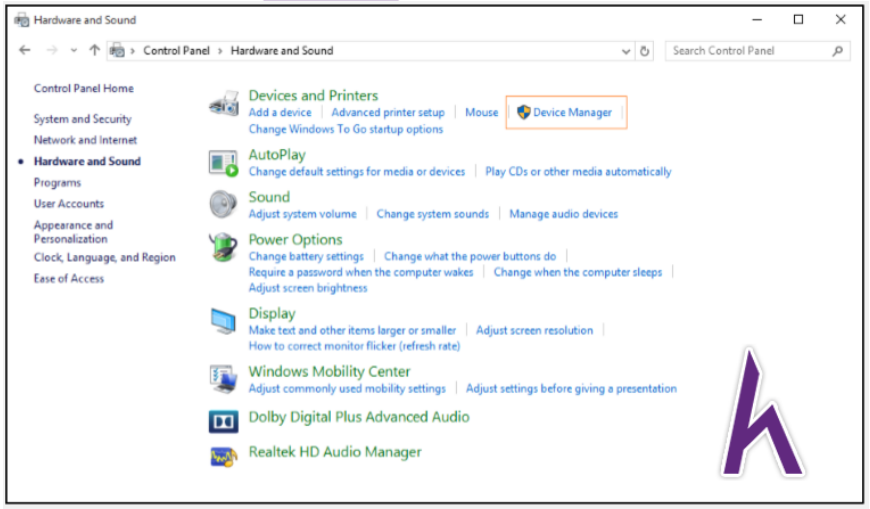

Figure 8-16 Hardware and Sounds

4. Chọn bộ điều hợp mạng (**Network Adapter**).

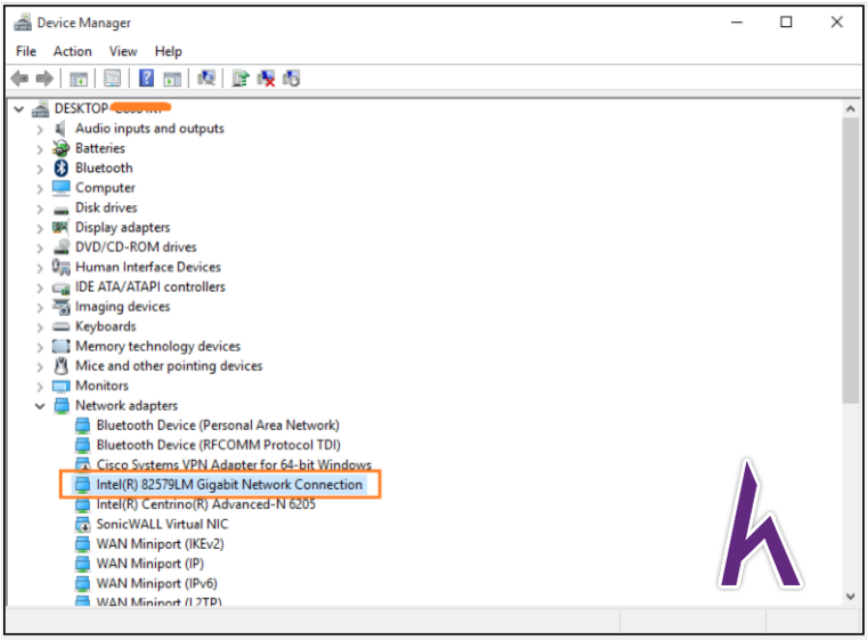

Figure 8-17 Device Manager

5. Click chuột phải vào bộ điều hợp mạng và chọn **Properties**.

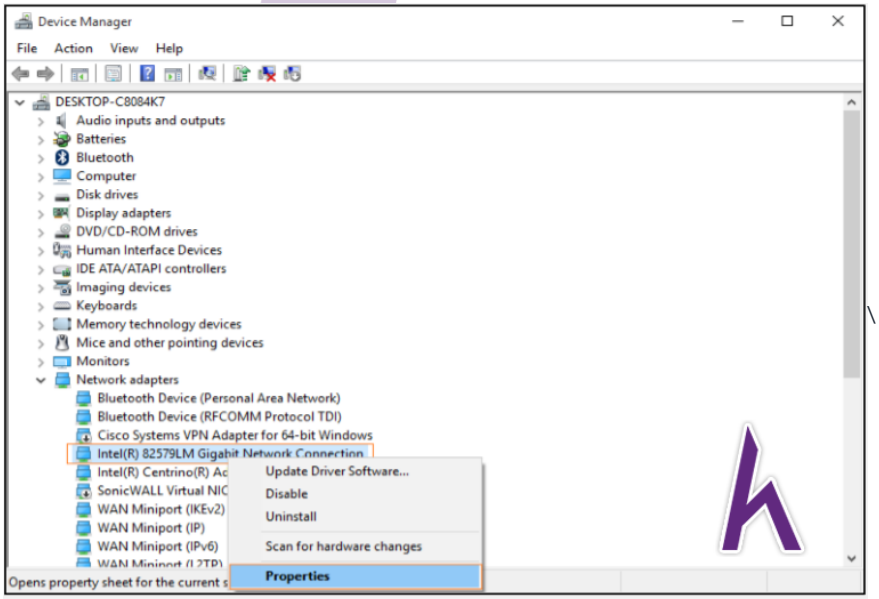

Figure 8-18 Network Adapters

6. Click vào **Advanced**.
7. Chọn **Locally Administered Address**.
8. Nhập một địa chỉ **MAC**.

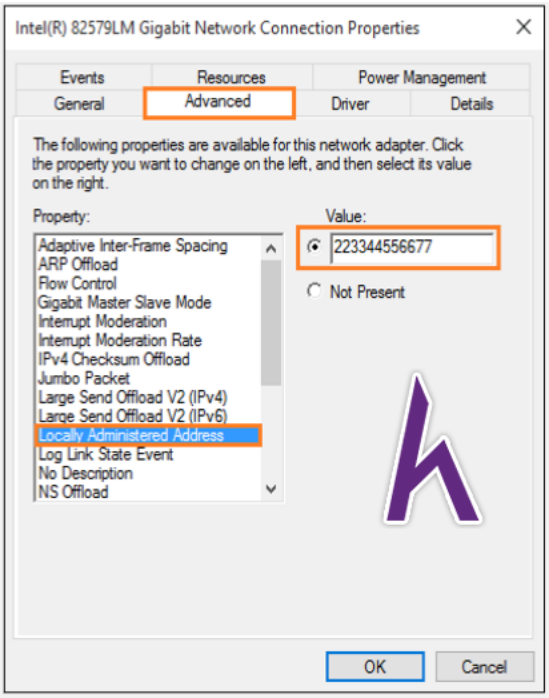

Figure 8-19 Network Adapter Properties

Xác thực

Để xác thực, vào **Command Prompt** và nhập dòng lệnh sau

```
C:\> ipconfig/all
```

Công cụ MAC Spoofing

Có rất nhiều công cụ hỗ trợ **MAC Spoofing** dễ dàng. Một số công cụ phổ biến:

- Technitium MAC address Changer
- SMAC

Cách chống lại MAC Spoofing

DHCP Snooping và thăm dò ARP động là những kĩ thuật hiệu quả để giảm thiểu tấn công **MAC Spoofing**. Bên cạnh đó, tính năng bảo vệ nguồn được thiết lập trên client đối với **Switch port**.

Bảo vệ nguồn IP là một tính năng trên port giúp lọc địa chỉ IP nguồn ở Layer 2. Tính năng này và quan sát và ngăn chặn mạo danh host chính thống. Host ác ý bị giới hạn với địa chỉ IP đã định sẵn. Bảo vệ nguồn sử dụng **DHCP Snooping** động hay kết buộc nguồn IP tĩnh để gắn địa chỉ IP với host trên port truy cập không đáng tin cậy ở Layer 2.

Ban đầu, tất cả các loại giao thông IP vào đều bị chặn trừ gói tin DHCP. Khi client nhận địa chỉ IP từ **DHCP server**, hay kết buộc nguồn IP tĩnh từ quản lí, giao thông với địa chỉ IP chỉ định được cho phép. Tất cả các gói tin giả đều bị từ chối. Bảo vệ nguồn ngăn chặn tấn công trong trường hợp mạo danh địa chỉ IP host gần gũi. Bảo vệ nguồn tạo ra một danh sách kiểm soát truy cập port ngầm (PACL).

DNS Poisoning

Kĩ thuật DNS Poisoning

Hệ thống tên miền (DNS) được sử dụng trong hệ thống mạng để dịch tên miền thành địa chỉ IP. Khi một DNS server nhận được yêu cầu, nó không có đầu vào, nó sẽ tạo lệnh hỏi bản dịch cho một DNS server khác. DNS server có bản dịch sẽ phản hồi với DNS yêu cầu, sau đó lệnh hỏi được giải quyết.

Trong trường hợp nhận được đầu vào sai, DNS server sẽ cập nhật dữ liệu của nó. Để hoạt động tốt hơn, DNS server tạo ra một bộ nhớ đệm để cập nhật đầu vào, từ đó giải quyết lệnh hỏi nhanh hơn. Đầu vào sai tạo ra sai sót trong bản dịch DNS cho đến khi bộ nhớ đệm hết hạn. DNS poisoning được thực hiện để hướng giao thông mạng đến thiết bị của kẻ tấn công.

Intranet DNS Spoofing

Intranet DNS Spoofing thường được thực hiện trong mạng LAN với Switced Network. Với sự hỗ trợ của kĩ thuật ARP poisoning, kẻ tấn công sẽ triển khai Intranet DNS Spoofing. Kẻ tấn công nghe trộm gói tin, trích rút ID của yêu cầu DNS và phản hồi bằng bản dịch IP sai để hướng giao thông đến mình. Kẻ tấn công phải hành động nhanh chóng trước khi DNS server chính thống giải quyết lệnh hỏi.

Internet DNS Spoofing

Internet DNS Spoofing được thực hiện bằng cách thay thế thiết lập DNS trên máy mục tiêu. Tất cả lệnh hỏi DNS được hướng đến DNS server ác ý mà kẻ tấn công điều khiển. Internet DNS Spoofing thường được thực hiện nhờ triển khai Trojan hay sửa đổi thiết lập DNS để chuyển hướng giao thông mạng.

Proxy Server DNS Poisoning

Giống như Internet DNS Spoofing, **Proxy Server DNS poisoning** được triển khai bằng cách thay thế thiết lập DNS từ trình duyệt web của mục tiêu. Tất cả lệnh hỏi sẽ được hướng đến server ác ý để hướng giao thông mạng đến thiết bị của kẻ tấn công.

DNS Cache Poisoning

Như chúng ta biết, người dùng Internet sử dụng DNS của nhà cung cấp dịch vụ internet (ISP). Trong hệ thống, những tổ chức sử dụng DNS Server của mình để cải thiện hoạt động bằng cách ghi bộ nhớ đệm thường xuyên. **DNS Cache poisoning** được thực hiện nhờ khai thác sai sót trong phần mềm DNS. Kẻ tấn công thêm hay chỉnh sửa đầu vào bộ nhớ đệm DNS, từ đó hướng giao thông mạng đến site ác ý. Khi Internal DNS server không thể xác nhận tính hợp lệ của phản hồi DNS từ DNS server có thẩm quyền, nó cập nhật đầu vào cục bộ để giải quyết yêu cầu của user.

Cách ngăn chặn DNS Spoofing

Công cụ nghe trộm

Wireshark

Wireshark là máy phân tích giao thức mạng phổ biến nhất, được sử dụng rộng rãi trong các tổ chức chính phủ, phi chính phủ, thương mại cũng như giáo dục. Nó là công cụ miễn phí dành cho Windows, Linux, MAC, BSD, Solaris và nhiều nền tảng khác. Wireshark cũng phát hành phiên bản cuối gọi là "TShark."