TẤN CÔNG & PHÒNG THỦ HỆ THỐNG

Module 6. Sniffing

1. Tổng quan
2. Một số kỹ thuật nghe lén và biện pháp phòng chống
3. Kỹ thuật phát hiện nghe lén

1. Tổng quan
2. Một số kỹ thuật nghe lén và biện pháp phòng chống
3. Kỹ thuật phát hiện nghe lén

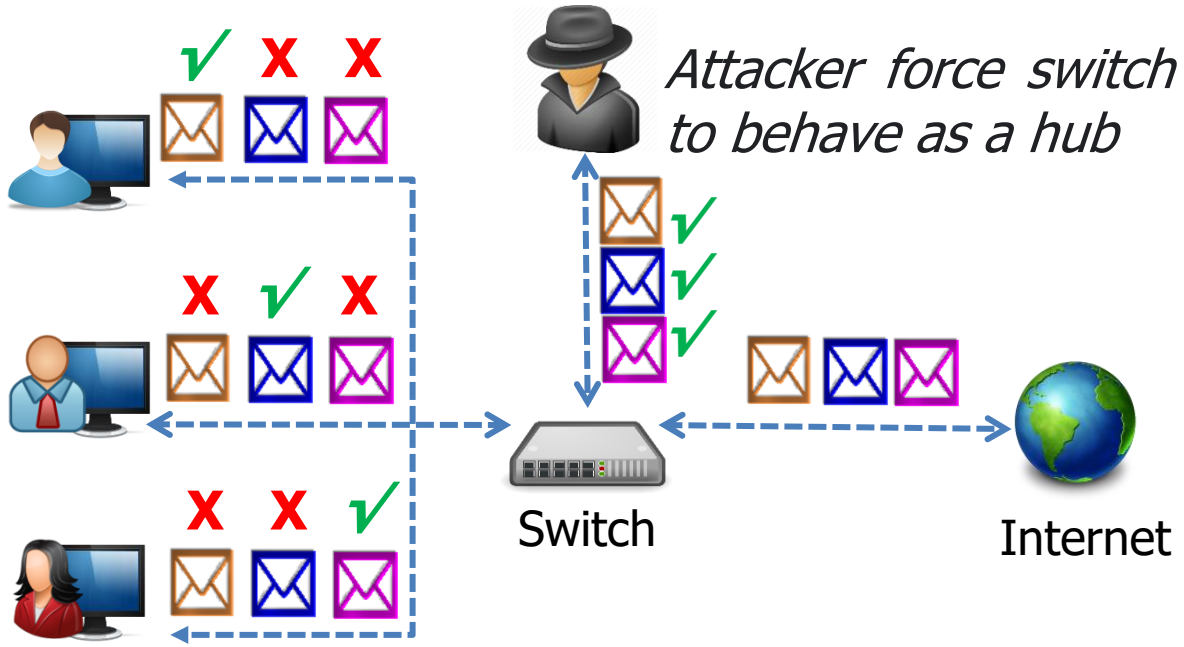
Network Sniffing

Packet Sniffing

- "Packet Sniffing" là quá trình theo dõi và bắt tất cả các gói dữ liệu đi qua một mạng nhất định bằng ứng dụng phần mềm hoặc thiết bị phần cứng.
- Nó cho phép attacker quan sát và truy cập toàn bộ lưu lượng dữ liệu mạng từ một điểm cho trước từ đó có thể thu thập được các thông tin nhạy cảm được truyền đi mà không sử dụng mã hóa

How a sniffer work?

- Sniffer chuyển NIC của hệ thống sang "promiscuous mode" để nó lắng nghe tất cả dữ liệu được truyền trên phân đoạn mạng của nó.



Type of Sniffing

Passive Sniffing

- Passive sniffing đề cập đến việc sniffing thông qua hub, khi đó lưu lượng được gửi đến tất cả các cổng.
- Nó giám sát toàn bộ các gói tin trong mạng không cần gửi bất kỳ gói tin bổ sung nào do đó passive sniffing trong suốt với người dùng.
- Trong một mạng sử dụng hub, mọi host đều nhìn thấy tất cả lưu lượng vì vậy các mạng hiện đại hiện nay đều sử dụng switches.

Active Sniffing

- Active sniffing được sử dụng để sniff mạng dựa trên switch.
- Active sniffing tiêm các gói ARP vào mạng để làm tràn bảng CAM.

Active Sniffing Techniques

- MAC Flooding
- DNS Poisoning
- ARP Poisoning
- DHCP Attacks
- Switch Port Stealing
- Spoofing Attack

How an Attacker Hacks the Network Using Sniffer

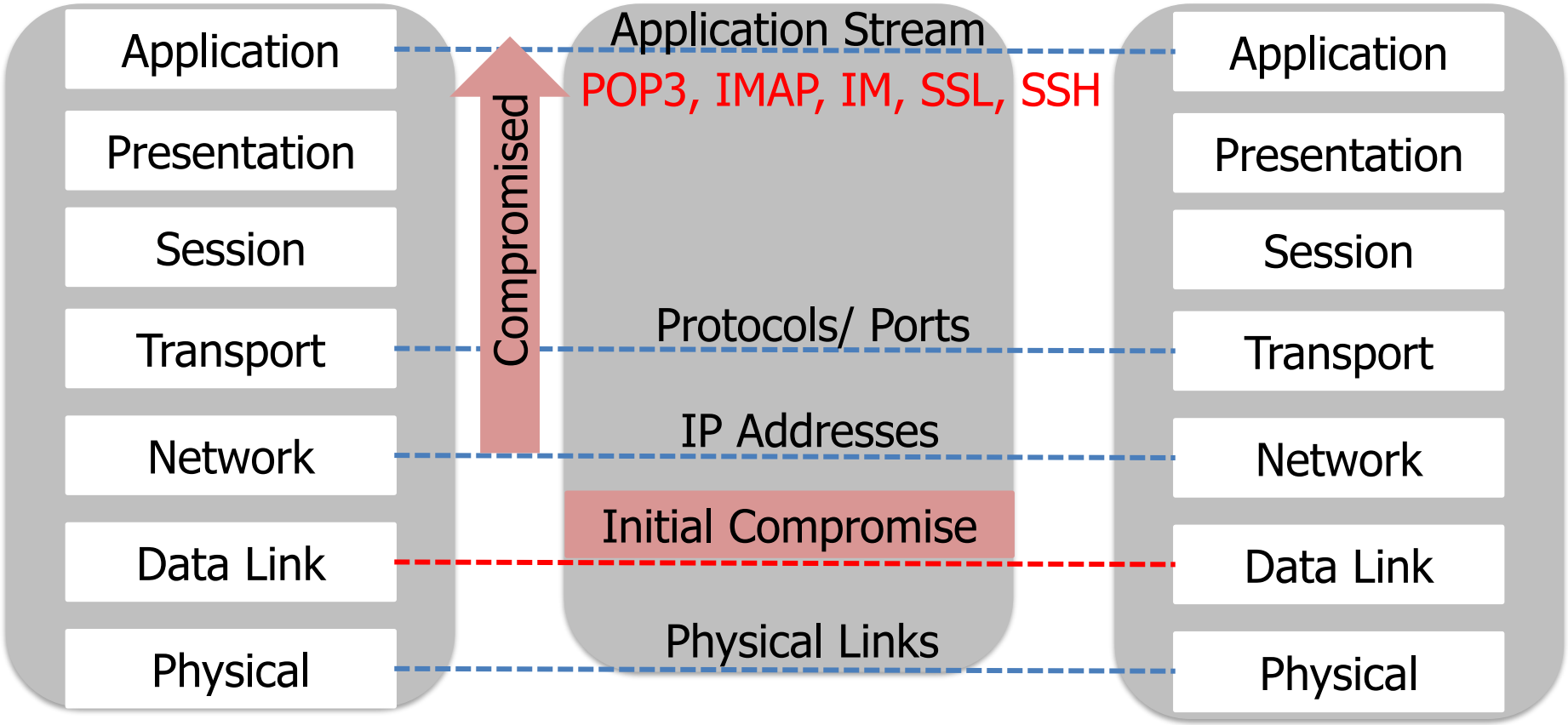
1. Attacker kết nối NIC trên máy tính của mình tới một cổng trên switch.
2. Attacker chạy các công cụ dò quét để tìm hiểu về cấu trúc mạng.
3. Attacker xác định máy nạn nhân.
4. Attacker đầu độc máy nạn nhân bằng cách sử dụng các kỹ thuật "ARP spoofing".
5. Lưu lượng dành cho máy nạn nhân được chuyển hướng đến attacker.
6. Attacker trích xuất thông tin nhạy cảm từ lưu lượng truy cập được chuyển hướng.

Protocols Vulnerable to Sniffing

- ❑ Telnet and Rlogin
- ❑ HTTP
- ❑ POP, IMAP
- ❑ SMTP and NNTP
- ❑ FTP

Sniffing in the Data Link Layer of the OSI Model

- Sniffers hoạt động ở tầng data link của mô hình OSI.
- Các lớp mạng trong mô hình OSI được thiết kế để hoạt động độc lập với nhau; nếu một sniffer thực hiện "sniff" dữ liệu trong lớp data link, thì lớp OSI trên sẽ không nhận biết được việc bị "sniff".



Hardware Protocol Analyzers (HPA)

- HPA có thể sử dụng cả phần mềm và phần cứng để thu tín hiệu mà không làm thay đổi lưu lượng mạng.
- Về cơ bản HPA có khả năng xử lý được nhiều data hơn so với Software Protocol Analyzer tại thời điểm quá tải.

N2X N5540A Agilent Protocol Analyzer

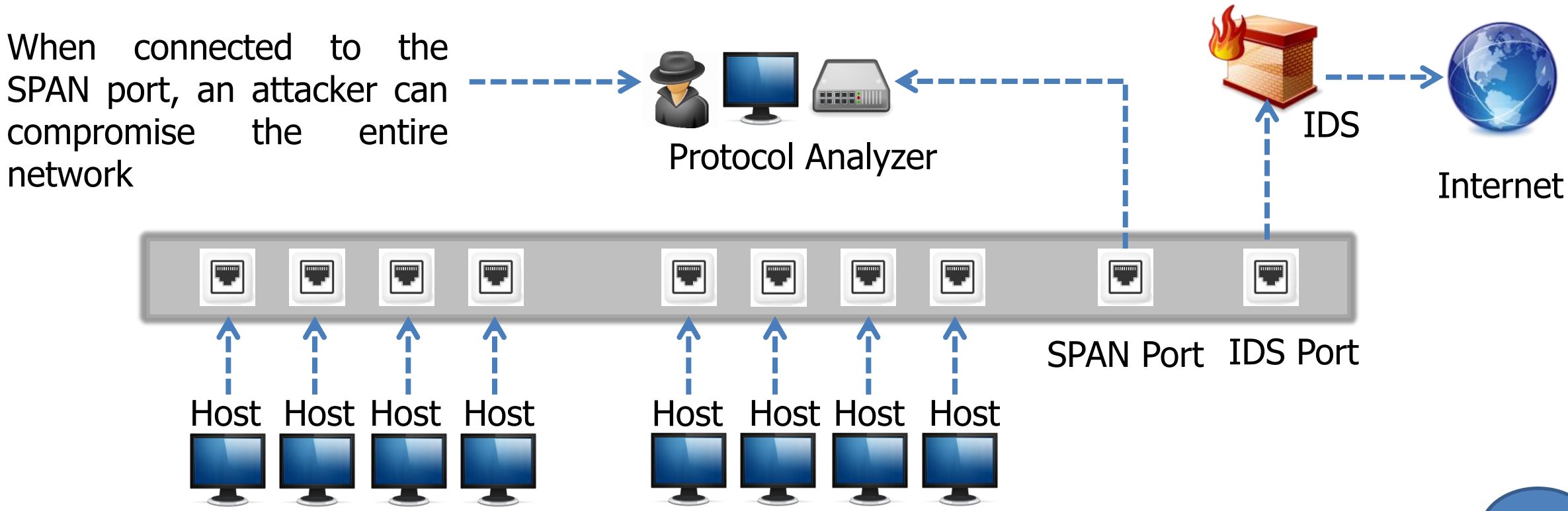
Keysight E2960B

Hardware Protocol Analyzer

- PTW60
- P5551A PCIe 5.0 Protocol Exerciser
- Voyager M4x Protocol Analyzer
- N2X N5540A Agilent Protocol Analyzer
- Xgig 1000

SPAN Port

- Cổng SPAN là một cổng được cấu hình để nhận một bản sao của mọi gói tin đi qua switch.
- Khi được kết nối với cổng SPAN, attacker có thể thâm nhập toàn bộ mạng.



Wiretapping

- Wiretapping là quá trình theo dõi các cuộc trò chuyện qua điện thoại và internet của bên thứ ba (Note: Wiretapping mà không có lệnh hoặc sự đồng ý của người có liên quan là hành vi vi phạm ở hầu hết các quốc gia.)
- Attacker kết nối thiết bị nghe (phần cứng, phần mềm hoặc kết hợp cả hai) với mạch truyền thông tin giữa hai điện thoại hoặc máy chủ trên internet.
- Wiretapping cho phép attacker giám sát, chặn, truy cập và ghi lại thông tin chứa trong luồng dữ liệu trên hệ thống liên lạc.

Types of Wiretapping

Active Wiretapping

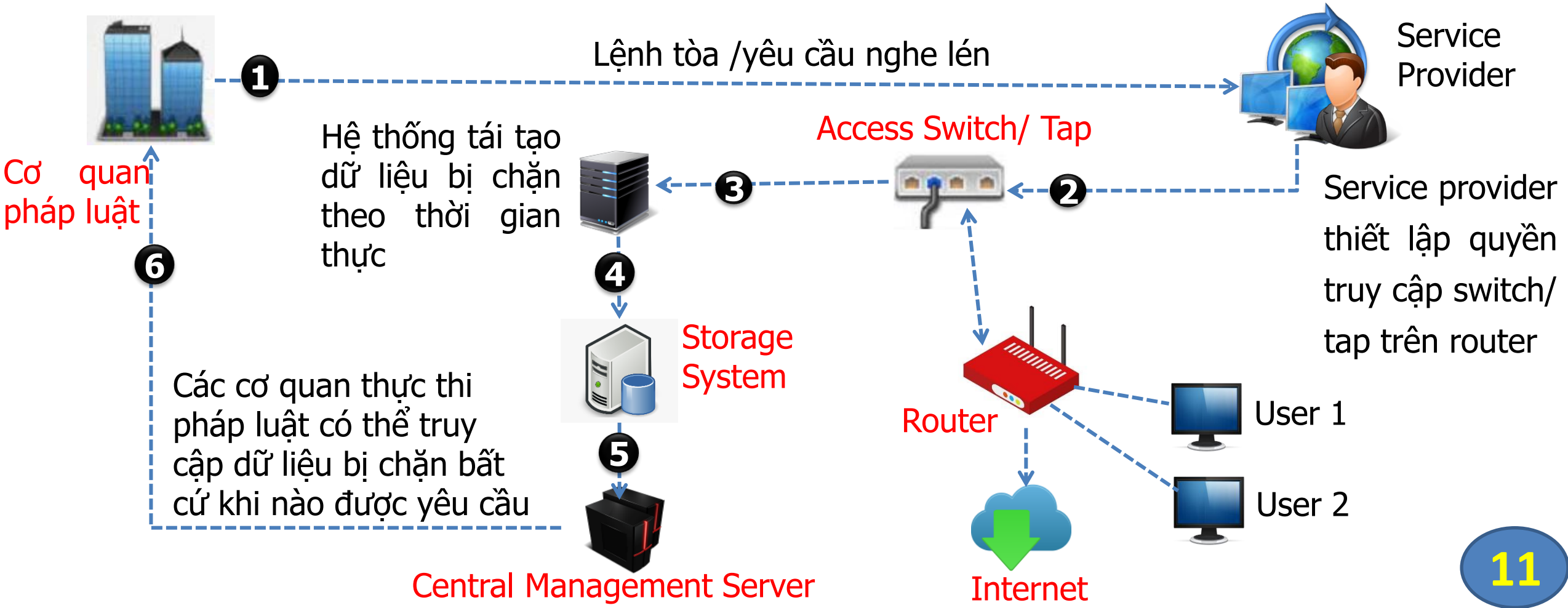
- Thực hiện việc giám sát, ghi lại, thay đổi và tiêm dữ liệu vào kết nối hoặc lưu lượng truy cập.

Passive Wiretapping

- Chỉ thực hiện giám sát và ghi lại lưu lượng và thu thập thông tin về dữ liệu mà nó chứa.

Lawful Interception

- Lawful Interception (Giám sát hợp pháp) đề cập đến việc ngăn chặn truyền thông dữ liệu hợp pháp giữa hai điểm đầu cuối để giám sát các dịch vụ viễn thông truyền thống, VoIP, dữ liệu và mạng đa dịch vụ.

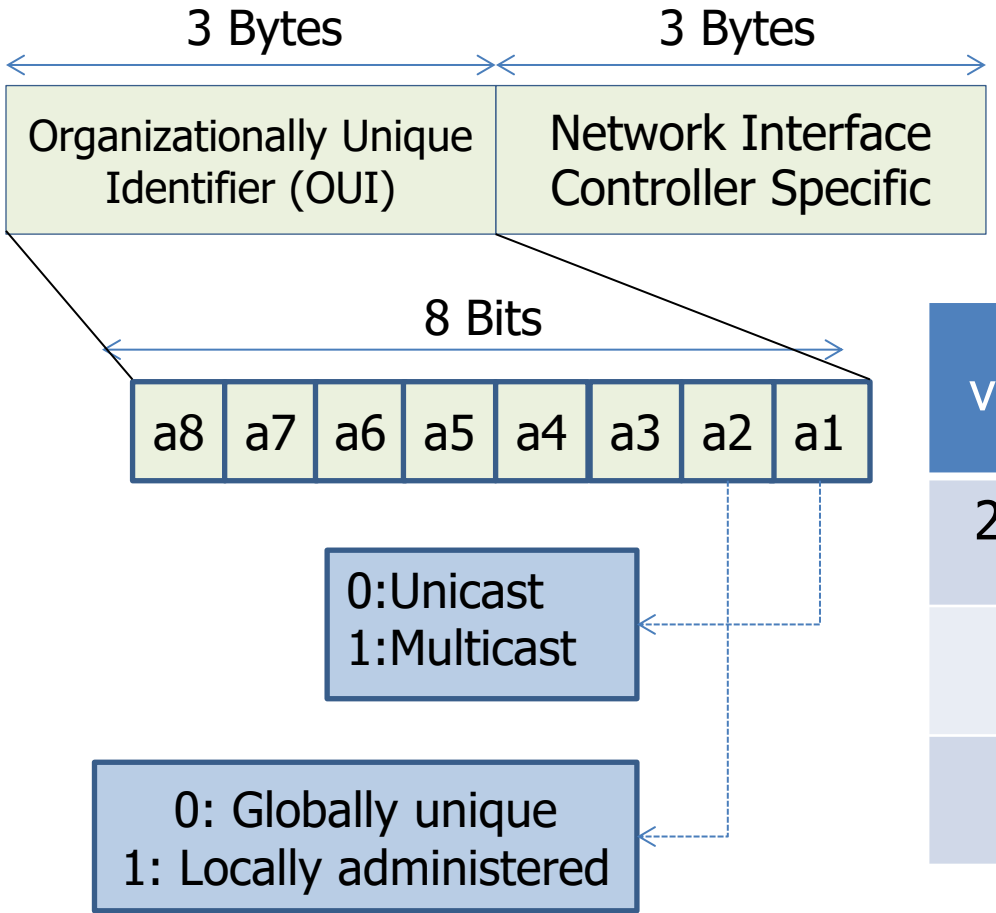


1. Tổng quan
2. Một số kỹ thuật nghe lén và biện pháp phòng chống
3. Kỹ thuật phát hiện nghe lén

MAC Address/CAM Table

- Mỗi switch đều có một bảng động chứa những thông tin như địa chỉ MAC tương ứng với các cổng vật lý và các tham số VLAN được gọi là bảng CAM (Content Addressable Memory).

MAC Address



CAM Table

vlan	MAC Add	Type	Learn	Age	Ports
255	00:d3.ad:34.12:3g	Dynamic	Yes	0	Gi5/2
5	as:23.df:45.45:t6	Dynamic	Yes	0	Gi5/2
5	er:23.23:er.t5:e3	Dynamic	Yes	0	Gi5/2

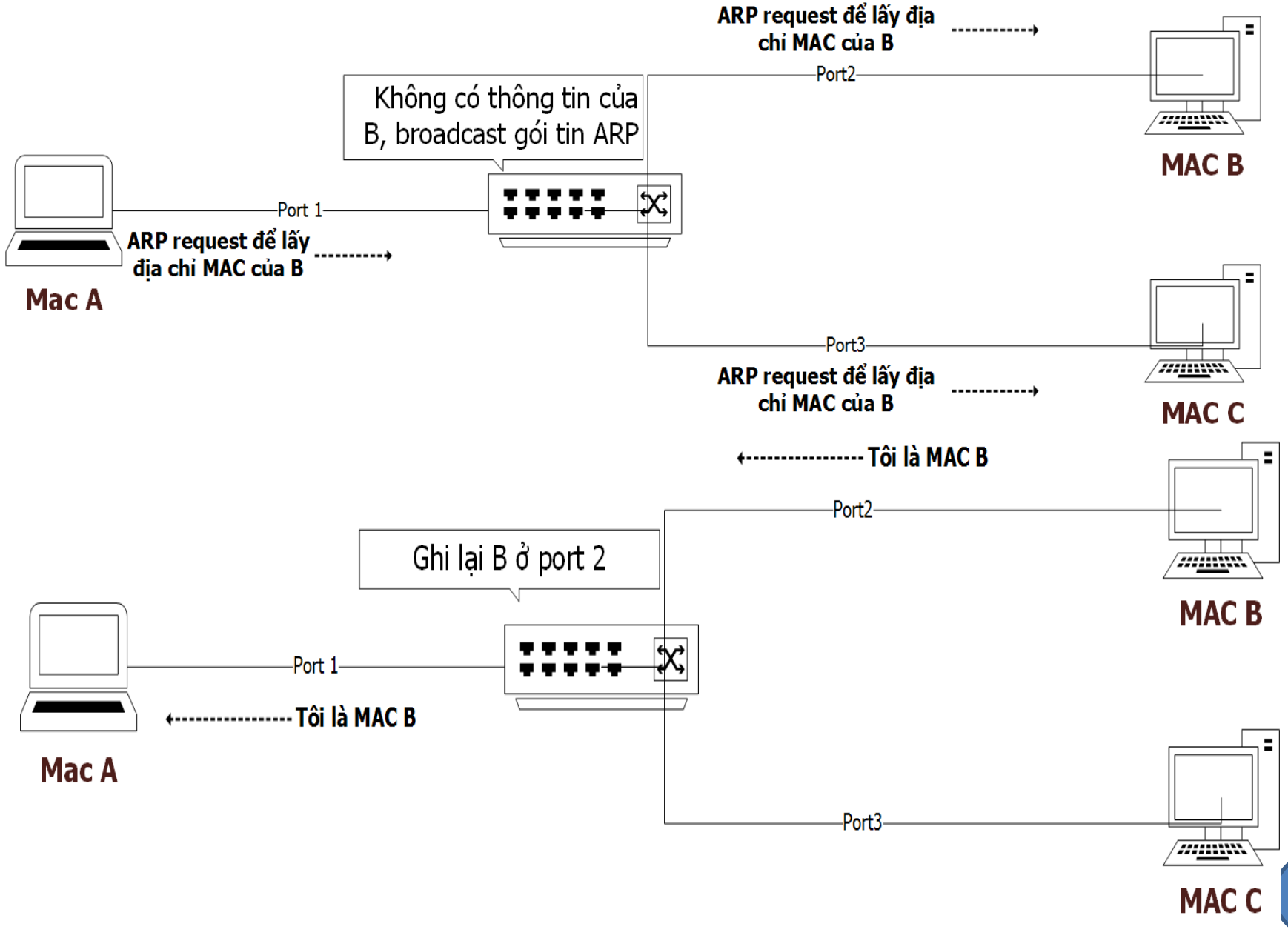
How CAM works (1/2)

MAC	PORT
A	1
C	3

Cam Table

MAC	PORT
A	1
B	2
C	3

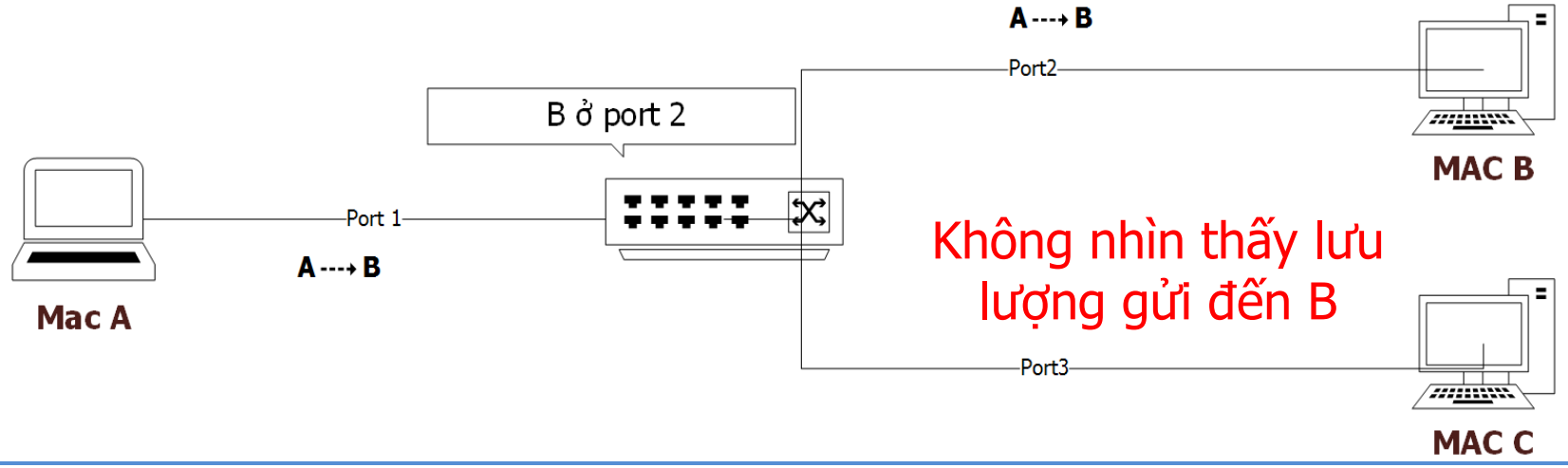
Cam Table



How CAM works (2/2)

MAC	PORT
A	1
B	2
C	3

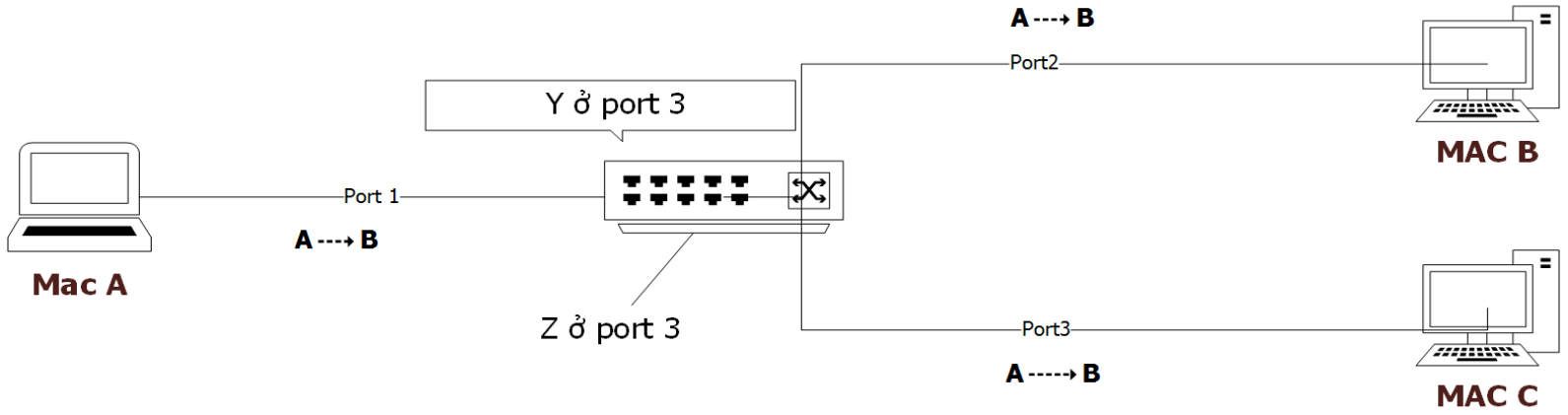
Cam Table



- Khi bảng CAM được ghi đầy, những request ARP sau đó sẽ làm tràn các port trên switch điều này làm cho switch "reset" về chế độ "học" – thực hiện gửi gói tin broadcast trên tất cả các port như hub.

MAC	PORT
Y	3
Z	3
C	3

Cam Table

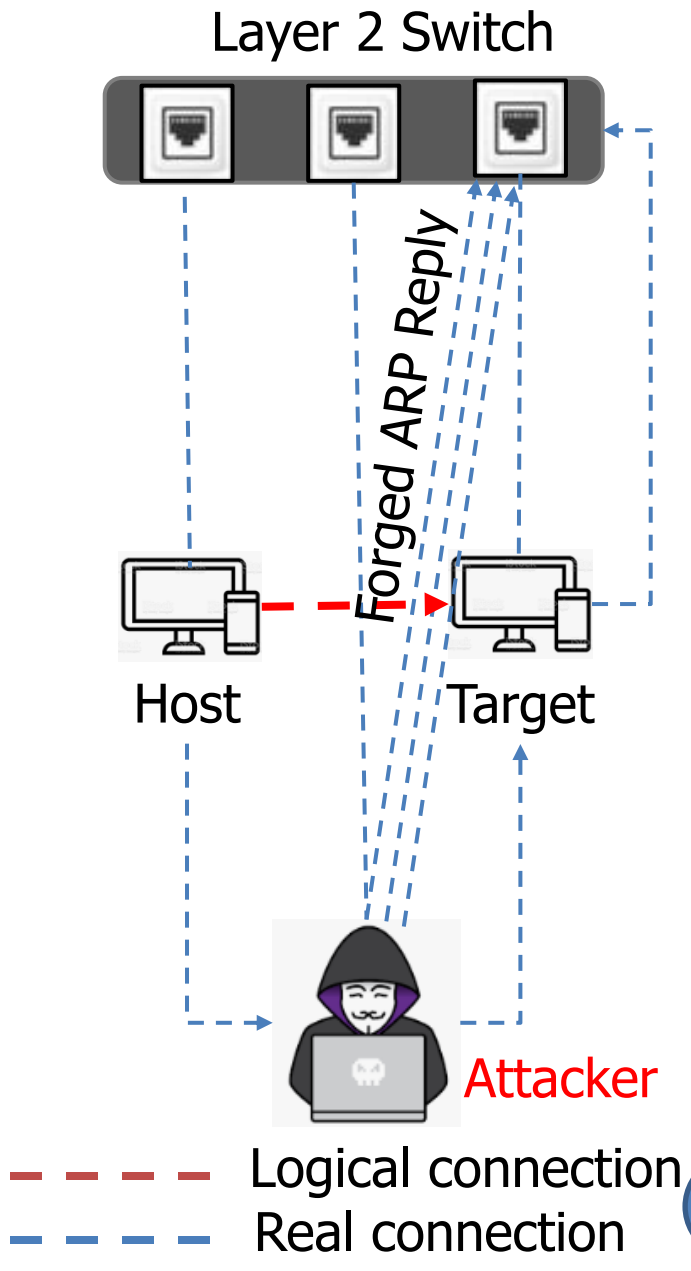


MAC Flooding

- MAC flooding là kỹ thuật làm tràn bảng CAM bằng cách gửi lưu lượng chứa địa chỉ MAC và IP giả mạo tới switch.
- Khi đó, switch sẽ hoạt động giống như hub và chuyển tất cả các gói tin tới tất cả các thiết bị trong mạng.
- Công cụ phổ biến: Macof – Unix/Linux tool, có khả năng gửi 131.000 gói tin giả mạo địa chỉ MAC và IP trong một phút.

Switch Port Stealing (1/4)

- Switch Port Stealing cũng là kỹ thuật nghe lén sử dụng MAC Flooding.
- Attacker sẽ gửi hàng loạt các gói tin ARP giả mạo với nguồn là địa chỉ MAC của nạn nhân và đích là địa chỉ MAC của attacker.
- Vì phải xử lí khối lượng tin lớn từ attacker và target host, switch phải thay đổi liên tục địa chỉ MAC giữa các cổng kết nối.
- Khi đó attacker sẽ có thể lấy cắp những dữ liệu mà đáng ra là được gửi cho nạn nhân.



Switch Port Stealing (2/4)

- Giả sử có 3 máy tính: Máy A, máy B (target) và máy C (Hacker)

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	Port C

- Bảng MAC của switch

Vlan	MAC Address	Type	Learn	Age	Ports
255	Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	0	Port A
5	Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	0	Port B
5	Host C	cc-dd-ee-ff-gg-hh	10.0.0.3	0	Port C

Switch Port Stealing (3/4)

1. Switch port stealing là một kỹ thuật sniffing giúp giả mạo cả địa chỉ IP và địa chỉ MAC của máy mục tiêu (Máy B).
2. Máy tính của hacker chạy một phần mềm sniffer để chuyển đổi card mạng của máy tính vào chế độ promiscuous mode.
3. Máy A (10.0.0.1), muốn giao tiếp với Máy B (10.0.0.2). Do đó, máy A gửi một yêu cầu ARP (Tôi muốn giao tiếp với 10.0.0.2. Địa chỉ MAC của 10.0.0.2 là gì?).
4. Switch phát tán yêu cầu ARP này tới tất cả các máy trong mạng.
5. Trước khi Máy B (target) có thể đáp ứng yêu cầu ARP, hacker đáp lại yêu cầu ARP bằng cách gửi một phản hồi ARP chứa địa chỉ MAC và IP giả mạo (Tôi là 10.0.0.2 và địa chỉ MAC của tôi là *bb-cc-dd-ee-ff-gg*). Hacker có thể đạt được điều này bằng cách tấn công *DoS* lên Máy B, làm chậm lại quá trình đáp ứng của nó.

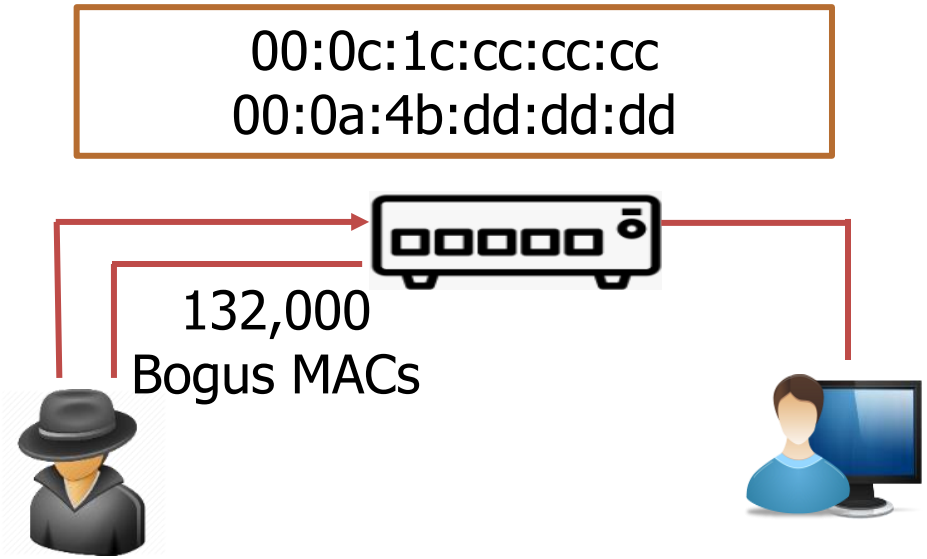
Switch Port Stealing (4/4)

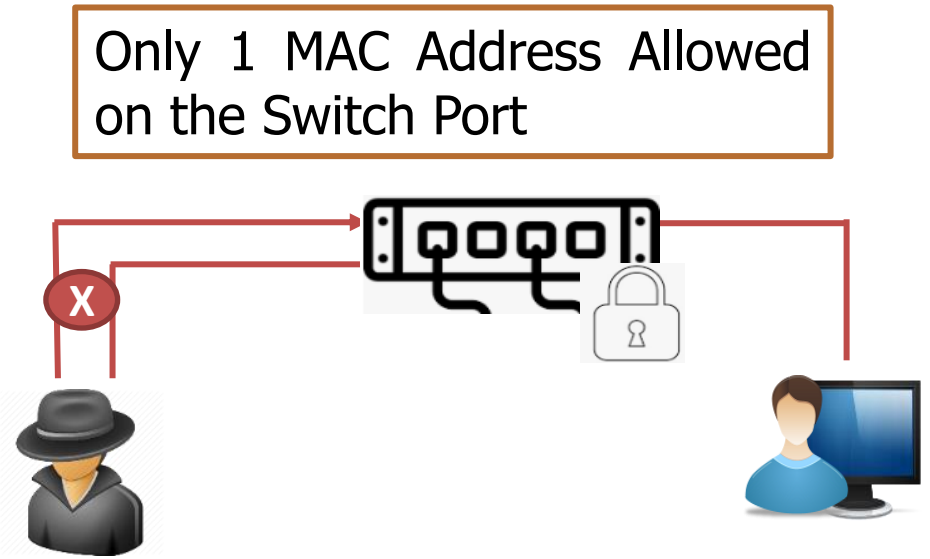
6. Bây giờ, bộ nhớ cache ARP trong switch ghi lại địa chỉ MAC và IP giả mạo.
7. Địa chỉ MAC giả mạo của Máy B (bb-cc-dd-ee-ff-gg) và cổng kết nối với máy tính của kẻ tấn công (Cổng C) và cập nhật bảng CAM của switch. Bây giờ, một kết nối được thiết lập giữa Máy A và máy tính của hacker (Máy C).

Machine	MAC Address	IP Address	Ports
Host A	aa-bb-cc-dd-ee-ff	10.0.0.1	Port A
Host B	bb-cc-dd-ee-ff-gg	10.0.0.2	Port B
Host C	bb-cc-dd-ee-ff-gg	10.0.0.2	Port C

MAC Table updated with a spoofed entry

How to defend against MAC Attacks

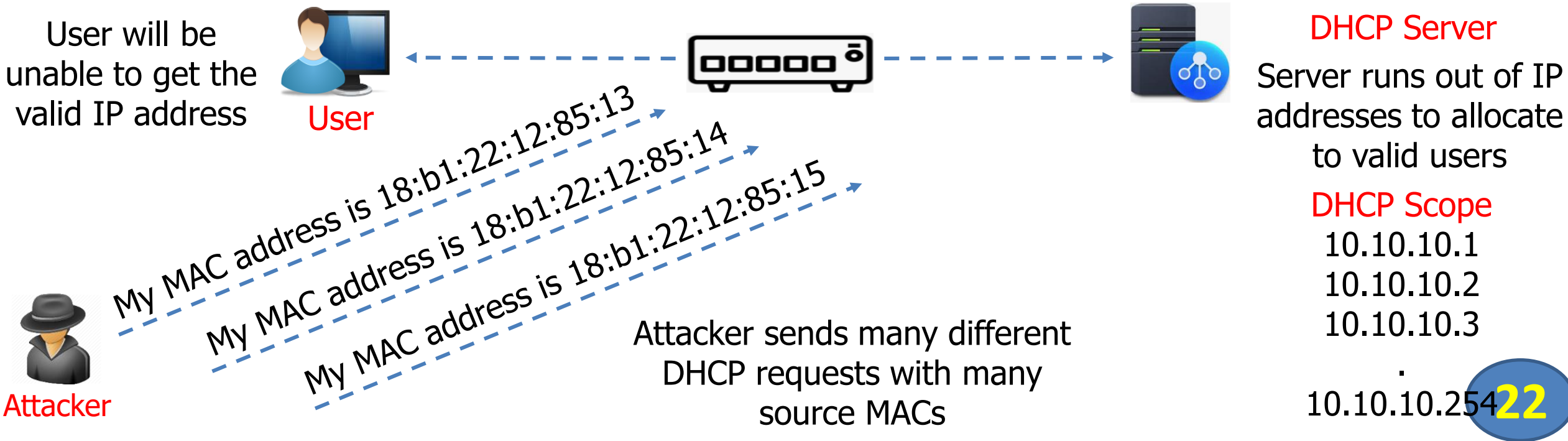




- Port Security là một tính năng nhận diện và giới hạn các địa chỉ MAC có thể truy cập vào cổng. Nếu ta gán một địa chỉ MAC an toàn cho một cổng an toàn, thì cổng chỉ chuyển tiếp các gói tin có địa chỉ nguồn nằm trong nhóm địa chỉ được xác định.

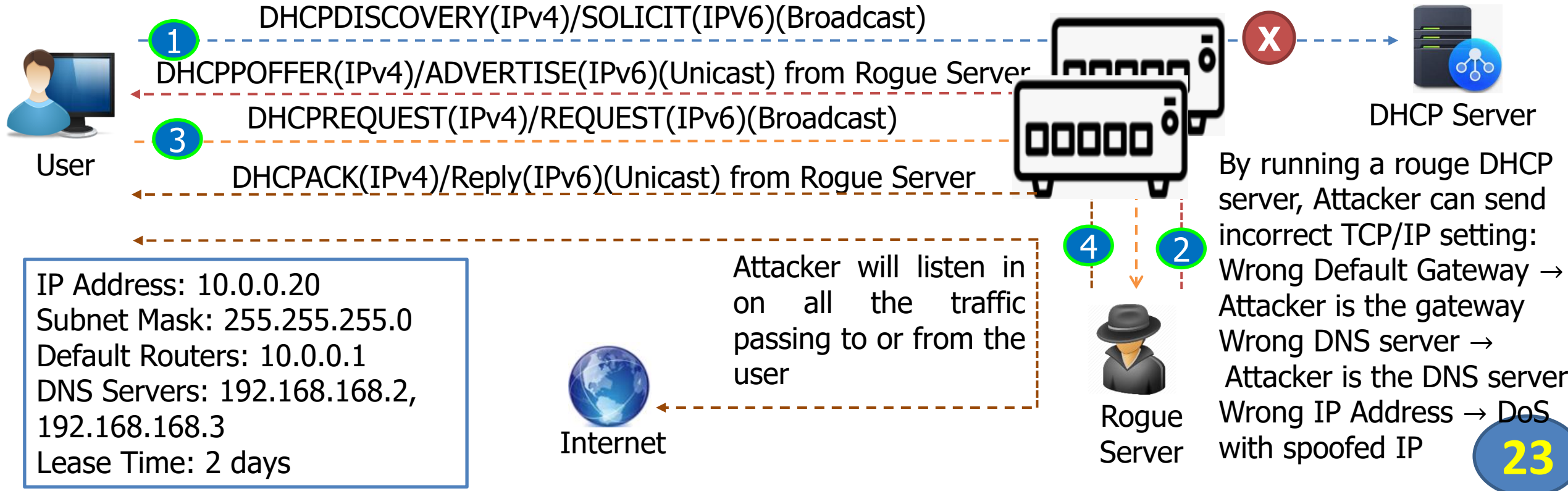
DHCP Starvation Attack

- Đây là một dạng tấn công DoS lên DHCP Server. Attacker gửi broadcast rất nhiều DHCP request với địa chỉ MAC giả mạo lên DHCP Server để giải phóng các địa chỉ IP khả dụng trong phạm vi của DHCP.
- Người dùng hợp lệ không thể nhận được hoặc yêu cầu địa chỉ mới thông qua DHCP và không thể truy cập được vào mạng.



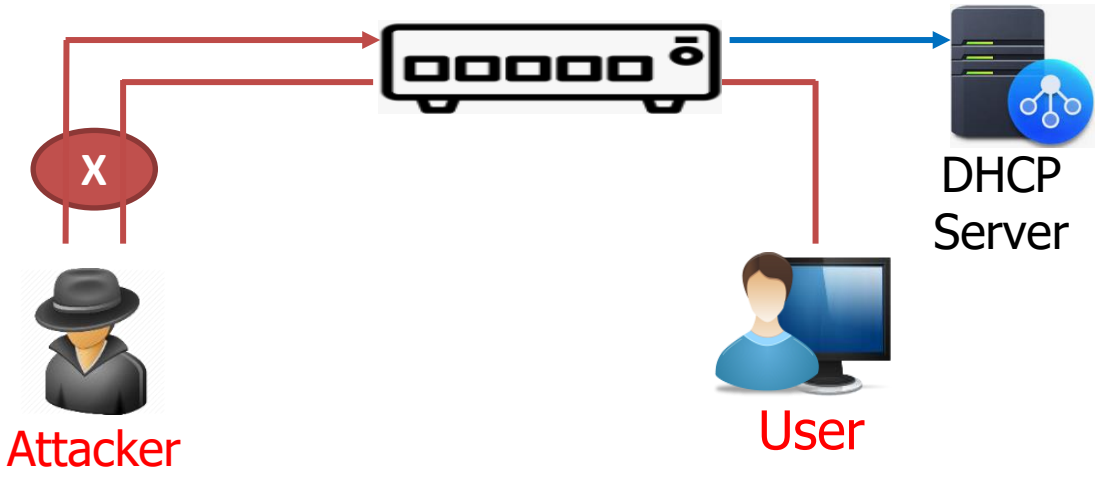
Rogue DHCP Server Attack

- Attacker thiết lập "rogue DHCP server" và phản hồi các yêu cầu DHCP bằng các địa chỉ IP không có thật dẫn đến việc truy cập mạng bị xâm phạm.
- Tấn công này hoạt động cùng với tấn công DHCP Starvation, attacker gửi "TCP/IP setting" cho người dùng sau khi đánh bật anh ta/cô ta khỏi "genuine DHCP server".



How to Defend Against DHCP Starvation and Rogue Server Attacks

❑ "Enable port security " cho phép chống lại DHCP starvation attack



❑ "Enable DHCP snooping" trên cổng mà DHCP server kết nối vào. Khi đã cấu hình, DHCP snooping không cho phép các cổng khác trên switch đáp ứng các gói tin DHCP Discover gửi từ các client. Lưu ý: Mọi cổng VLAN đều là không tin cậy (theo mặc định)

IOS Switch Commands

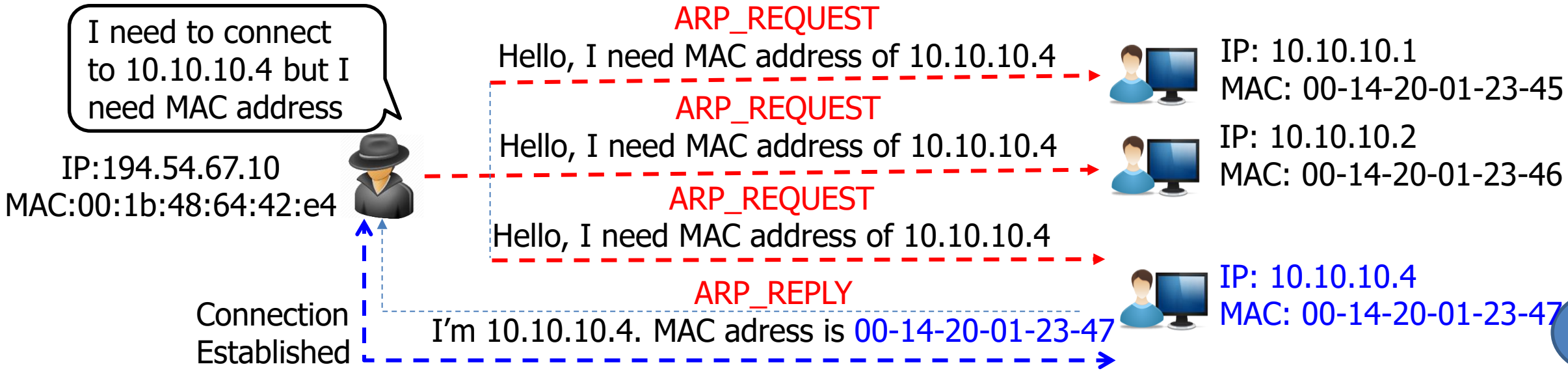
switchport port-security
switchport port-security maximum 1
switchport port-security violation restrict
switchport port-security aging time 2
#switchport port-security aging type inactivity
#switchport port-security mac-address sticky

IOS Global Commands

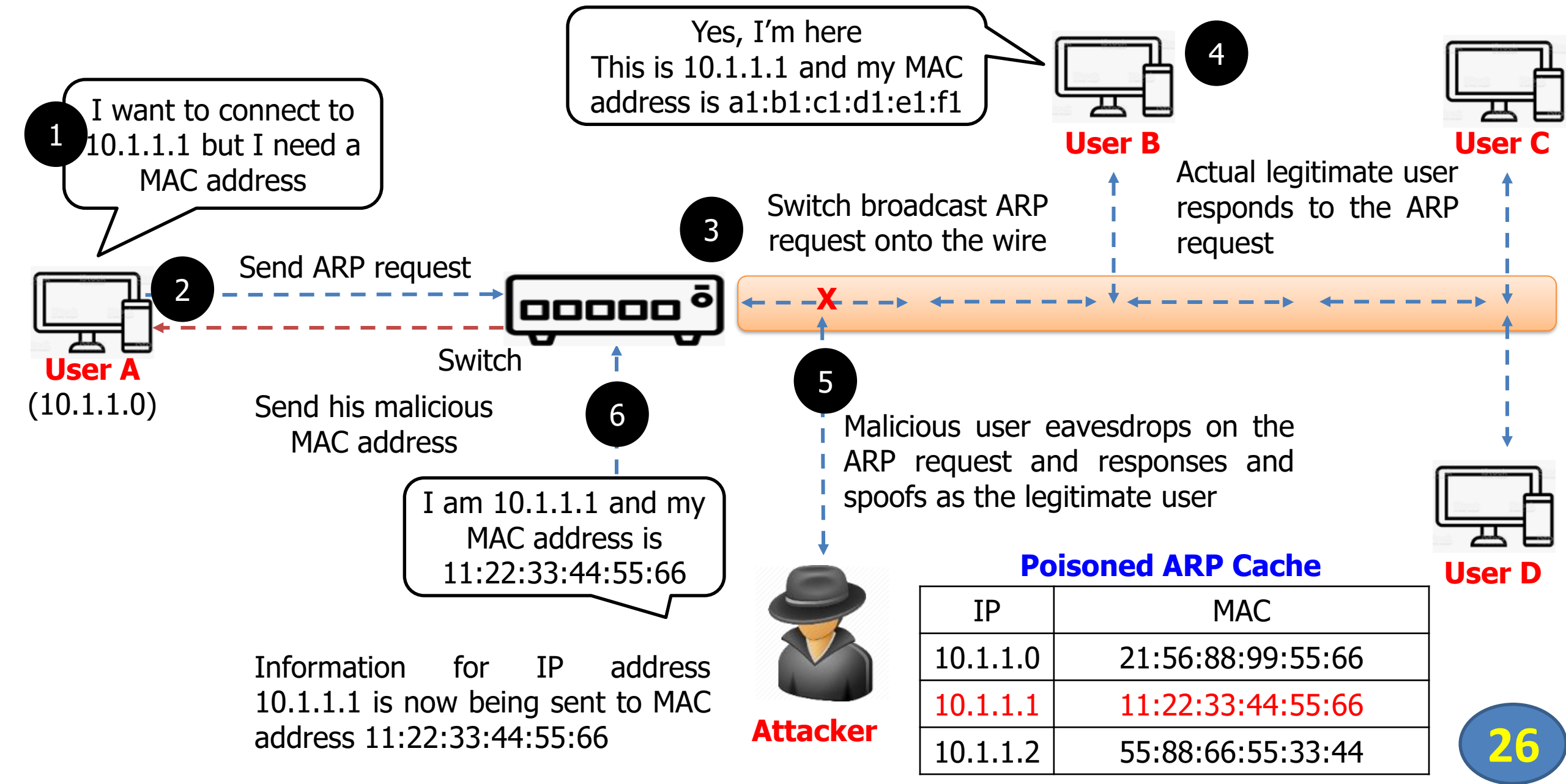
ip dhcp snooping → this turns on DHCP snooping
ip dhcp snooping vlan 4, 104 → this configures VLANs to snoop
ip dhcp snooping trust → this configures interface as trusted

ARP Spoofing Attack

- Các gói ARP có thể được giả mạo để gửi dữ liệu đến máy của attacker.
- ARP spoofing liên quan đến việc tạo nhiều ARP request và ARP reply "giả mạo" để làm quá tải switch.
- Switch được đặt ở "forwarding mode" sau khi các bảng ARP bị tràn với các gói ARP reply giả mạo và sau đó attacker có thể "sniff" tất cả các gói tin trong mạng
- Attacker làm tràn ARP cache của máy mục tiêu với các "entries" giả mạo (còn được gọi là "poisoning").



How does ARP Spoofing Attack Work



Poisoned ARP Cache

IP	MAC
10.1.1.0	21:56:88:99:55:66
10.1.1.1	11:22:33:44:55:66
10.1.1.2	55:88:66:55:33:44

Threats of ARP Poisoning

❑ Sử dụng "fake ARP messages", attacker có thể chuyển hướng tất cả thông tin liên lạc giữa hai máy, dẫn đến tất cả lưu lượng được trao đổi qua PC của attacker.

1. Packet Sniffing
2. Session Hijacking
3. VoIP Call Tapping
4. Manipulating Data
5. Man-in-the-Middle Attack
6. Data Interception
7. Connection Hijacking
8. Connection Resetting
9. Stealing Passwords
10. Denial-of-Service Attack

ARP Poisoning Tools

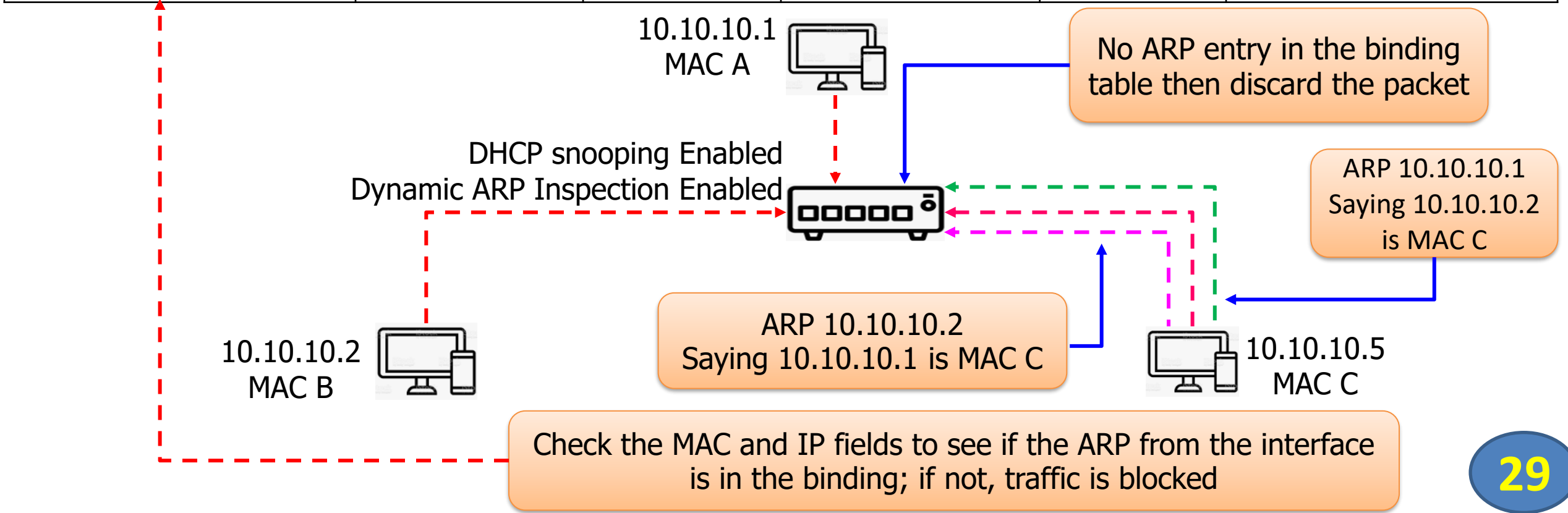
1. Better CAP
2. Ettercap
3. dsniff
4. MITMf
5. ARPSpoofTool
6. Cain & Abel

How to Defend Against ARP Poisoning

- Triển khai "Dynamic ARP inspection (DAI)" bằng cách dùng DHCP Snooping Binding Table

sh ip dhcp snooping binding

MacAddress	ipAddress	Lease	Type	Vlan	Interface
1a:12:3b:2f:df:1c	10.10.10.8	125864	dhcp-snooping	4	FastEthernet3/18



Configuring DHCP Snooping và Dynamic ARP Inspection (1/2)

01

```
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ^z
Switch(config)# show dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLAN: 10
DHCP snooping is operational on following VLAN: 10
DHCP snooping is configured on following L3
Interface:
……
DHCP snooping trust/rate is configured on the following Interface:
  Interface          Trusted       rate limit ( pps  )
  ------------       ----------    --------------------
```

02

```
Switch(config)# show ip dhcp snooping binding
MacAddress          IpAddress       Lease          Type           VLAN        Interface
-------------------------------------------------------------------------------------------
1a:12:3b:2f:df:1c   10.10.10.8      125864     dhcp-snooping       4        FastEthernet0/3
```

Configuring DHCP Snooping và Dynamic ARP Inspection (2/2)

03

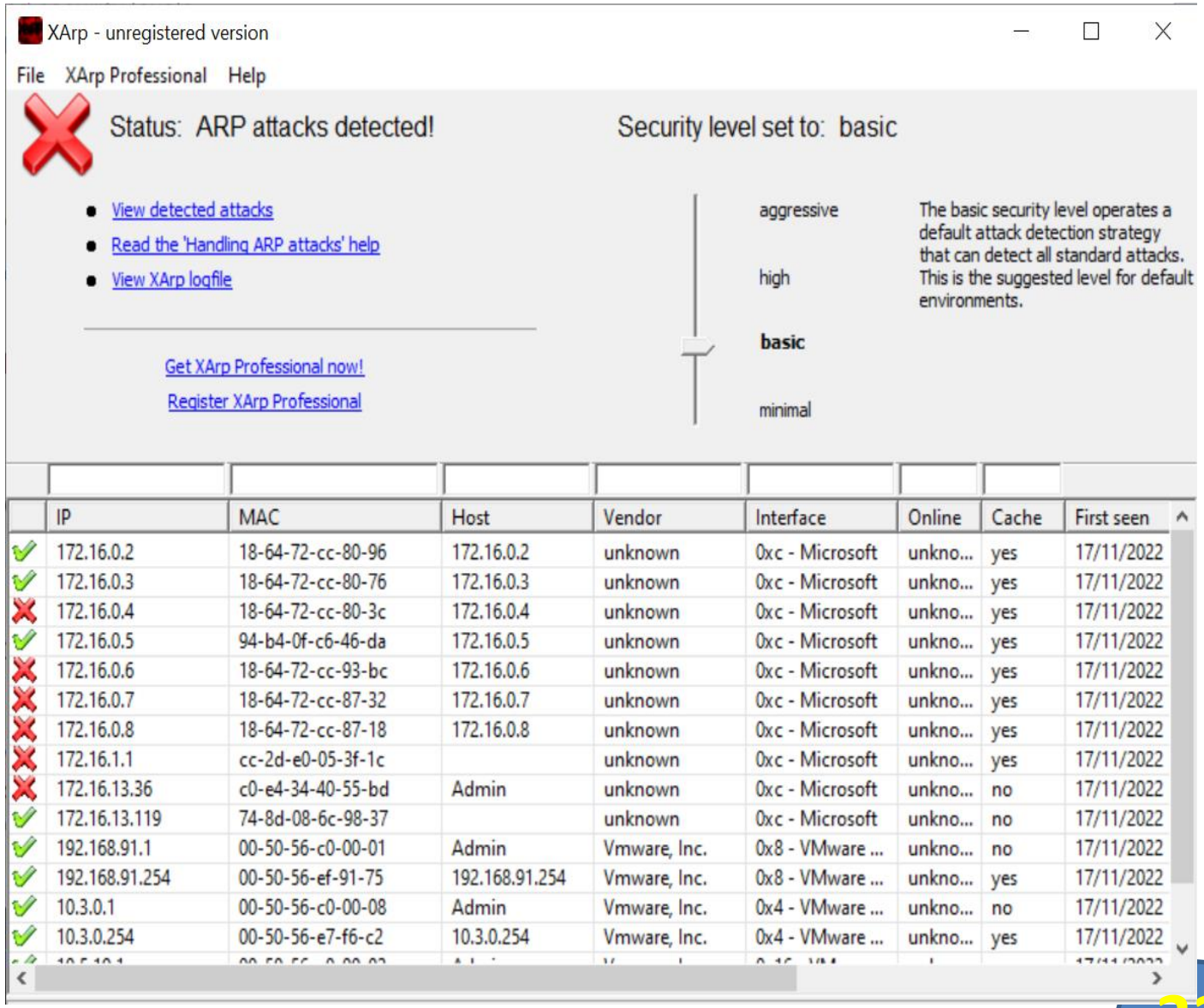
```
Switch(config)# ip dhcp snooping vlan 10 - 20
Switch(config)# ip arp inspection vlan 10 - 20
Switch(config)# interface range GigabitEthernet0/1 - 10
Switch(config)# ip arp inspection trust
Source Mac Validation: Disabled/Destination Mac Validation: Disabled/IP Address Validation: Disabled
Vlan  Configuration Operation  ACL Match   Static ACL
10     Enabled         Active
Vlan    ACL Logging      DHCP Logging      Probe Logging
10       Deny              Deny              Off
Vlan  Forwarded    Dropped    DHCP Drops   ACL Drops
10        0              0              0            0
Vlan    DHCP Permits    ACL Permits    Probe Permits     Source MAC Failures
10             0              0              0                  0
Vlan  Dest Mac Failures  IP validation Failures  Invalid Protocol Data
10            0                 0                        0
```

```
%SW_DAI-4-DHCP_SNOOPING_DENY: 1 invalid ARPs
(Res) on Fa0/5, vlan 10.((0013.6050.acf4/192.168.10.1/ffff.ffff.ffff/192.168.10.1/05:37:31 UTC M
30 2017
```

04

ARP Spoofing Dectection Tools

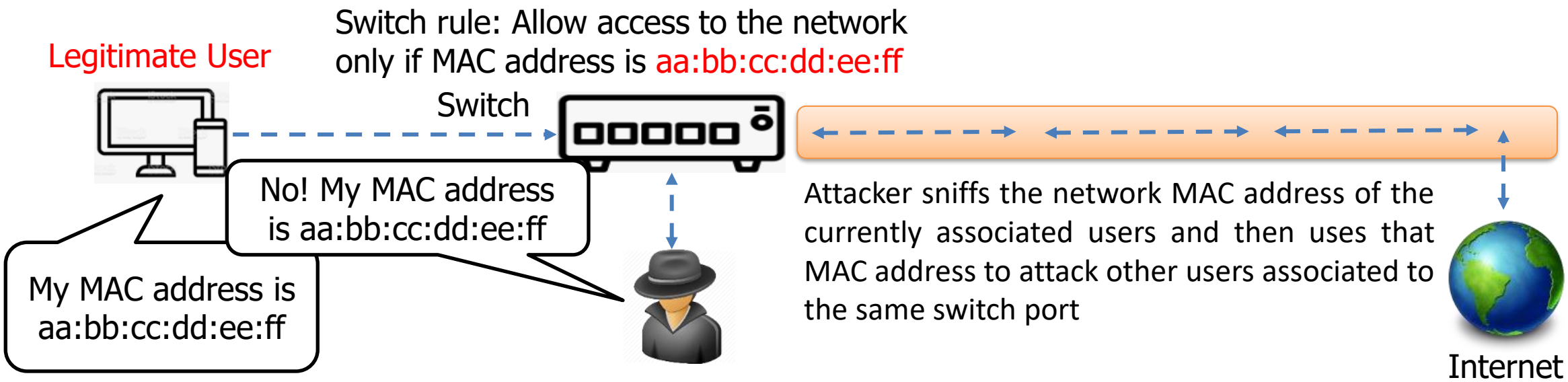
- ❑ XARP
- ❑ ArpON
- ❑ ARP AntiSpoofer
- ❑ ARPStraw
- ❑ shARP



IP	MAC	Host	Vendor	Interface	Online	Cache	First seen
172.16.0.2	18-64-72-cc-80-96	172.16.0.2	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.3	18-64-72-cc-80-76	172.16.0.3	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.4	18-64-72-cc-80-3c	172.16.0.4	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.5	94-b4-0f-c6-46-da	172.16.0.5	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.6	18-64-72-cc-93-bc	172.16.0.6	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.7	18-64-72-cc-87-32	172.16.0.7	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.0.8	18-64-72-cc-87-18	172.16.0.8	unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.1.1	cc-2d-e0-05-3f-1c		unknown	0xc - Microsoft	unkno...	yes	17/11/2022
172.16.13.36	c0-e4-34-40-55-bd	Admin	unknown	0xc - Microsoft	unkno...	no	17/11/2022
172.16.13.119	74-8d-08-6c-98-37		unknown	0xc - Microsoft	unkno...	no	17/11/2022
192.168.91.1	00-50-56-c0-00-01	Admin	Vmware, Inc.	0x8 - VMware ...	unkno...	no	17/11/2022
192.168.91.254	00-50-56-ef-91-75	192.168.91.254	Vmware, Inc.	0x8 - VMware ...	unkno...	yes	17/11/2022
10.3.0.1	00-50-56-c0-00-08	Admin	Vmware, Inc.	0x4 - VMware ...	unkno...	no	17/11/2022
10.3.0.254	00-50-56-e7-f6-c2	10.3.0.254	Vmware, Inc.	0x4 - VMware ...	unkno...	yes	17/11/2022

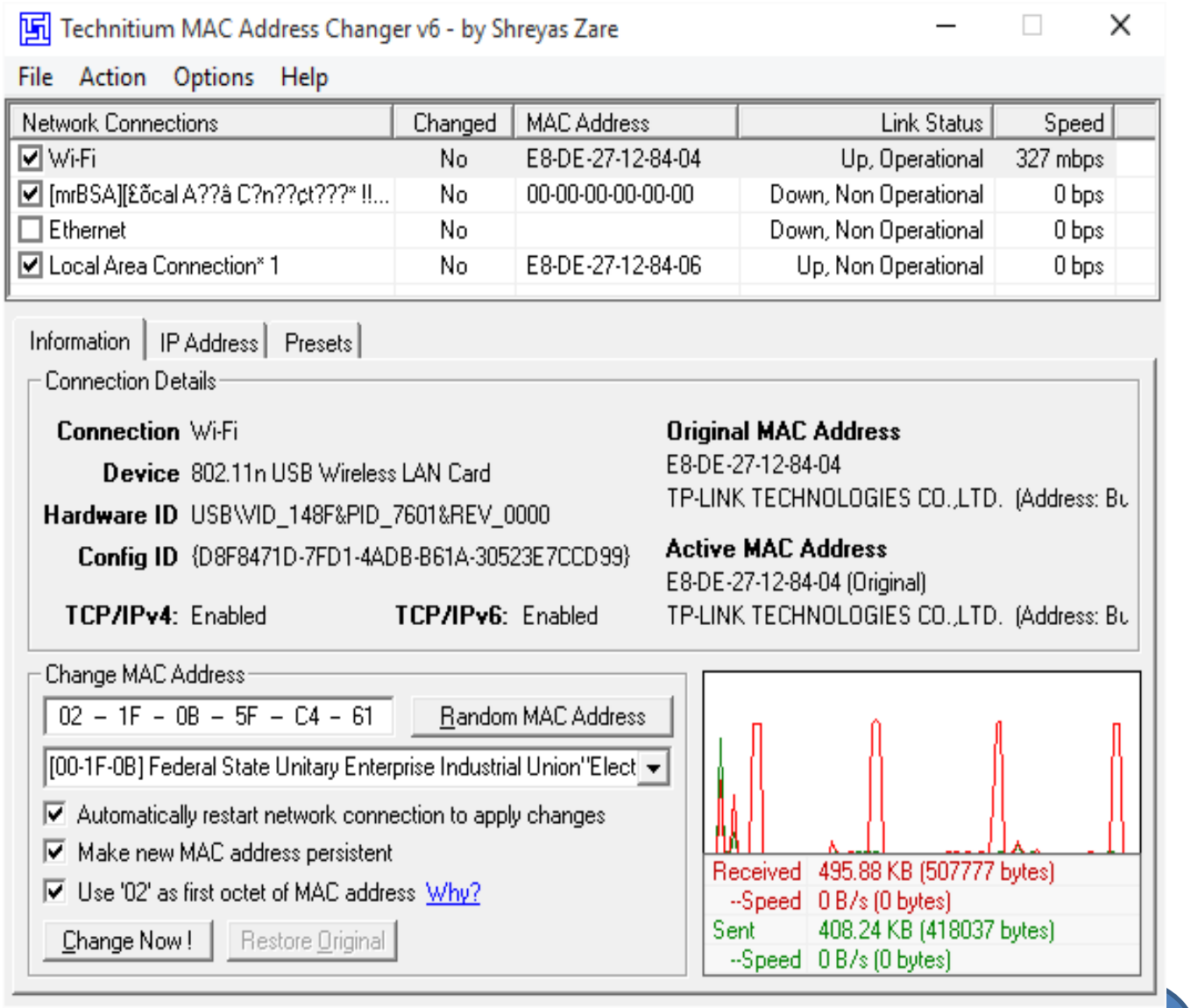
MAC spoofing/Duplicating

- Tấn công sao chép MAC được khởi chạy bằng cách nghe lén địa chỉ MAC của clients thường xuyên liên kết với switch và sử dụng lại một trong những địa chỉ đó.
- Bằng cách lắng nghe lưu lượng truy cập trên mạng, người dùng độc hại có thể chặn và sử dụng địa chỉ MAC của người dùng hợp lệ để nhận tất cả lưu lượng đến dành cho người dùng đó.
- Tấn công này cho phép attacker có quyền truy cập vào mạng và chiếm lấy danh tính của ai đó trên mạng.



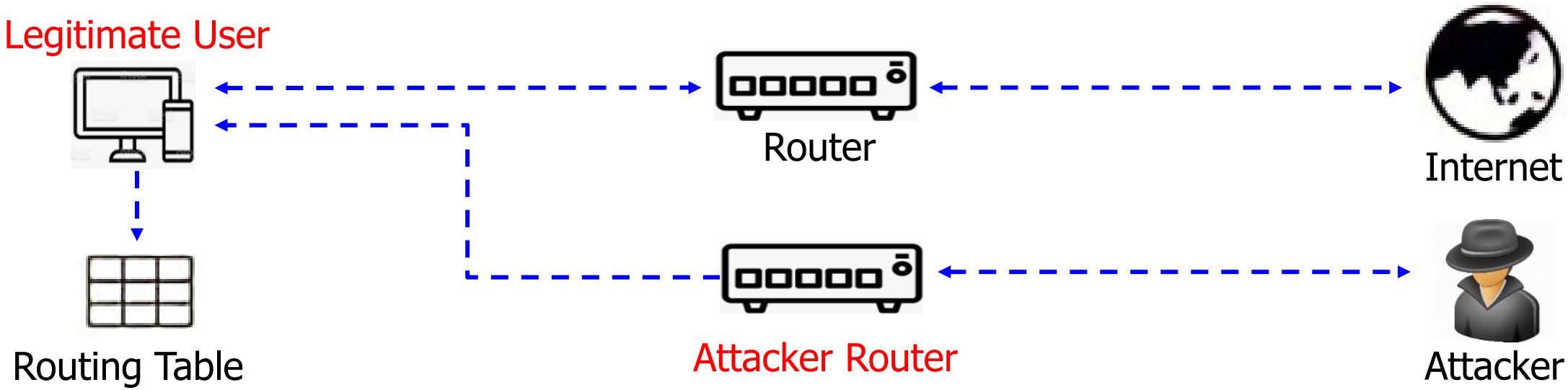
MAC Spoofing Tools

- SMAC
- Technitium MAC Address Changer
- MAC Address Changer
- Change MAC Address
- Easy MAC Changer
- Spoof-Me-Now



IRDP Spoofing

- ICMP Router Discovery Protocol (IRDP) là một giao thức định tuyến cho phép host phát hiện địa chỉ IP của các routers đang hoạt động trên subnet của họ bằng cách lắng nghe "Router Solicitation" và "Router Advertisement" query message.
- Attacker gửi "spoofed IRDP router advertisement message" tới host trên subnet, khiến nó thay đổi default router của mình thành bất cứ thứ gì attacker chọn.
- Attacker có thể sử dụng spoofed IRDP để khởi động tấn công MiTM, DoS và nghe lén kênh truyền.

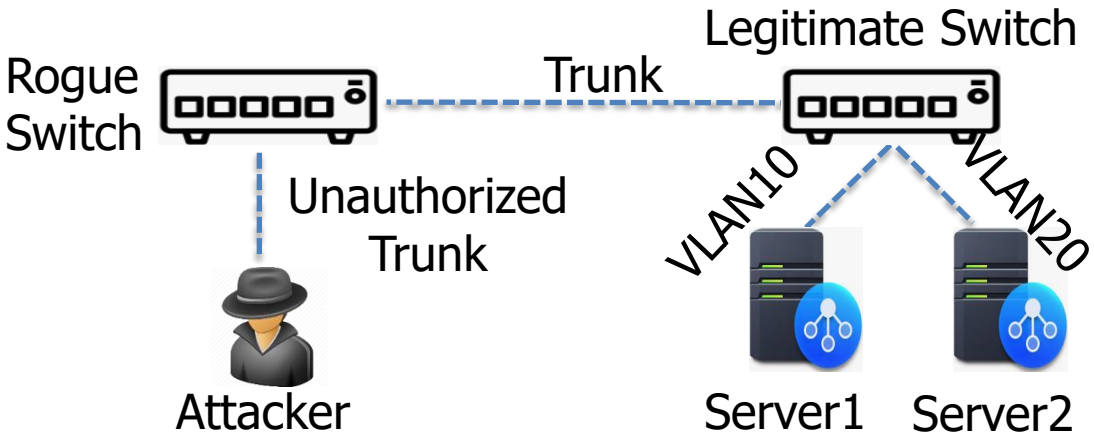


VLAN Hopping

- VLAN hopping là một kĩ thuật được sử dụng để nhắm mục tiêu tài nguyên mạng có trên virtual LAN sử dụng 2 phương pháp chính: Switch Spoofing và Double Tagging.
- Attacker thực hiện tấn công VLAN hopping để đánh cắp thông tin nhạy cảm, sửa đổi hoặc xoá dữ liệu, cài đặt chương trình độc hại và phát tán mã độc trên toàn mạng.

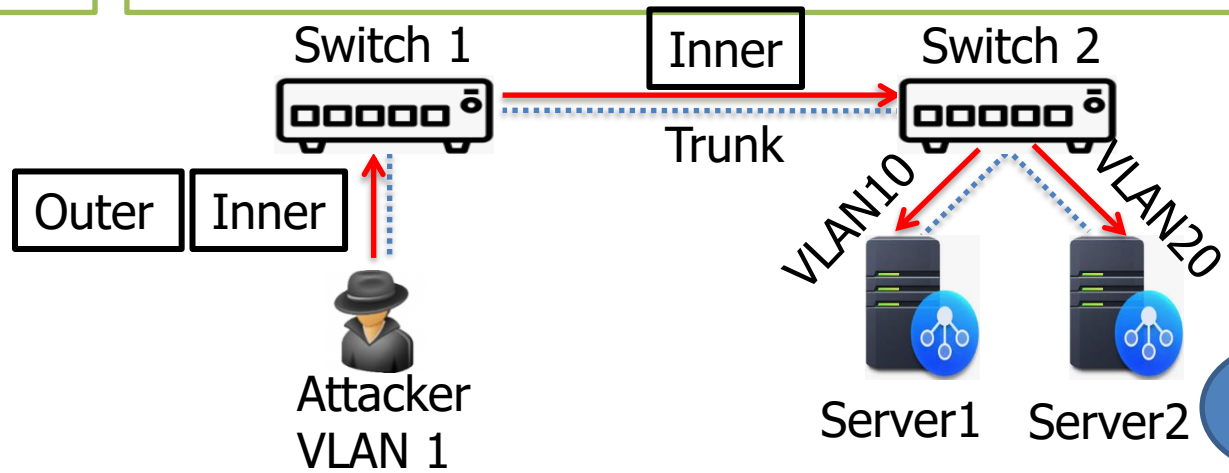
Switch Spoofing

- Attacker kết nối "rogue switch" vào mạng bằng cách đánh lừa switch hợp pháp từ đó tạo ra trunk link giữa chúng



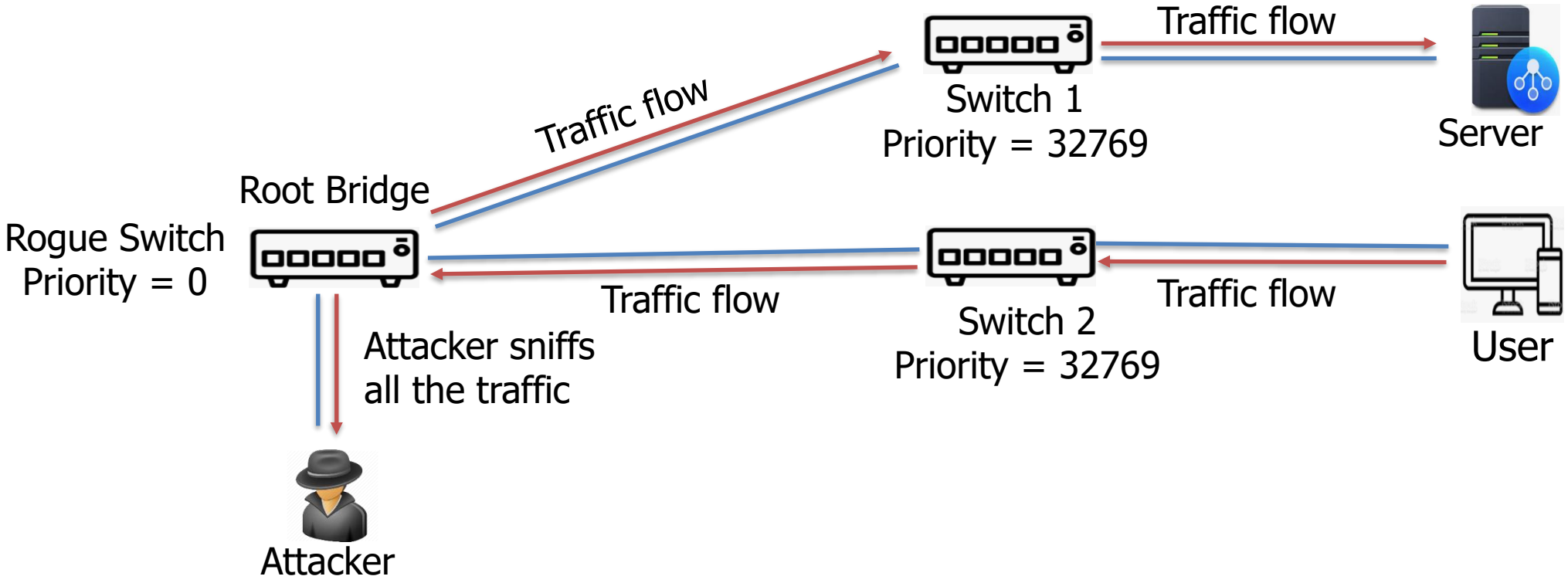
Double Tagging

- Attacker thêm và sửa tags trong Ethernet frame từ đó cho phép "traffic" qua bất kỳ VLAN nào trong mạng



STP Attack

- Attackers kết nối rogue switch vào mạng để thay đổi hoạt động của STP protocol và nghe lén tất cả lưu lượng mạng
- Attackers thực hiện cấu hình trên rogue switch sao cho để mức ưu tiên thấp hơn bất kỳ switch nào khác trong mạng. Việc này biến nó thành "root bridge", do đó cho phép attackers nghe lén được tất cả lưu lượng truy cập trong mạng

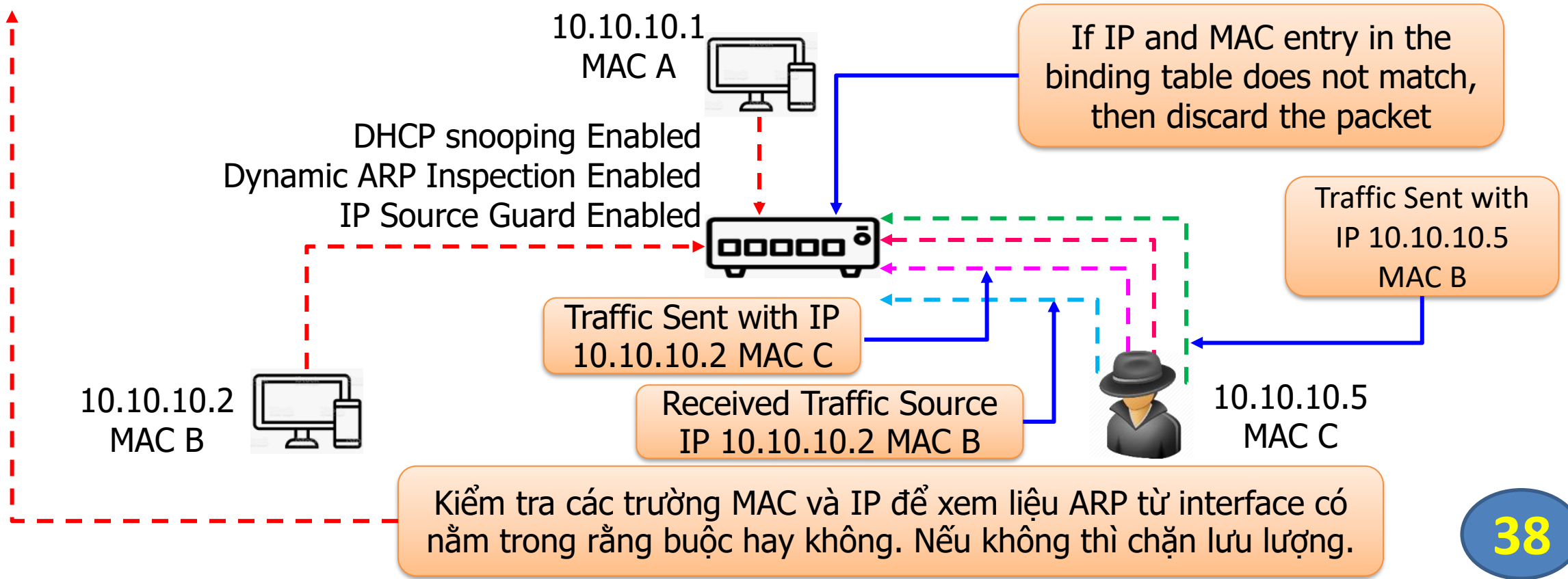


How to Defend Against MAC Spoofing

❑ Sử dụng DHCP Snooping Binding Table, Dynamic ARP Inspection và IP Source Guard

sh ip dhcp snooping binding

MacAddress	ipAddress	Lease	Type	Vlan	Interface
2a:33:4c:2f:4a:1c	10.10.10.9	185235	dhcp-snooping	4	FastEthernet3/18



How to Defend Against VLAN Hopping

Defend agains Switch Spoofing

- Cấu hình rõ ràng các cổng dưới dạng cổng truy cập và đảm bảo rằng tất cả các cổng truy cập được cấu hình để không thiết lập "trunks"

#switchport mode access

#switchport mode nonegotiate

- Đảm bảo rằng tất cả các cổng "trunk" được cấu hình không thiết lập "trunks"

switch(config-if)# switchport mode trunk

switch(config-if)# switchport mode nonegotiate

Defend agains Double Tagging

- Đảm bảo rằng mỗi cổng truy cập được gán với VLAN ngoại trừ VLAN mặc định (VLAN 1)

#switchport access vlan 2

- Đảm bảo rằng các native VLAN trên tất cả các cổng "trunk" được đổi thành unused VLAN ID:

#switchport trunk native vlan 999

- Đảm bảo rằng native VLAN trên tất cả cổng "trunk" đều được gắn thẻ rõ ràng:

#vlan dot1q tag native

How to Defend Against STP Attacks

BPDU Guard

❑ Kích hoạt BPDU Guard trên tất cả PortFast edge ports:

#configure terminal

#interface gigabiteethernet slot/port

#spanning-tree portfast bpduguard

Loop Guard

❑ Kích hoạt Loop Guard trên một interface:

#configure terminal

#interface gigabiteethernet slot/port

#spanning-tree guard loop

Root Guard

❑ Kích hoạt Root Guard trên một interface:

#configure terminal

#interface gigabiteethernet slot/port

#spanning-tree guard root

UDLD

❑ Kích hoạt UDLD (Unidirectional Link Detection) trên một interface:

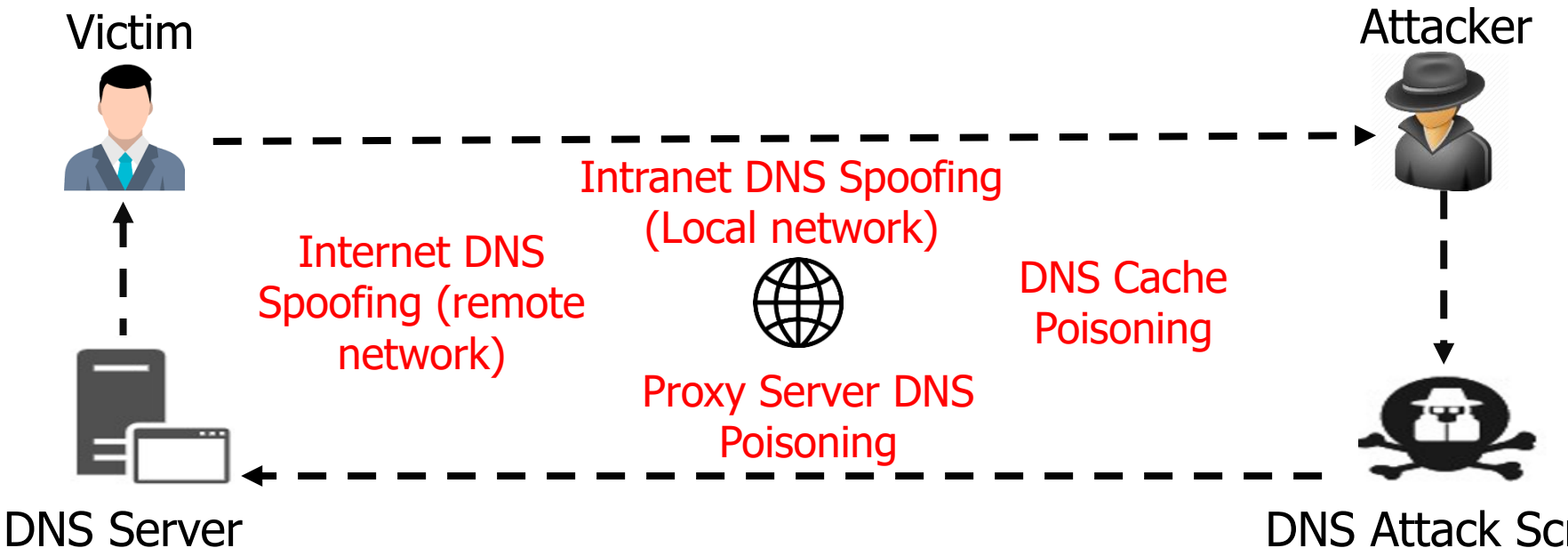
#configure terminal

#interface gigabiteethernet slot/port

#udld {enable | disable | aggressive}

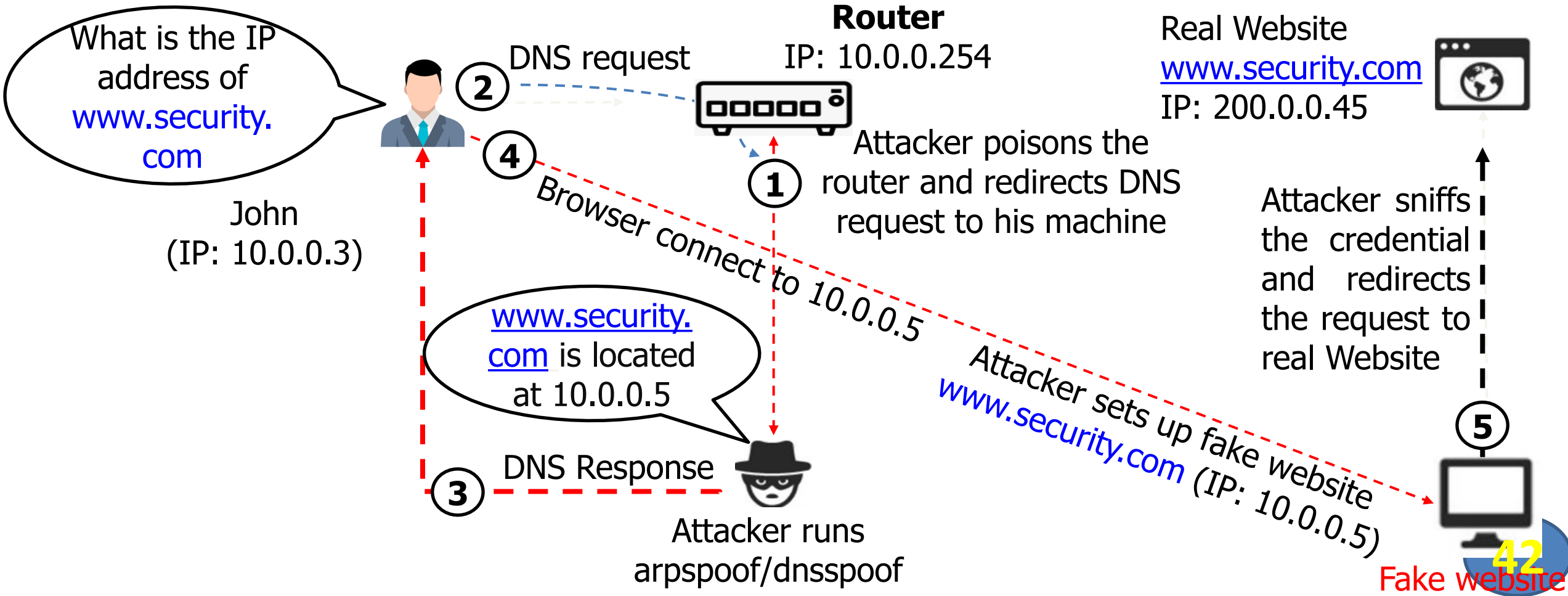
DNS Poisoning Techniques

- DNS poisoning là một kỹ thuật đánh lừa DNS server tin rằng nó đã nhận được thông tin xác thực trong khi thực tế nó không nhận được bất kỳ thông tin xác thực nào
- DNS poisoning cho phép attacker thay thế "IP address entries" trên một DNS server nhất định bằng các địa chỉ IP do attacker kiểm soát
- Attacker có thể tạo "fake DNS entries" cho máy chủ (chứa nội dung độc hại) với các tên tương tự như tên của máy chủ mục tiêu



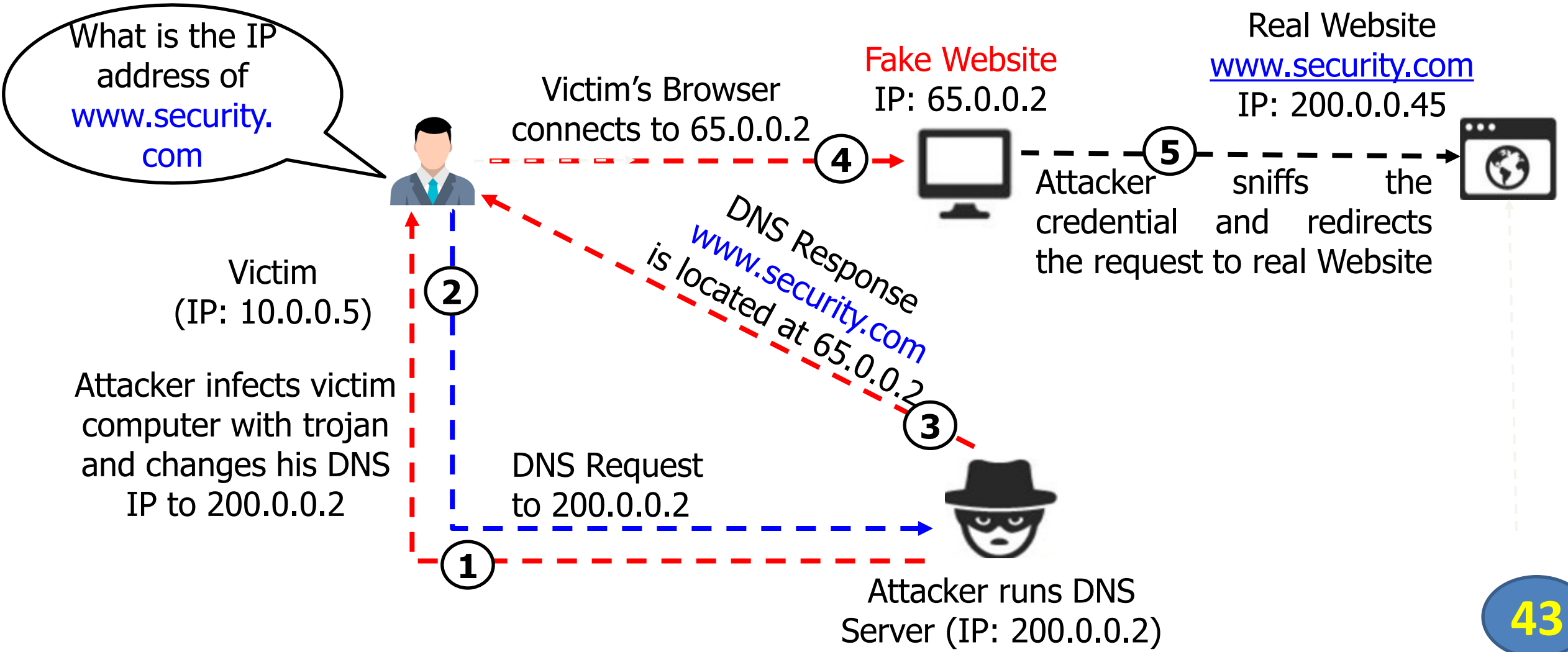
Intranet DNS Spoofing

- Trong kỹ thuật này, hệ thống của attacker phải được kết nối với mạng cục bộ (LAN) và có thể nghe lén các gói tin
- Nó hoạt động tốt với switches sử dụng ARP Poison Routing



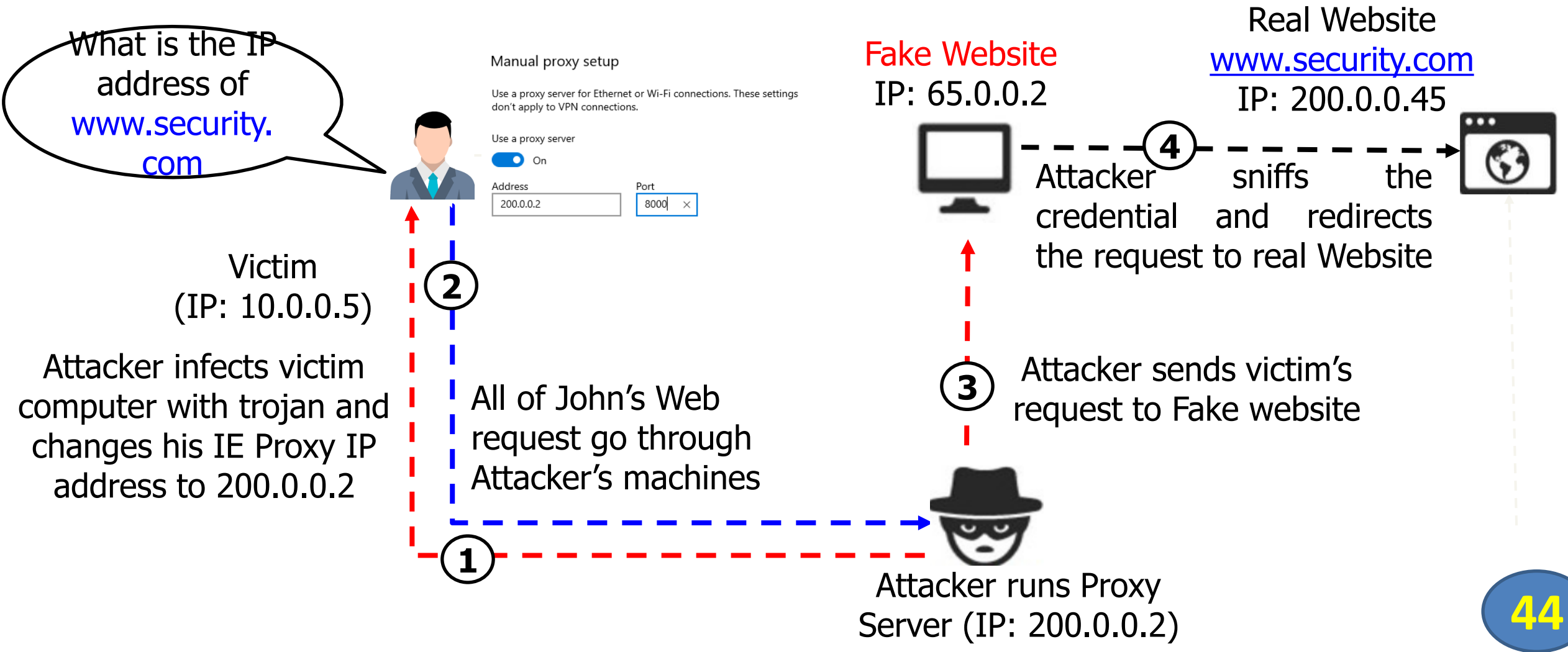
Internet DNS Poisoning

❑ Attacker thực hiện lây nhiễm máy tính người dùng với trojan và thay đổi địa chỉ DNS server trên máy người dùng trỏ về địa chỉ IP của attacker



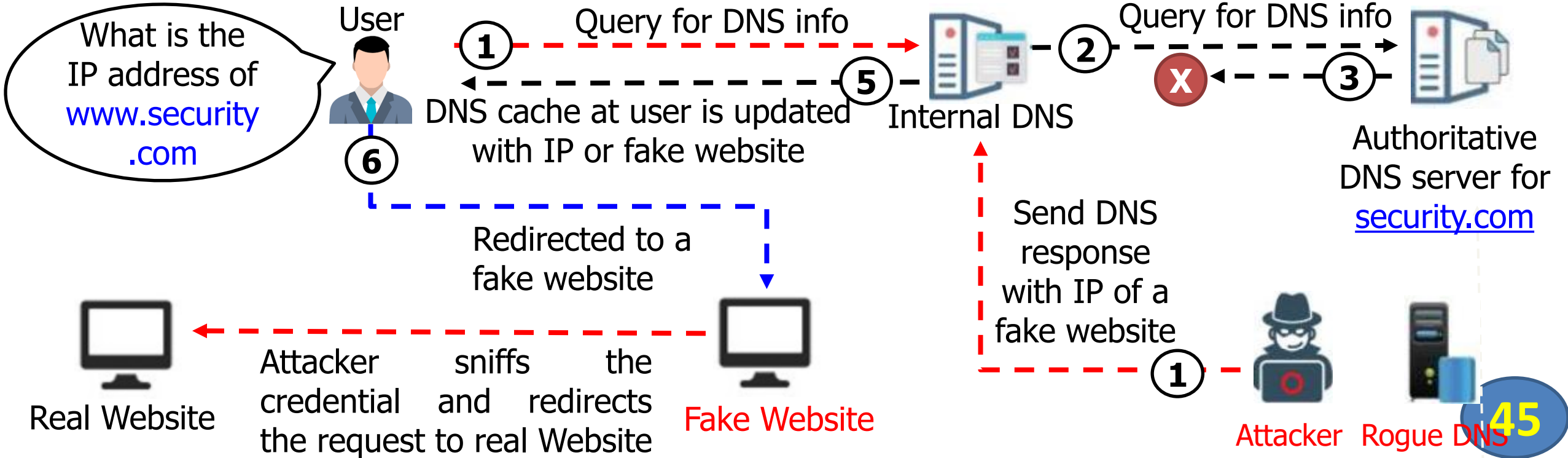
Proxy Server DNS Poisoning

❑ Kẻ tấn công gửi Trojan đến máy nạn nhân để thay đổi cài đặt trên máy chủ proxy và chuyển hướng đến trang web giả mạo



DNS Cache Poisoning

- DNS Cache Poisoning đề cập đến việc thay đổi hoặc thêm DNS record giả mạo vào DNS resolver cache dẫn đến việc chuyển hướng đến một trang web độc hại
- Nếu DNS resolver không thể xác thực được các DNS response đã được nhận từ một nguồn có thẩm quyền thì nó sẽ lưu các "entries" không chính xác vào cache và phân phát chúng cho những người dùng đưa ra yêu cầu tương tự



DNS Poisoning Tool

- DerpNSpoof
- DNS Spoof
- DNS-poison
- Ettercap
- Evilgrade
- DNS Poisoning Tool

How to Defend Against DNS Spoofing (1/2)

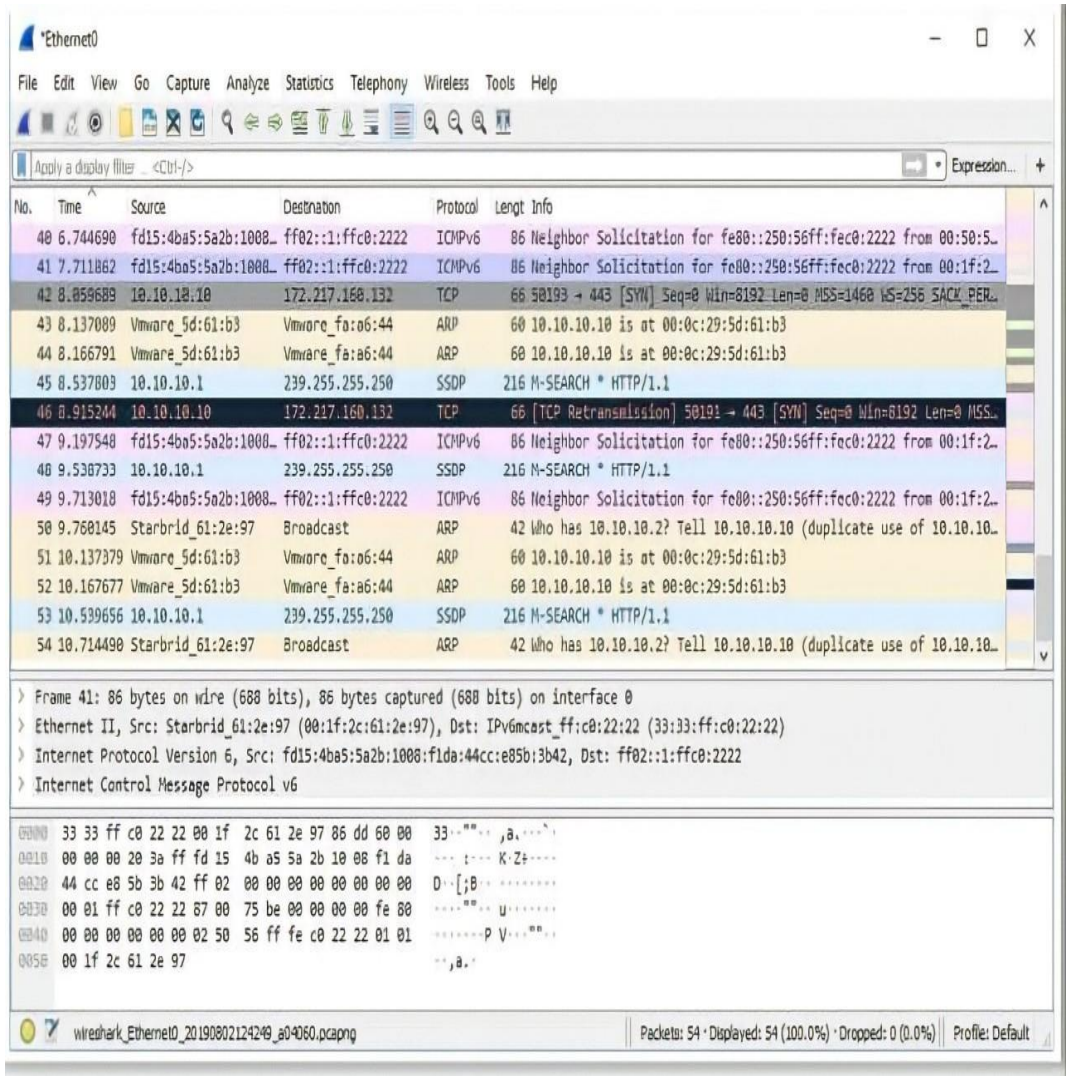
- Triển khai DNSSEC Extension
- Sử dụng SSL để bảo mật lưu lượng
- Phân giải tất cả các truy vấn DNS đến local DNS server
- Chặn DNS request được gửi đến external servers
- Cấu hình FW để hạn chế external DNS lookup
- Triển khai IDS
- Cấu hình DNS resolver để sử dụng cổng nguồn ngẫu nhiên mới cho mỗi truy vấn gửi đi

How to Defend Against DNS Spoofing (2/2)

- Hạn chế DNS recusing service (toàn bộ hoặc một phần) đối với người dùng được uỷ quyền.
- Sử dụng DNS Non-Existent Domain (NXDOMAIN) rate limiting.
- Bảo mật các máy nội bộ.
- Sử dụng statics ARP và IP tables.
- Không cho phép lưu lượng gửi đi sử dụng cổng UDP 53 làm cổng nguồn mặc định
- Kiểm tra và kiểm toán máy chủ DNS thường xuyên để loại bỏ các lỗ hổng.

Sniffing Tool: Wireshark

- Wireshark cho phép bạn thu thập và tương tác với lưu lượng đang chạy trên mạng.
- Wireshark sử dụng Winpcap để thu thập gói tin trên mạng.
- Wireshark thu thập lưu lượng mạng trực tiếp từ mạng Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay và FDDI.
- Một bộ lọc để hiển thị dữ liệu tuỳ chỉnh có thể được sử dụng.



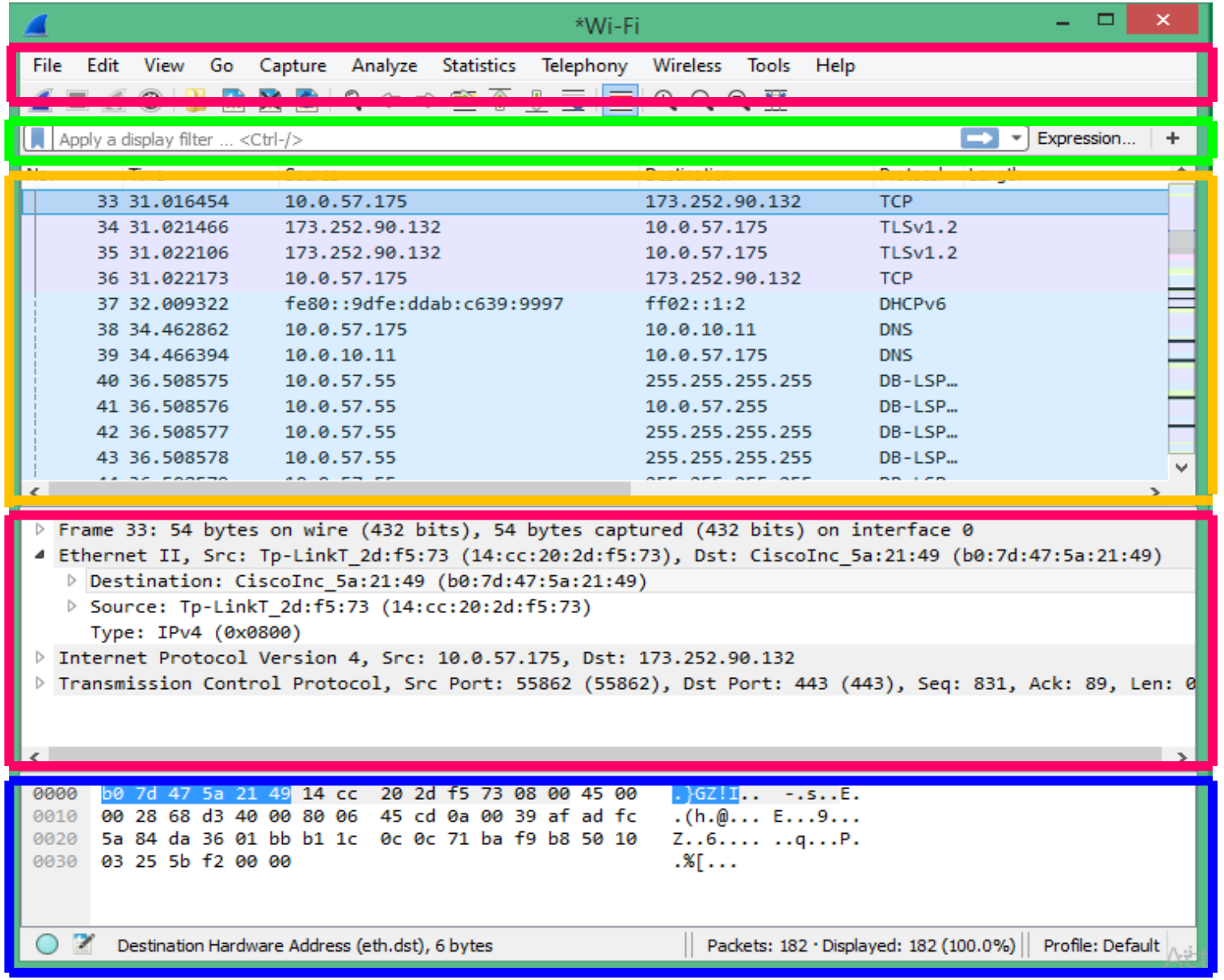
Sniffing Tool: Wireshark

1. Thanh công cụ
2. Bộ lọc

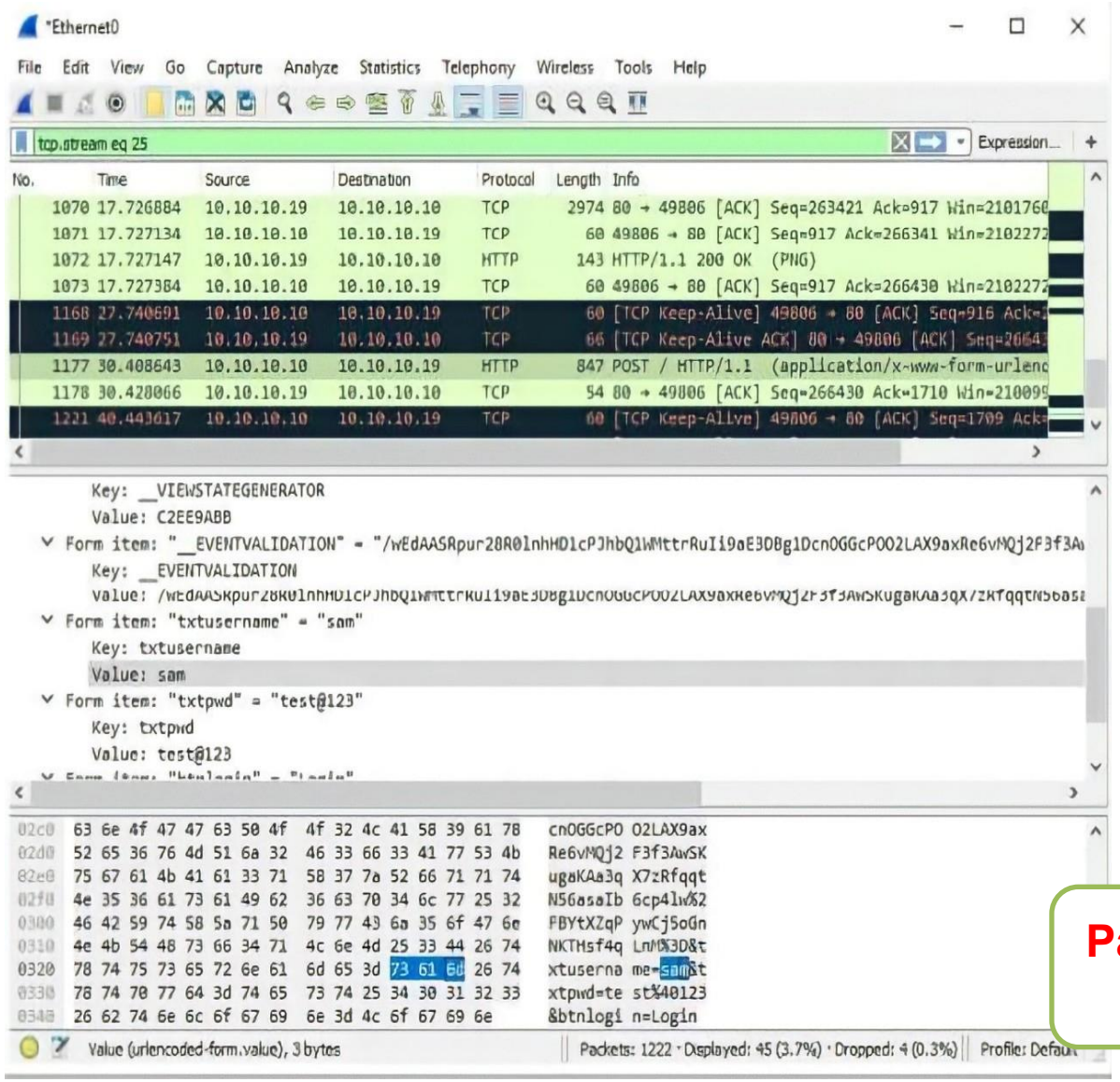
3. Danh sách các gói tin bắt được

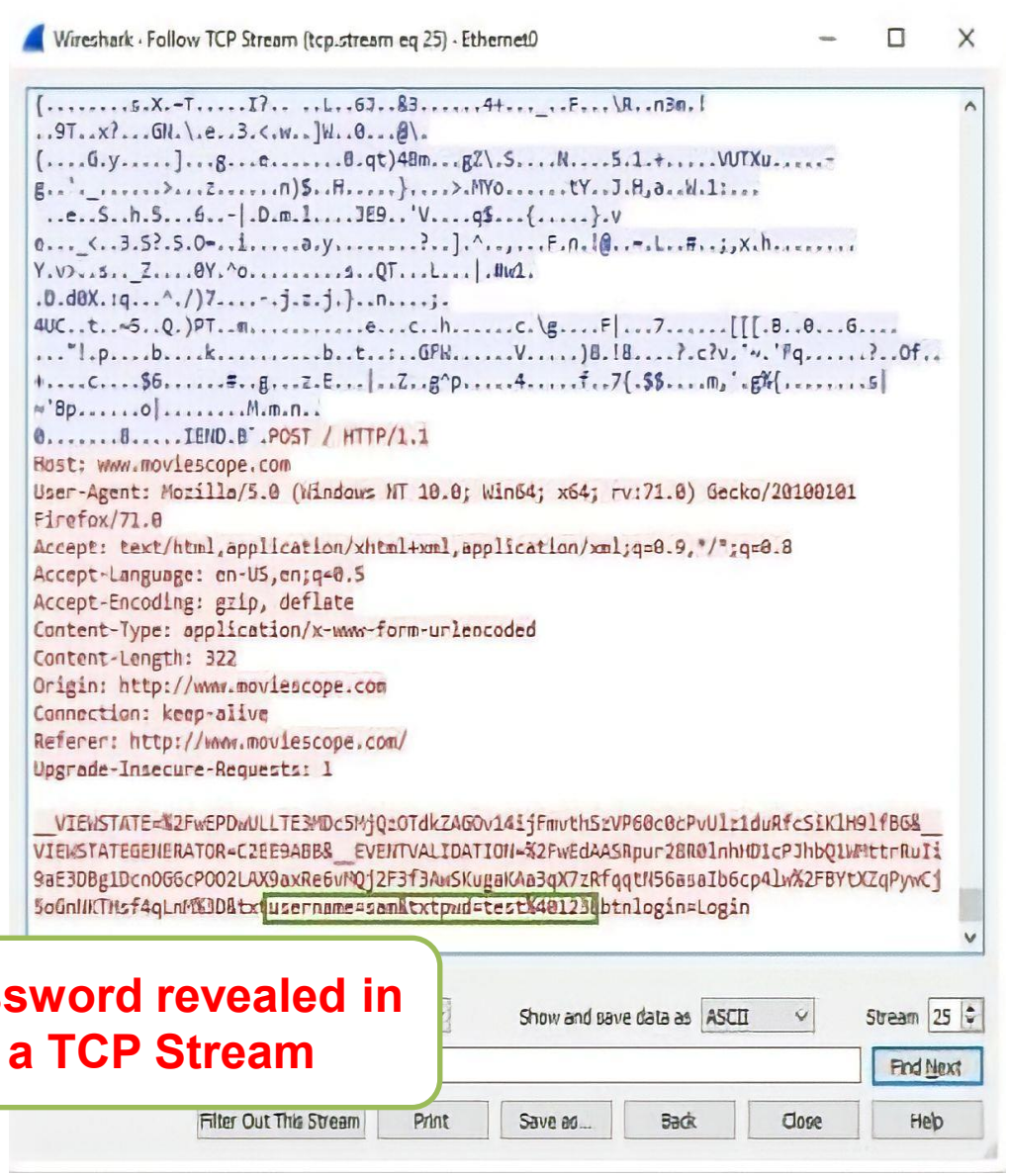
4. Thông tin chi tiết về gói tin được chọn

5. Nội dung gói tin ở dạng hex và ASCII



Follow TCP Stream in Wireshark





Password revealed in a TCP Stream

Display Filters in Wireshark

Display Filtering by Protocol	❑ Ví dụ: Nhập giao thức vào hộp bộ lọc: arp, http, tcp, udp, dns, hoặc ip
Monitoring the Specific Ports	❑ tcp.port==23 ❑ ip.addr==192.168.1.100 && tcp.port=23
Filtering by IP Addresses	❑ ip.addr == 10.0.0.4 or ip.addr == 10.0.0.5 ❑ ip.addr == 10.0.0.4
Other Filters	❑ ip.dst == 10.0.1.50 && frame.pkt_len > 400 ❑ ip.addr == 10.0.1.12 && icmp && frame.number > 15 && frame.number < 30 ❑ ip.src==205.153.65.30 or ip.dst==205.153.63.30

Sniffing Tools

- Observer Analyzer
- OmmiPeek
- Caspa Network Analyzer
- PRTG Network Monitor
- SolarWinds
- Xplico
- Colasoft Packet Builder
- Sniffer Wicap (for Mobile)
- FaceNiff (for Mobile)
- Packet Capture (for Mobile)

Additional Sniffing Tools

- PRTG Network Monitor
- CommView
- Csniffer
- Colasoft Packet Builder
- NetResident
- Ether Ape
- RSA NetWitness Investigator
- ntopng
- Network Probe
- Tcpdump
- smartSniff
- WebsiteSniffer
- NetFlow Analyzer
- Free Network Analyzer
- Kismet

1 Tổng quan

2 Một số kỹ thuật nghe lén và biện pháp phòng chống

3 Kỹ thuật phát hiện nghe lén

How to Detect Sniffing

Check the Devices Running in Promiscuous Mode

- Kiểm tra xem có máy nào đang chạy ở chế độ promiscuous hay không.
- Chế độ Promiscuous cho phép một thiết bị mạng có thể đánh chặn và đọc từng các gói tin được gửi đến.

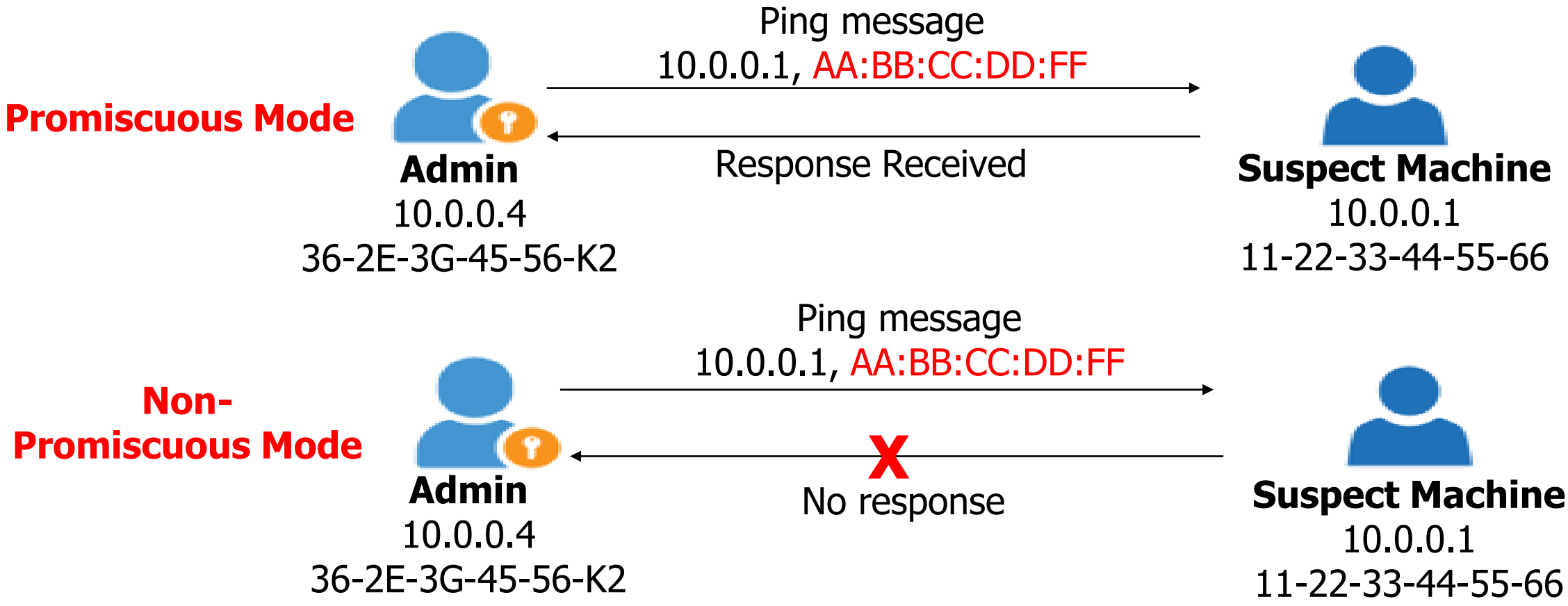
Run IDS

- IDS có thể thông báo cho quản trị viên về các hành động đáng ngờ như địa chỉ MAC của một thiết bị bất kỳ thay đổi.

Run Network Tools

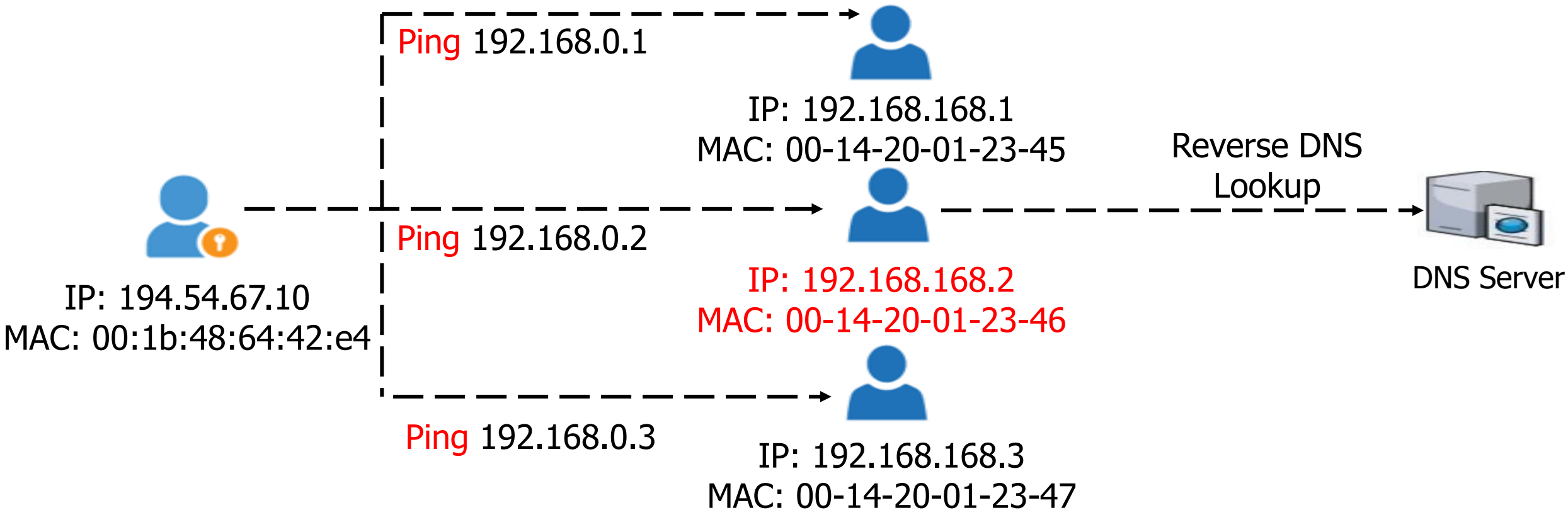
- Sử dụng các công cụ giám sát mạng cho việc phát hiện các gói nghi ngờ

Sniffer Detection Techniques: Ping Method



- Gửi ping request tới máy nghi ngờ với địa chỉ IP và địa chỉ MAC không chính xác. Ethernet adapter sẽ từ chối nó vì địa chỉ MAC không khớp, trong khi máy nghi ngờ chạy sniffer sẽ phản hồi vì nó không chối các gói có địa chỉ MAC khác.

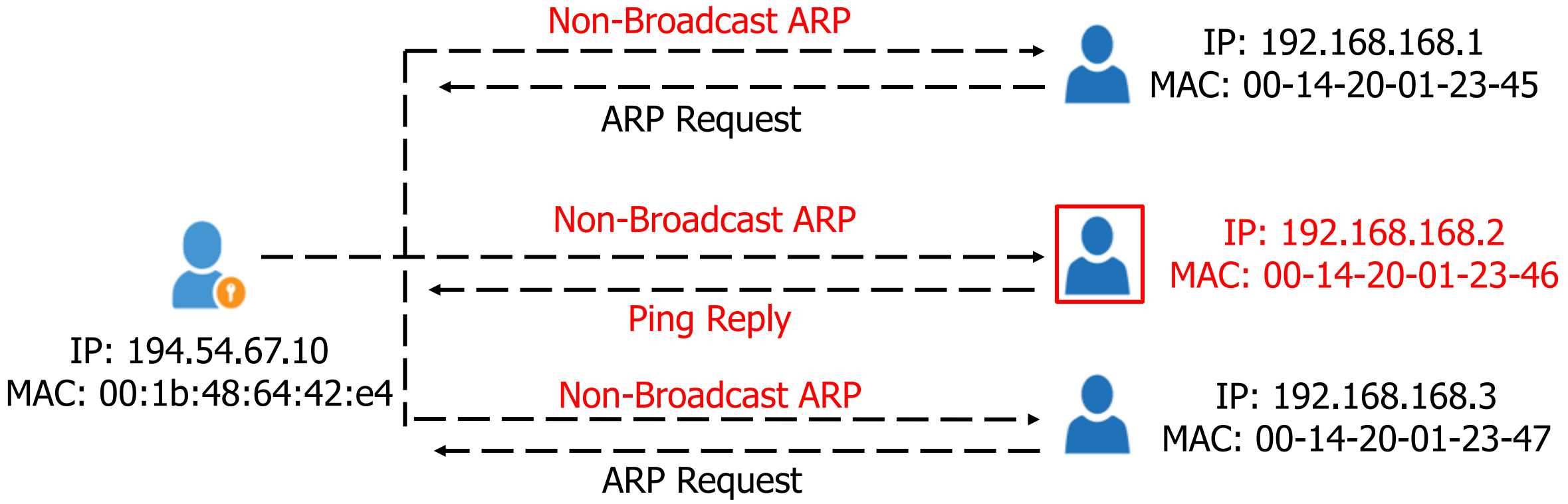
Sniffer Detection Techniques: DNS Method



- Hầu hết các chương trình sniffer thực hiện "reverse DNS lookup" để xác định máy qua địa chỉ IP (chuyển từ IP sang domain)
- Máy tính tạo ra "reverse DNS lookup" rất có khả năng đang chạy sniffer.

Sniffer Detection Techniques: ARP Method

- Chỉ có máy tính ở chế độ Promiscuous thực hiện lưu trữ thông tin ARP (ánh xạ địa chỉ IP và địa chỉ MAC)
- Máy tính ở chế độ Promiscuous sẽ trả lời gói ping vì nó có thông tin chính xác về máy chủ gửi yêu cầu ping trong bộ nhớ cache của nó, các máy còn lại sẽ gửi "ARP request" để xác định nguồn gốc của yêu cầu ping.

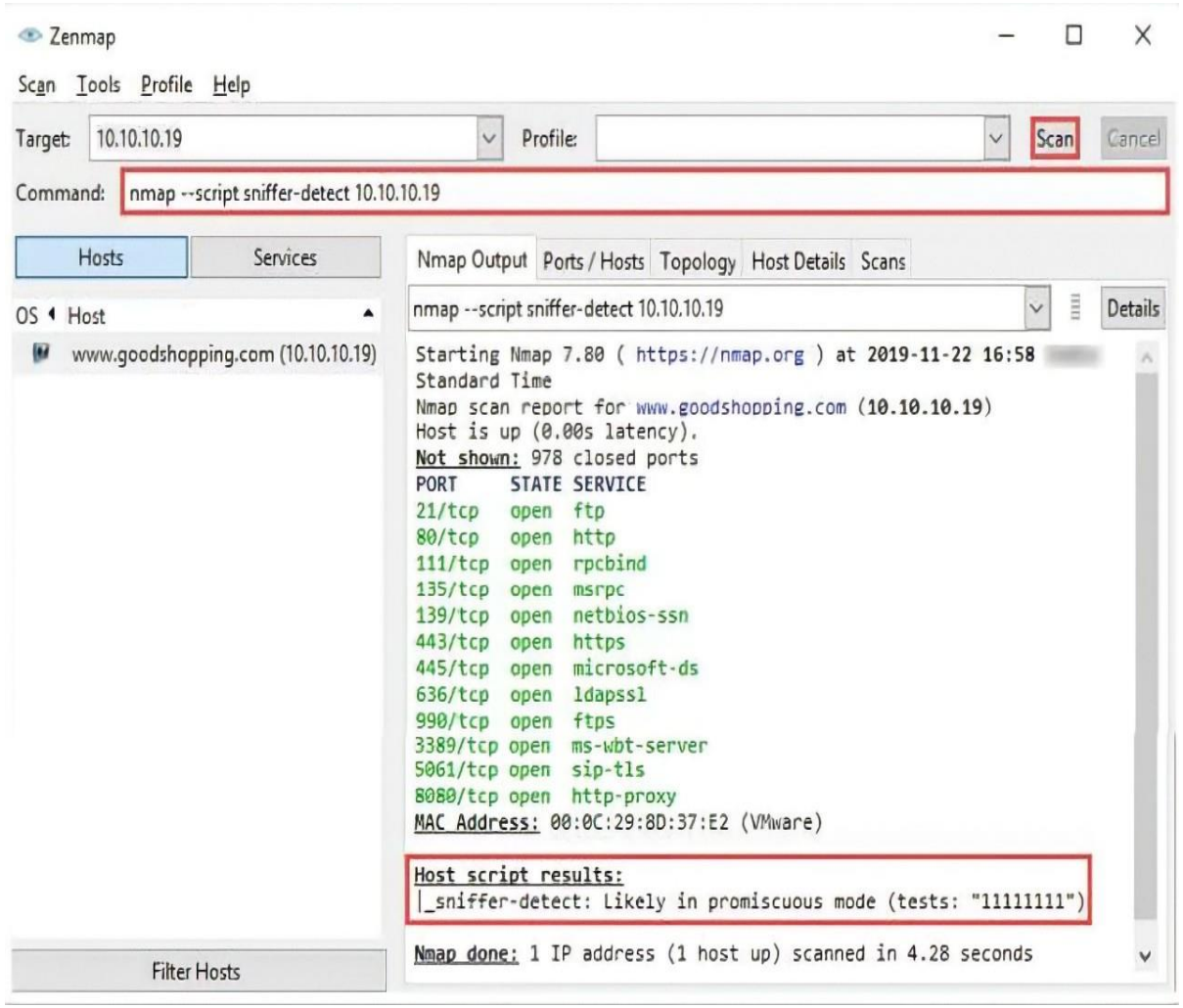


Promiscuous Detection Tool

- **Nmap's NSE script** cho phép kiểm tra xem một hệ thống trên mạng local có NIC đang ở chế độ Promiscuous hay không.

  nmap --script=sniffer-detect [Target]

- **NetScan Tools Pro** bao gồm công cụ Promiscuous Mode Scanner có khả năng phát hiện NIC đang ở chế độ Promiscuous.
- **PromqryUI 1.0** - công cụ của Microsoft có thể sử dụng để phát hiện NIC đang chạy ở chế độ promiscuous

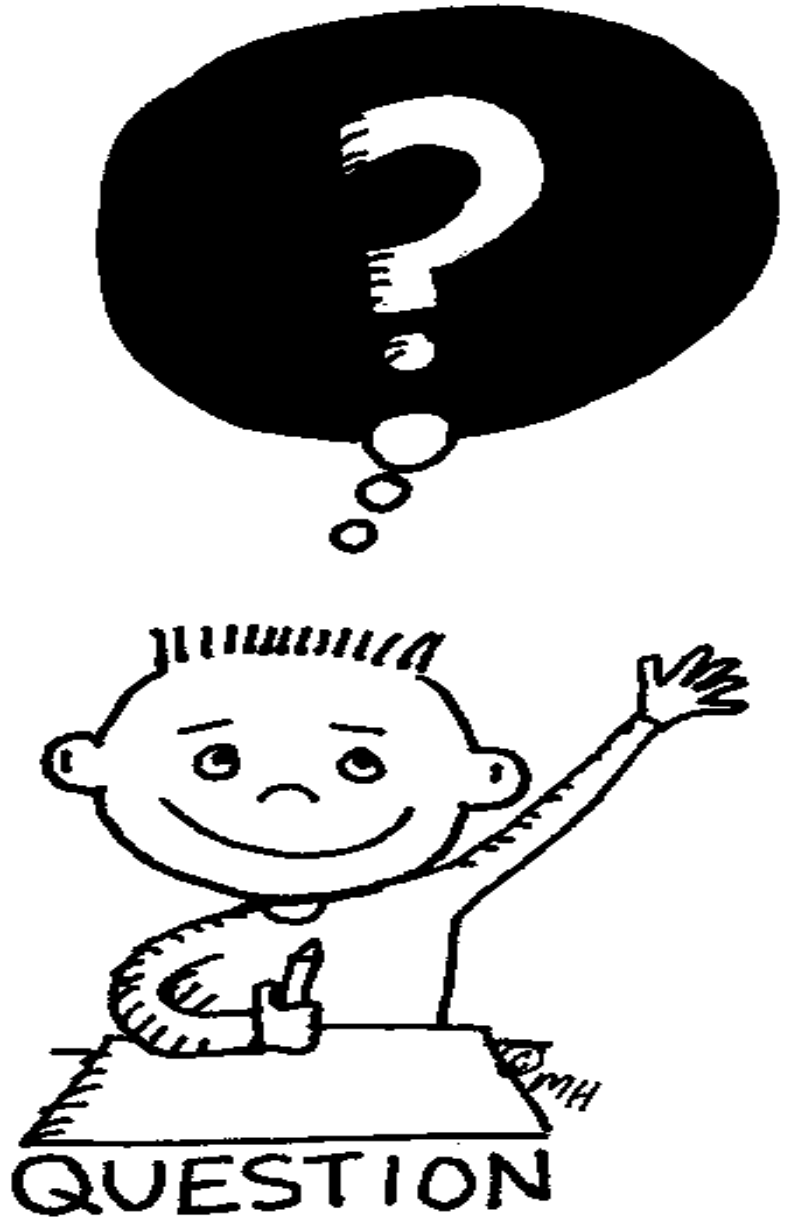


How to defend again sniffing (1/2)

- Hạn chế truy cập vật lý tới hạ tầng mạng
- Sử dụng mã hóa đầu cuối để bảo vệ thông tin bí mật
- Thêm vĩnh viễn địa chỉ MAC và cổng tương ứng vào bộ nhớ cache ARP
- Sử dụng địa chỉ IP tĩnh và bảng ARP để ngăn kẻ tấn công thêm các "ARP entries" giả mạo cho các máy trong mạng
- Tắt "network identification broadcasts" và hạn chế người dùng được ủy quyền
- Sử dụng các giao thức mã hóa như SSH, SCP, HTTPS, TLS/SSL… để bảo vệ người dùng
- Sử dụng IPv6 thay vì IPv4

How to defend again sniffing (2/2)

- Sử dụng switch thay vì hub vì switch chỉ cung cấp dữ liệu cho người nhận xác định.
- Lấy MAC trực tiếp từ NIC thay vì OS. Điều này giúp ngăn chặn việc giả mạo địa chỉ MAC.
- Sử dụng công cụ để xác định xem có NIC nào đang chạy ở chế độ quảng bá hay không.
- Sử dụng "access-control lists" (ACL) để chỉ cho phép truy cập vào một dải địa chỉ IP tin cậy trong mạng.


QUESTION