Module 10

Sniffing and Spoofing

Ansh Bhawnani

Sniffing Concepts

Module 10

1. Introduction

Module 10

Sniffing Concepts

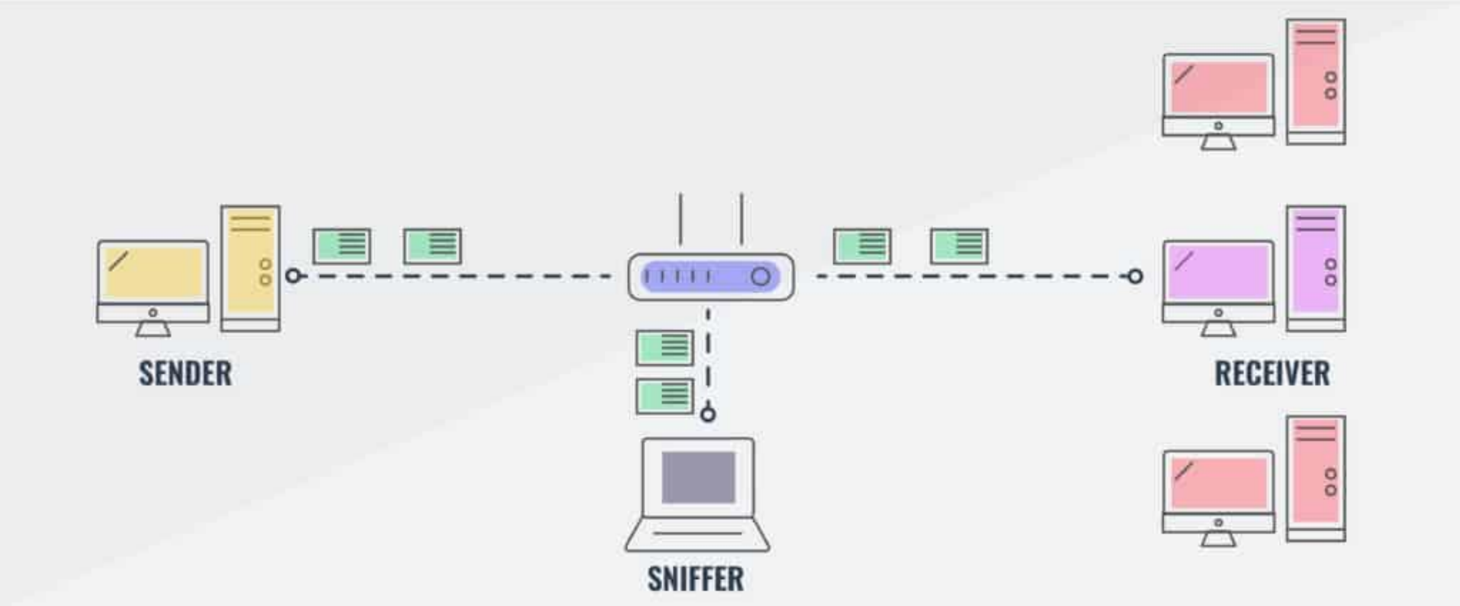
- Sniffing is a process of monitoring and capturing all data packets passing through a given network using sniffing tools.
- It is a form of wiretap applied to computer networks.
- Many enterprises' switch ports are open.
- Anyone in the same physical location can plug into the network using an Ethernet cable.

Sniffing Concepts

How a Sniffer Works

- **Promiscuous Mode**: Sniffer turns the NIC of a system to the promiscuous mode so that it listens to all the data transmitted on its segment.
- **Decode Information**: A sniffer can constantly monitor all the network traffic to a computer through the NIC by decoding the information encapsulated in the data packet.

Sniffing Concepts



2. Types of Sniffing

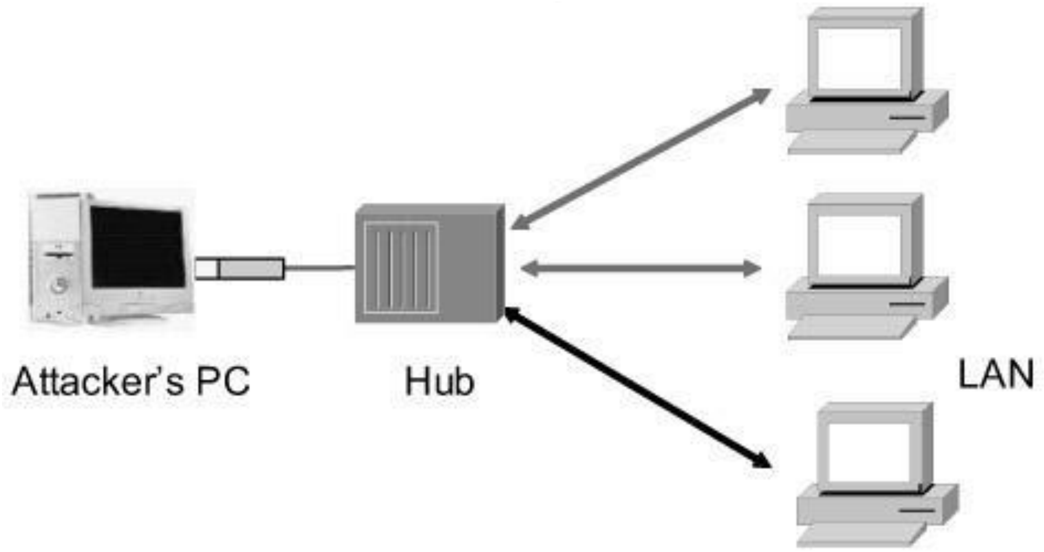
Module 10

Sniffing Concepts

Passive Sniffing

- Passive sniffing means sniffing through a hub, on a hub the traffic is sent to all ports.
- It involves only monitoring of the packets sent by others without sending any additional data packets in the network traffic.
- In a network that use hubs to connect systems, all hosts on the network can see all traffic therefore attacker can easily capture traffic going through the hub.
- Hub usage is out-dated today. Most modern networks use switches.

Sniffing Concepts

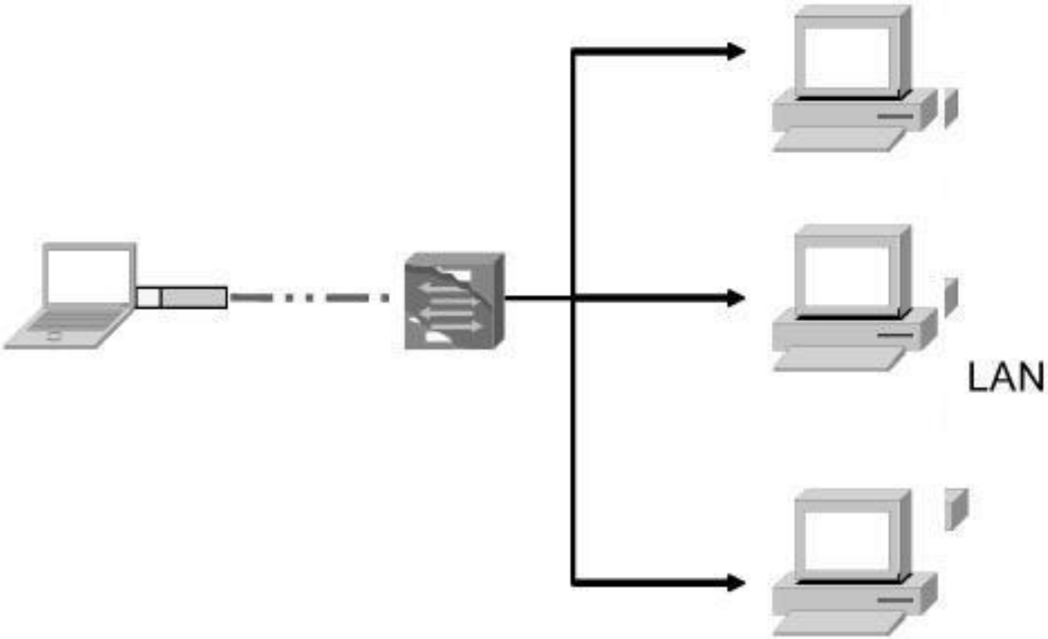


Sniffing Concepts

Active Sniffing

- Active sniffing is used to sniff a switch-based network.
- The attacker forces a switch to act like a hub.
- Active sniffing involves injecting address resolution packets (ARP) into the network to flood the switch's Content Addressable Memory (CAM) table, CAM keeps track of which host is connected to which port.

Sniffing Concepts



Sniffing Concepts

- **Active Sniffing Techniques**:
  - MAC Flooding
  - DNS Poisoning
  - ARP Poisoning
  - DHCP Attacks
  - Switch Port Stealing
  - Spoofing Attack

Sniffing Concepts

How an Attacker Hacks the Network Using Sniffers

- An attacker connects his laptop to a switch port.
- He runs discovery tools to learn about network topology.
- He identifies victim's machine to target his attacks.
- He poisons the victim machine by using ARP spoofing techniques.
- The traffic destined for the victim machine is redirected to the attacker.
- The hacker extracts passwords and sensitive data from the redirected traffic.

Sniffing Concepts

Protocol Vulnerable to Sniffing

- **HTTP**: Data sent in clear text
- **Telnet and Rlogin**: Keystrokes including user names and passwords
- **POP**: Passwords and data sent in clear text
- **IMAP**: Passwords and data sent in clear text
- **SMTP and NNTP**: Passwords and data sent in clear text
- **FTP**: Passwords and data sent in clear text

Sniffing Concepts

Sniffing in the Data Link Layer of the OSI Model

- Sniffers operate at the Data Link layer of the OSI model.
- Networking layers in the OSI model are designed to work independently of each other; if a sniffer sniffs data in the Data Link layer, the upper OSI layer will not be aware of the sniffing.

3. Hardware Protocol Analyzer

Module 10

Sniffing Concepts

Hardware Protocol Analyzer

- A hardware protocol analyzer is a piece of equipment that captures signals without altering the traffic in a cable segment.
- It can be used to monitor network usage and identify malicious network traffic generated by hacking software installed in the network.
- It captures a data packet, decodes it, and analyzes its content according to certain predetermined rules.
- It allows attacker to see individual data bytes of each packet passing through the cable.

Sniffing Concepts

Keysight N2X N5540A

Keysight E2960B

RADCOM PrismLite Protocol Analyzer

RADCOM Prism UltraLite
Protocol Analyzer

FLUKE Networks OptiView® XG
Network Analyzer

FLUKE Networks OneTouch™
AT Network Assistant

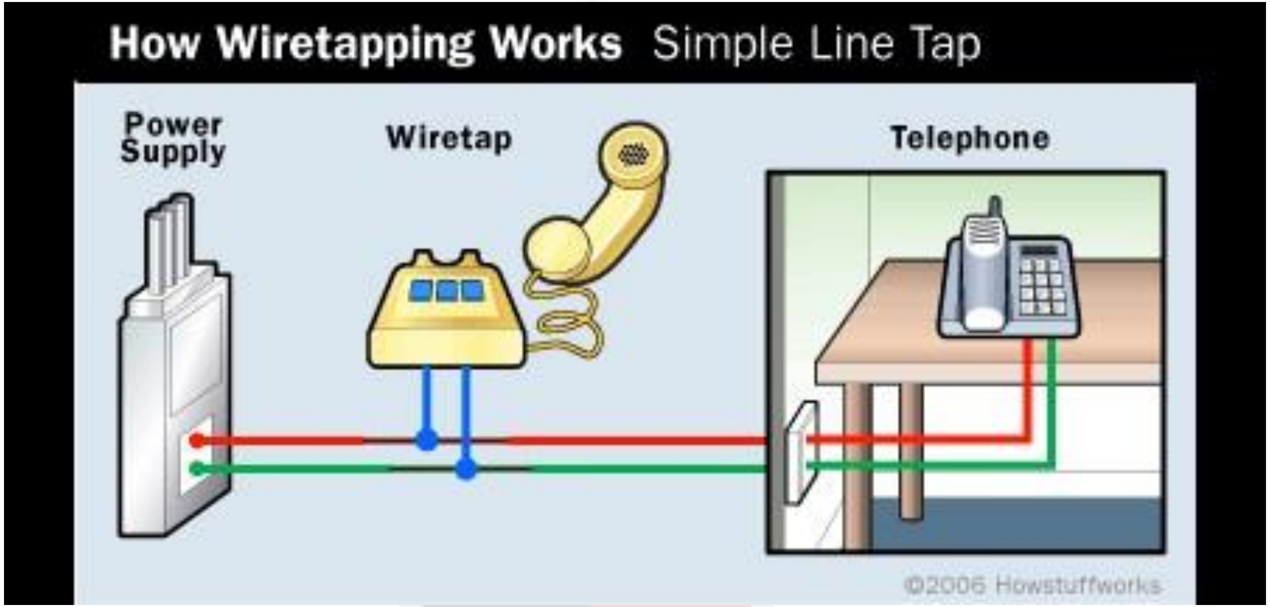
4. Wiretapping

Module 10

Sniffing Concepts

- Wiretapping is the process of monitoring telephone and Internet conversations by a third party.
- Attackers connect a listening device (hardware/software) to the circuit carrying information between two phones or hosts on the Internet.
- It allows an attacker to monitor, intercept, access, and record information contained in a data flow in a communication system.
- **Types of Wiretapping**:
  - **Active Wiretapping**: It monitors, records, alters and also injects something into the communication or traffic.
  - **Passive Wiretapping**: It only monitors and records the traffic and gain knowledge of the data it contains.

Sniffing Concepts



Sniffing Concepts

Lawful Interception

- Lawful interception refers to legally intercepting data communication between two end points for surveillance on the traditional telecommunications, VoIP, data, and multiservice networks.

Wiretapping Case Study: PRISM

- PRISM stands for "Planning Tool for Resource Integration, Synchronization, and Management," and is a "data tool" designed to collect and process "foreign intelligence" that passes through American servers.
- NSA wiretaps a huge amount of foreign internet traffic that is routed through or saved on U.S. servers.

MAC Attacks

Module 10

1. MAC Flooding

Module 10

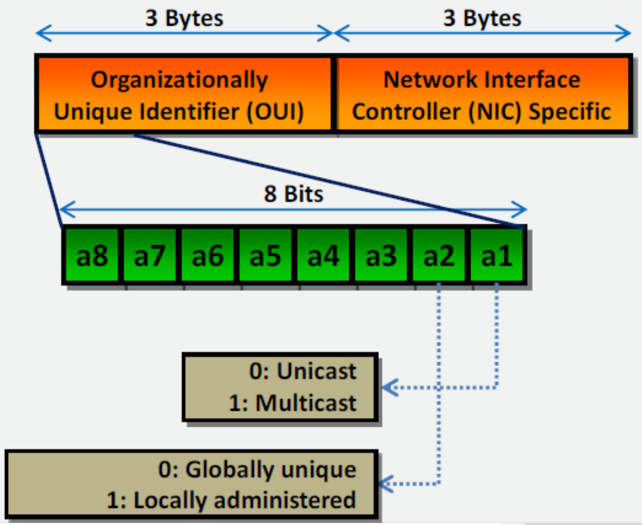
MAC Attacks

MAC Address/CAM Table

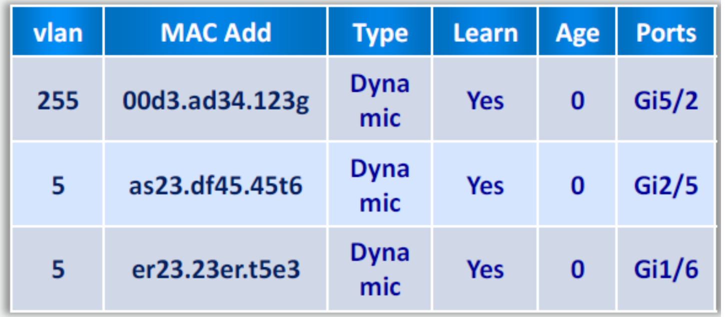
- Each switch has a fixed size dynamic Content Addressable Memory (CAM) table.
- The CAM table stores information such as MAC addresses available on physical ports with their associated VLAN parameters.

MAC Attacks

MAC Address

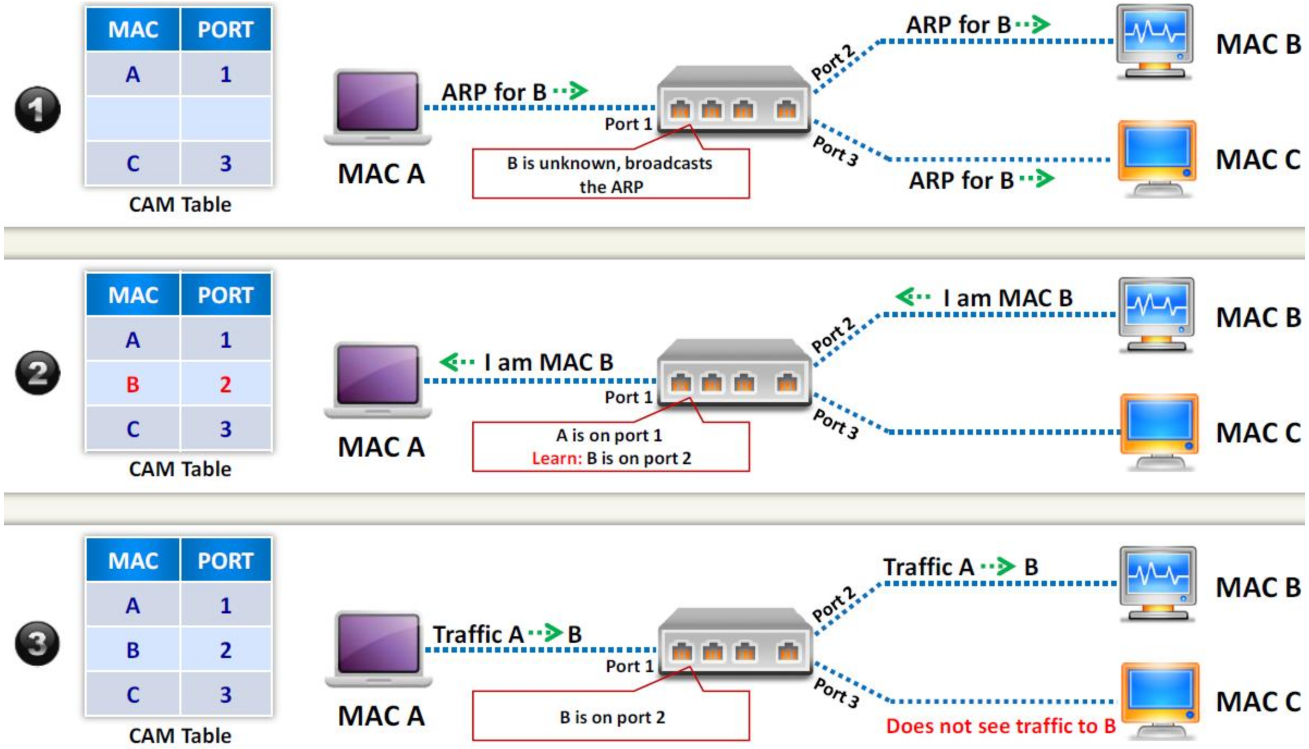


CAM Table



vlan	MAC Add	Type	Learn	Age	Ports
255	00d3.ad34.123g	Dyna mic	Yes	0	Gi5/2
5	as23.df45.45t6	Dyna mic	Yes	0	Gi2/5
5	er23.23er.t5e3	Dyna mic	Yes	0	Gi1/6

MAC Attacks



1

MAC	PORT
A	1
C	3

CAM Table

2

MAC	PORT
A	1
B	2
C	3

CAM Table

3

MAC	PORT
A	1
B	2
C	3

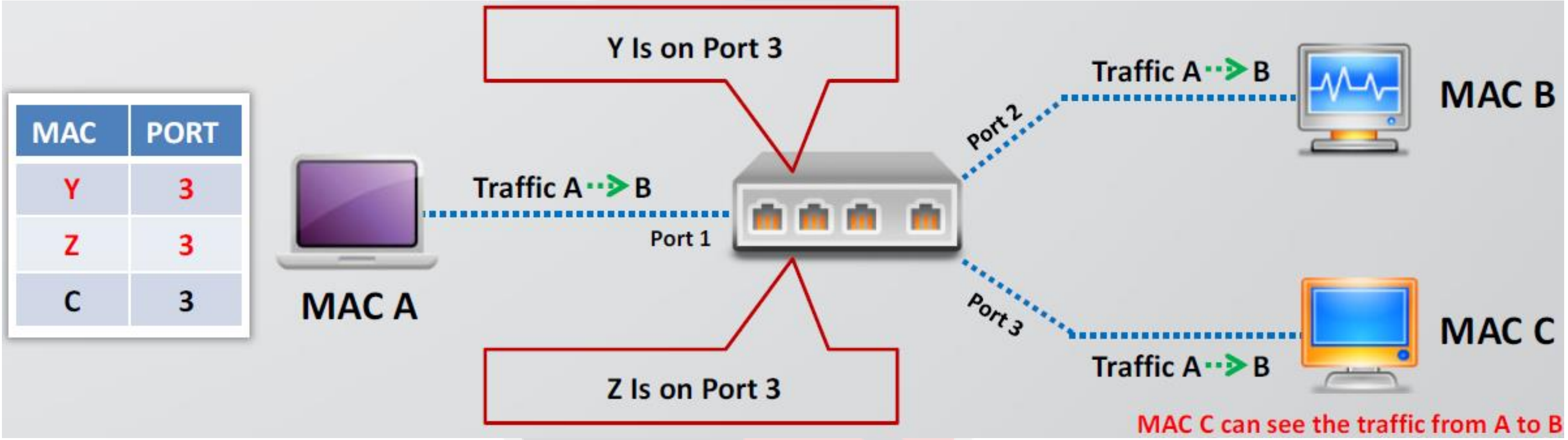
CAM Table

MAC Attacks

What Happens When CAM Table Is Full?

- Once the CAM table on the switch is full, additional ARP request traffic will flood every port on the switch.
- This will change the behavior of the switch to reset to it's learning mode or fail open mode, broadcasting on every port similar to a hub.
- This attack will also fill the CAM tables of adjacent switches.

MAC Attacks



MAC	PORT
Y	3
Z	3
C	3

MAC C can see the traffic from A to B

MAC Attacks

MAC Flooding

- MAC flooding involves flooding of CAM table with fake MAC address and IP pairs until it is full.
- Switch then acts as a hub by broadcasting packets to all machines on the network and attackers can sniff the traffic easily.

2. Switch Port Stealing

Module 10

MAC Attacks

- Switch Port Stealing sniffing technique uses MAC flooding to sniff the packets.
- Attacker floods the switch with forged gratuitous ARP packets with target MAC address as source and his own MAC address as destination.
- A race condition of attacker's flooded packets and target host packets will occur and thus switch has to change his MAC address binding constantly between two different ports.

MAC Attacks

- In such case if attacker is fast enough, he will able to direct the packets intended for the target host toward his switch port.
- Attacker now manages to steal the target host switch port and sends ARP request to stolen switch port to discover target hosts' IP address.
- When attacker gets ARP reply, this indicates that target host's switch port binding has been restored and attacker can now able to sniff the packets sent toward targeted host.

3. Defend against MAC attacks

Module 10

MAC Attacks

- Configuring Port Security on Cisco switch.
- Port security can be used to restrict inbound traffic from only a selected set of MAC addresses and limit MAC flooding attack.

DHCP Attacks

Module 10

1. How DHCP works

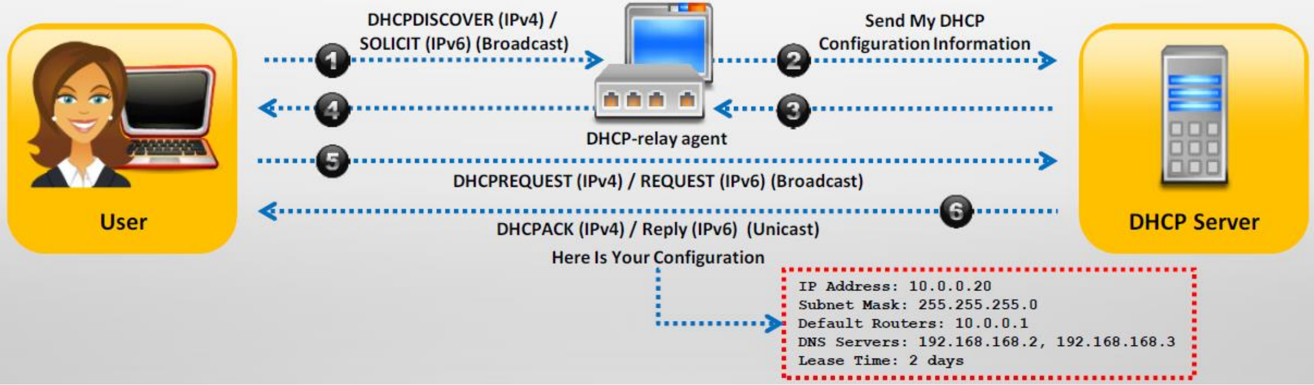
Module 10

DHCP Attacks

- DHCP servers maintain TCP/IP configuration information in a database such as valid TCP/IP configuration parameters, valid IP addresses, and duration of the lease offered by the server.
- It provides address configurations to DHCP-enabled clients in the form of a lease offer.
- Client broadcasts **DHCPDISCOVER/SOLICIT** request asking for DHCP Configuration Information.
- DHCP-relay agent captures the client request and unicasts it to the DHCP servers available in the network.
- DHCP server unicasts **DHCPOFFER/ADVERTISE**, which contains client and server's MAC address.

DHCP Attacks

- Relay agent broadcasts **DHCPOFFER/ADVERTISE** in the client's subnet.
- Client broadcasts **DHCPREQUEST/REQUEST** asking DHCP server to provide the DHCP configuration information.
- DHCP server sends unicast **DHCPACK/REPLY** message to the client with the IP config and information.


DHCPDISCOVER (IPv4) / SOLICIT (IPv6) (Broadcast)
1
Send My DHCP Configuration Information
2
3
4
DHCP-relay agent
5
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
6
DHCPACK (IPv4) / Reply (IPv6) (Unicast)
Here Is Your Configuration
User
DHCP Server

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days
```

DHCP Attacks

OP Code	Hardware Type	Hardware Length	HOPS
Transaction ID (XID)			
Seconds		Flags	
Client IP Address (CIADDR)			
Your IP Address (YIADDR)			
Server IP Address (SIADDR)			
Gateway IP Address (GIADDR)			
Client Hardware Address (CHADDR)—16 bytes			
Server Name (SNAME)—64 bytes			
Filename—128 bytes			
DHCP Options			

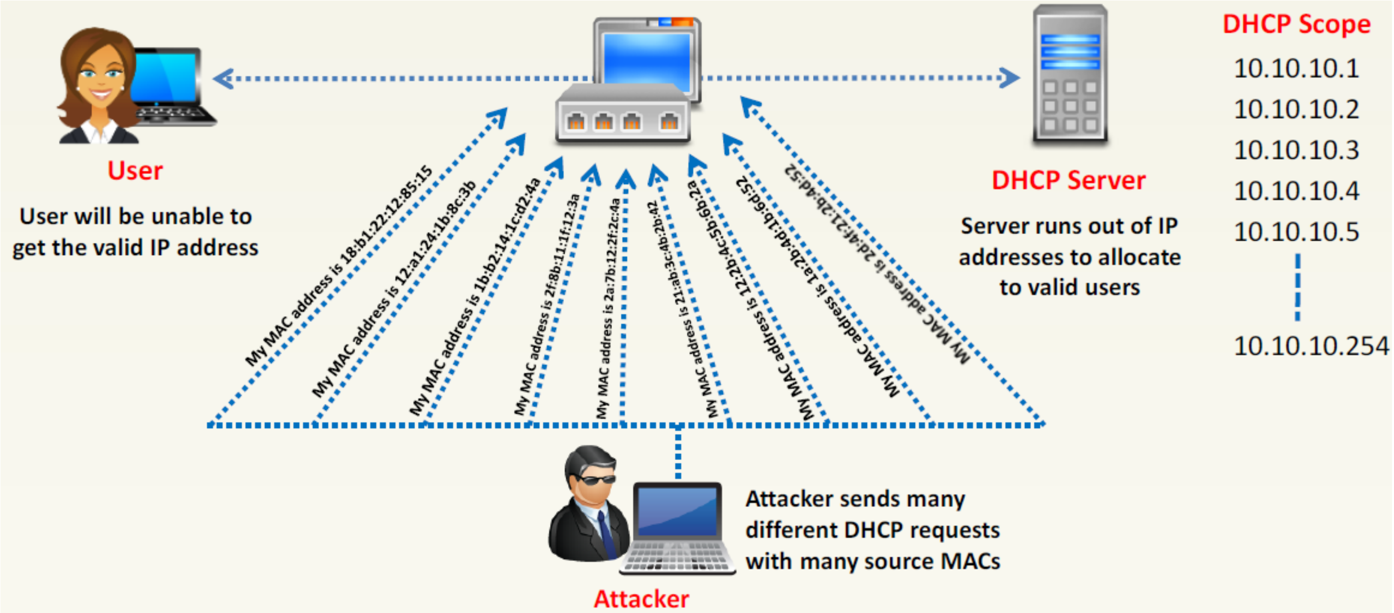
2. DHCP Starvation attack

Module 10

DHCP Attacks

- This is a denial-of-service (DoS) attack on the DHCP servers where attacker broadcasts forged DHCP requests and tries to lease all of the DHCP addresses available in the DHCP scope.
- As a result legitimate user is unable to obtain or renew an IP address requested via DHCP, failing access to the network access. .

DHCP Attacks



User
My MAC address is 18:b1:22:12:85:15
My MAC address is 12:a1:24:1b:8c:3b
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:2c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4C:5b:6b:2a
My MAC address is 1a:2b:4d:1b:6d:52
My MAC address is 2d:4f:21:2b:4d:52
DHCP Server
DHCP Scope
Attacker

User will be unable to get the valid IP address

Server runs out of IP addresses to allocate to valid users

DHCP Scope

10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.4
10.10.10.5
10.10.10.254

Attacker sends many different DHCP requests with many source MACs

DHCP Attacks

- This is a denial-of-service (DoS) attack on the DHCP servers where attacker broadcasts forged DHCP requests and tries to lease all of the DHCP addresses available in the DHCP scope.
- As a result legitimate user is unable to obtain or renew an IP address requested via DHCP, failing access to the network access. .

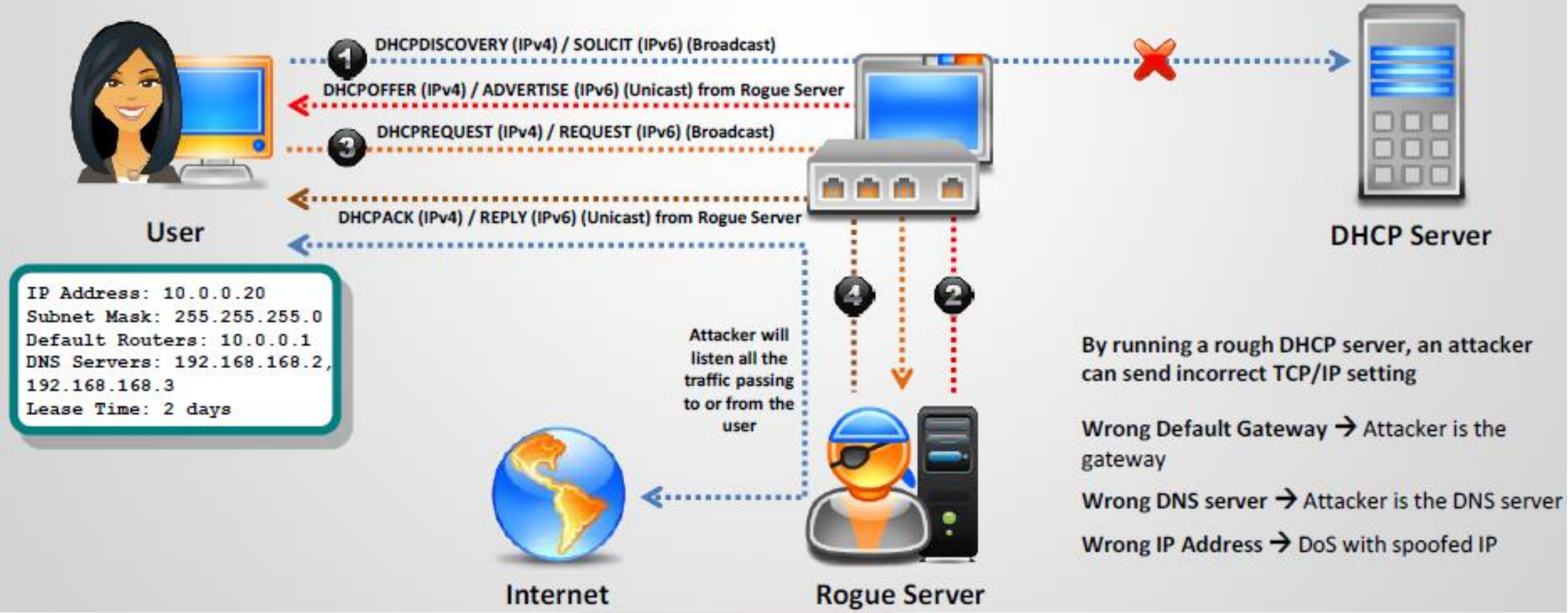
3. Rogue DHCP server attack

Module 10

DHCP Attacks

- Attacker sets rogue DHCP server in the network and responds to DHCP requests with bogus IP addresses; this results in compromised network access.
- This attack works in conjunction with the DHCP Starvation attack; attacker sends TCP/IP setting to the user after knocking him/her out from the genuine DHCP server.

DHCP Attacks


User
1
DHCPDISCOVERY (IPv4) / SOLICIT (IPv6) (Broadcast)
DHCPOFFER (IPv4) / ADVERTISE (IPv6) (Unicast) from Rogue Server
3
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
DHCPACK (IPv4) / REPLY (IPv6) (Unicast) from Rogue Server
DHCP Server
4
2
Attacker will listen all the traffic passing to or from the user
Internet
Rogue Server

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2,
192.168.168.3
Lease Time: 2 days
```

By running a rough DHCP server, an attacker can send incorrect TCP/IP setting

Wrong Default Gateway → Attacker is the gateway

Wrong DNS server → Attacker is the DNS server

Wrong IP Address → DoS with spoofed IP

4. Defend Against DHCP Starvation and Rogue Server Attack

Module 10

DHCP Attacks

- Enable port security to defend against DHCP starvation attack.
  - Configuring MAC limit on switch's edge ports drops the packets from further MACs once the limit is reached.
- Enable DHCP snooping that allows switch to accept DHCP transaction coming only from a trusted port.

ARP Attacks

Module 10

1. ARP Introduction

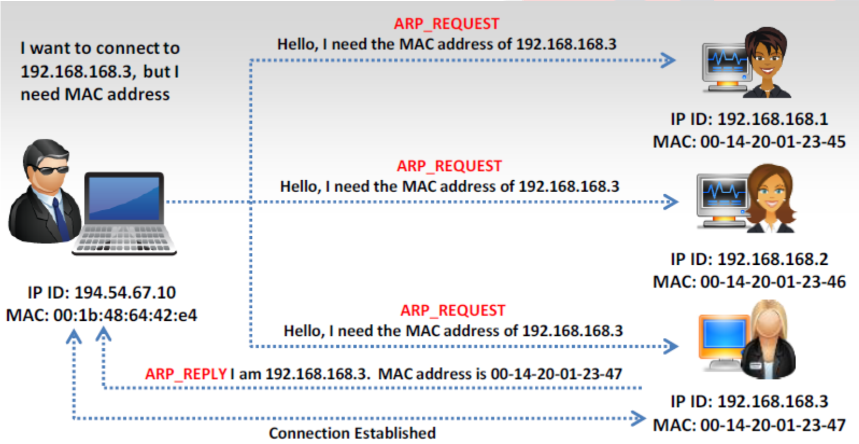
Module 10

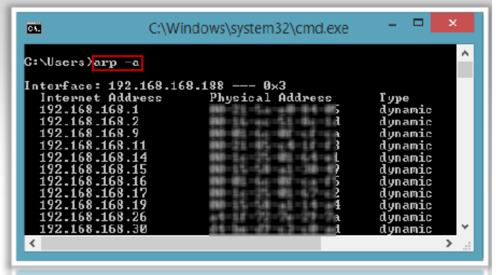
ARP Attacks

- Address Resolution Protocol (ARP) is a stateless protocol used for resolving IP addresses to machine (MAC) addresses.
- All network devices (that needs to communicate on the network) broadcasts ARP queries in the network to find out other machines' MAC addresses.
- When one machine needs to communicate with another, it looks up its ARP table. If the MAC address is not found in the table, the **ARP_REQUEST** is broadcasted over the network.
- All machines on the network will compare this IP address to their MAC address.

ARP Attacks

- If one of the machine in the network identifies with this address, it will respond to ARP_REQUEST with its IP and MAC address. The requesting machine will store the address pair in the ARP table and communication will take place.


I want to connect to 192.168.168.3, but I need MAC address
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.1
MAC: 00-14-20-01-23-45
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.2
MAC: 00-14-20-01-23-46
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 194.54.67.10
MAC: 00:1b:48:64:42:e4
ARP_REPLY I am 192.168.168.3. MAC address is 00-14-20-01-23-47
IP ID: 192.168.168.3
MAC: 00-14-20-01-23-47
Connection Established



```
C:\Users>arp -a

Interface: 192.168.168.188 --- 0x3
  Internet Address      Physical Address      Type
  192.168.168.1         [redacted]            dynamic
  192.168.168.2                               dynamic
  192.168.168.9                               dynamic
  192.168.168.11                              dynamic
  192.168.168.14                              dynamic
  192.168.168.15                              dynamic
  192.168.168.16                              dynamic
  192.168.168.17                              dynamic
  192.168.168.19                              dynamic
  192.168.168.26                              dynamic
  192.168.168.30                              dynamic
```

2. ARP Spoofing Attack

Module 10

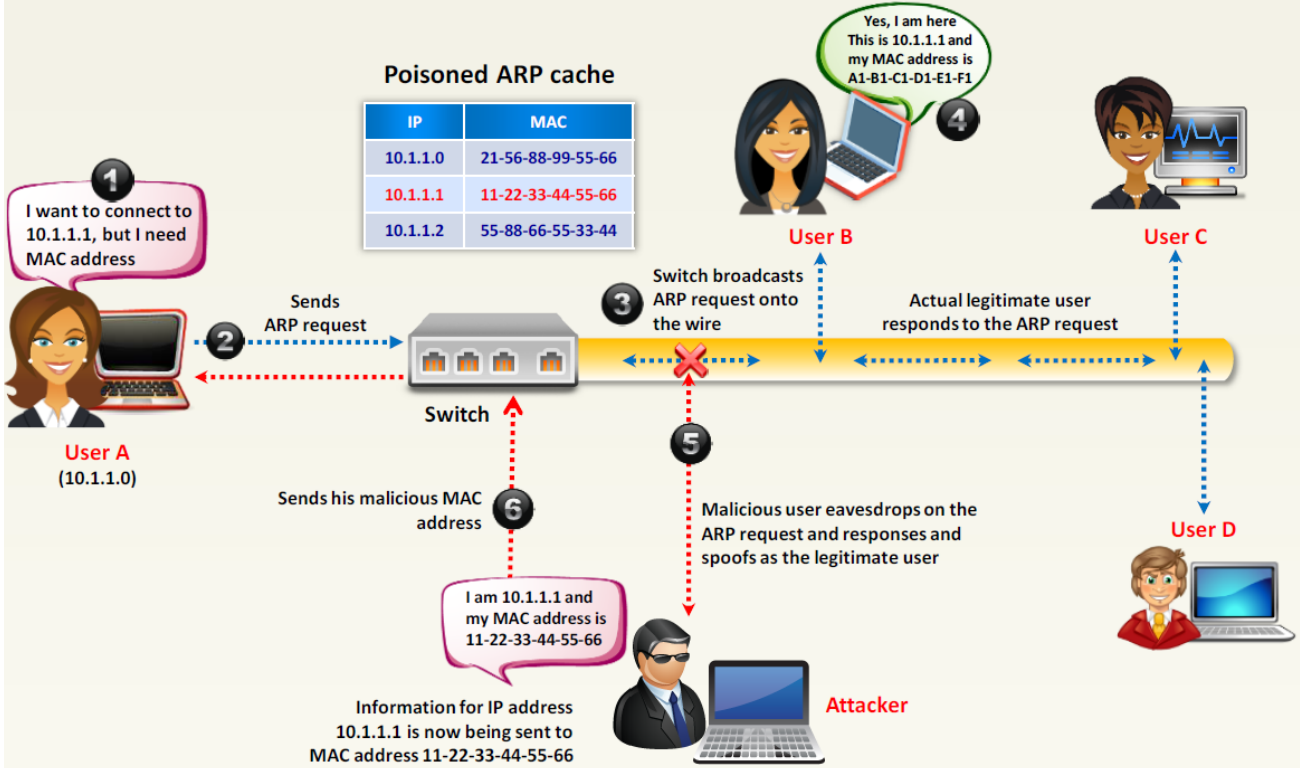
ARP Attacks

- ARP packets can be forged to send data to the attacker's machine.
- ARP Spoofing involves constructing a large number of forged ARP request and reply packets to overload a switch.
- Switch is set in "forwarding mode" after ARP table is flooded with spoofed ARP replies and attackers can sniff all the network packets.
- Attackers flood a target computer's ARP cache with forged entries, which is also known as poisoning.

3. How ARP Spoofing works

Module 10

ARP Attacks



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

1 I want to connect to 10.1.1.1, but I need MAC address

User A (10.1.1.0)

2 Sends ARP request

Switch

3 Switch broadcasts ARP request onto the wire

User B

4 Yes, I am here This is 10.1.1.1 and my MAC address is A1-B1-C1-D1-E1-F1

User C

Actual legitimate user responds to the ARP request

User D

5 Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user

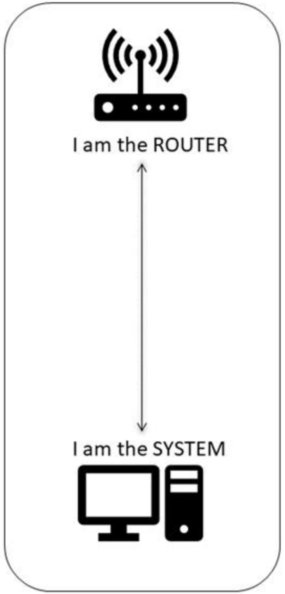
6 Sends his malicious MAC address

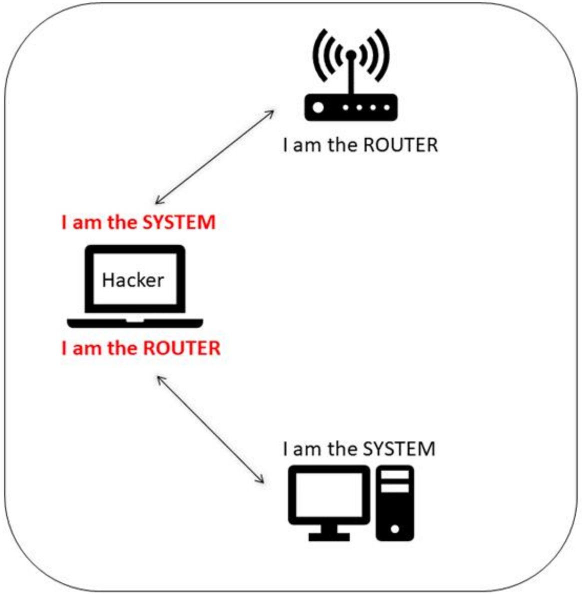
I am 10.1.1.1 and my MAC address is 11-22-33-44-55-66

Attacker

Information for IP address 10.1.1.1 is now being sent to MAC address 11-22-33-44-55-66

ARP Attacks





ARP Spoofing

ARP Attacks

- **Threats of ARP Poisoning**
  - Using fake ARP messages, an attacker can divert all communications between two machines so that all traffic is exchanged via his/her PC.
- **The threats of ARP poisoning include**:
  - Packet Sniffing
  - Session Hijacking
  - VoIP Call Tapping
  - Man-in-the-Middle Attack (Interception and Manipulation)
  - Connection Hijacking
  - Connection Resetting
  - Stealing Passwords
  - Denial-of-Service (DoS) Attack

ARP Attacks

ARP Poisoning Tools: Cain & Abel and WinArpAttacker

- **Cain & Abel**: Cain & Abel allows sniffing packets of various protocols on switched LANs by hijacking IP traffic of multiple hosts concurrently.
- **WinArpAttacker**: WinArpAttackdr sends IP conflict packets to target computers as fast as possible and diverts all communications.

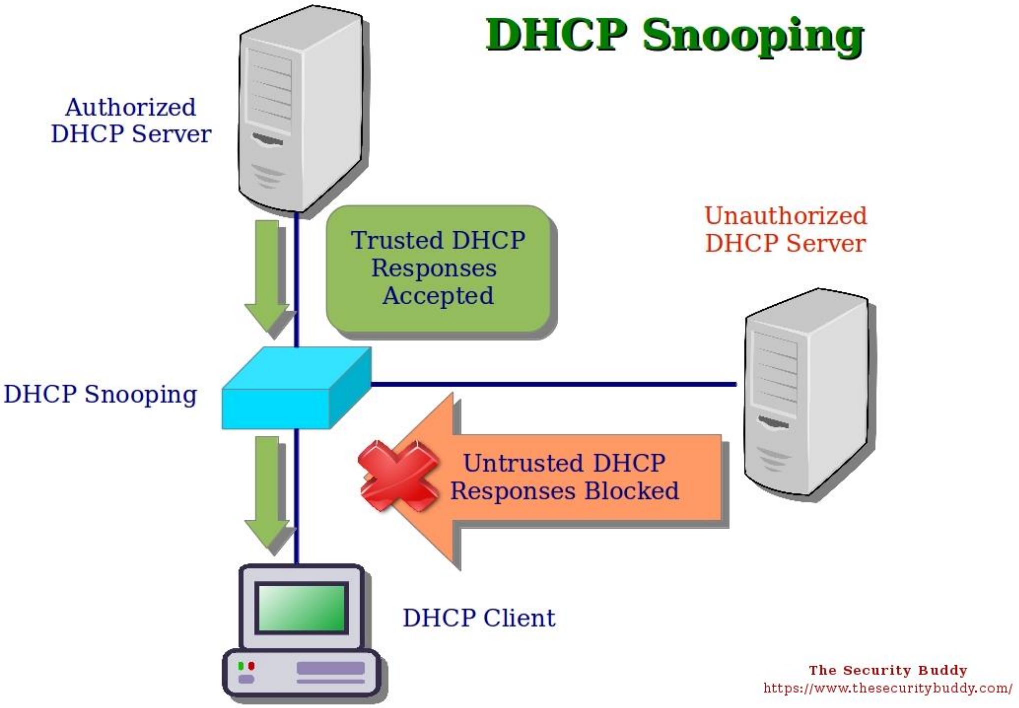
4. Defend against ARP Poisoning

Module 10

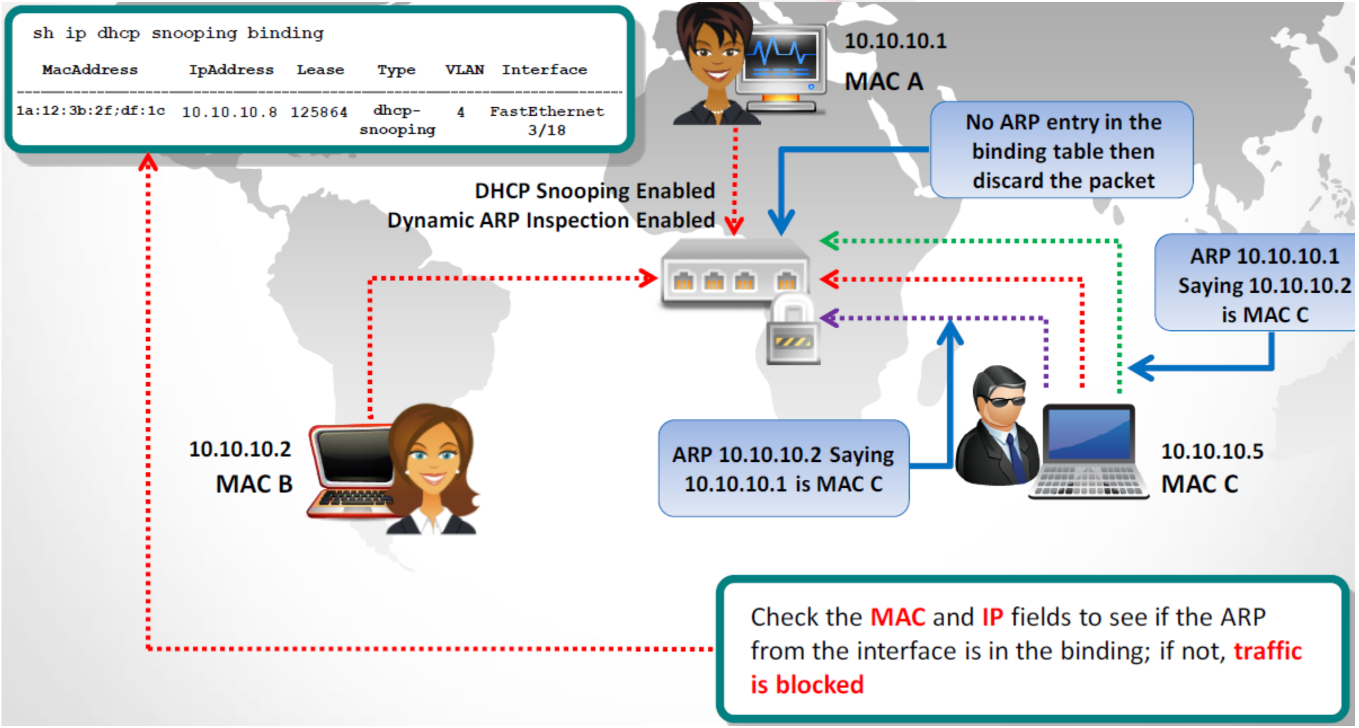
ARP Attacks

- Implement **Dynamic ARP Inspection** Using **DHCP Snooping** Binding Table.
  - DHCP Snooping rejects invalid and malicious ARP packets
  - DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a bindings database of valid tuples (MAC address, IP address, VLAN interface).
  - The switch drops ARP packet if the sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database.

ARP Attacks


DHCP Snooping
Authorized DHCP Server
Trusted DHCP Responses Accepted
Unauthorized DHCP Server
DHCP Snooping
Untrusted DHCP Responses Blocked
DHCP Client
The Security Buddy
https://www.thesecuritybuddy.com/

ARP Attacks



```
 sh ip dhcp snooping binding

  MacAddress        IpAddress   Lease     Type    VLAN  Interface
----------------------------------------------------------------------
1a:12:3b:2f;df:1c  10.10.10.8  125864    dhcp-     4   FastEthernet
                                        snooping           3/18
```

No ARP entry in the binding table then discard the packet

ARP 10.10.10.1 Saying 10.10.10.2 is MAC C

ARP 10.10.10.2 Saying 10.10.10.1 is MAC C

Check the MAC and IP fields to see if the ARP from the interface is in the binding; if not, traffic is blocked

ARP Attacks

ARP Spoofing Detection: XArp

- XArp helps users to detect ARP attacks and keep their data private.
- It allows administrators to monitor whole subnets for ARP attacks.
- Different security levels and fine tuning possibilities allow normal and power users to efficiently use XArp to detect ARP attacks.

Spoofing Attacks

Module 10

1. MAC Spoofing

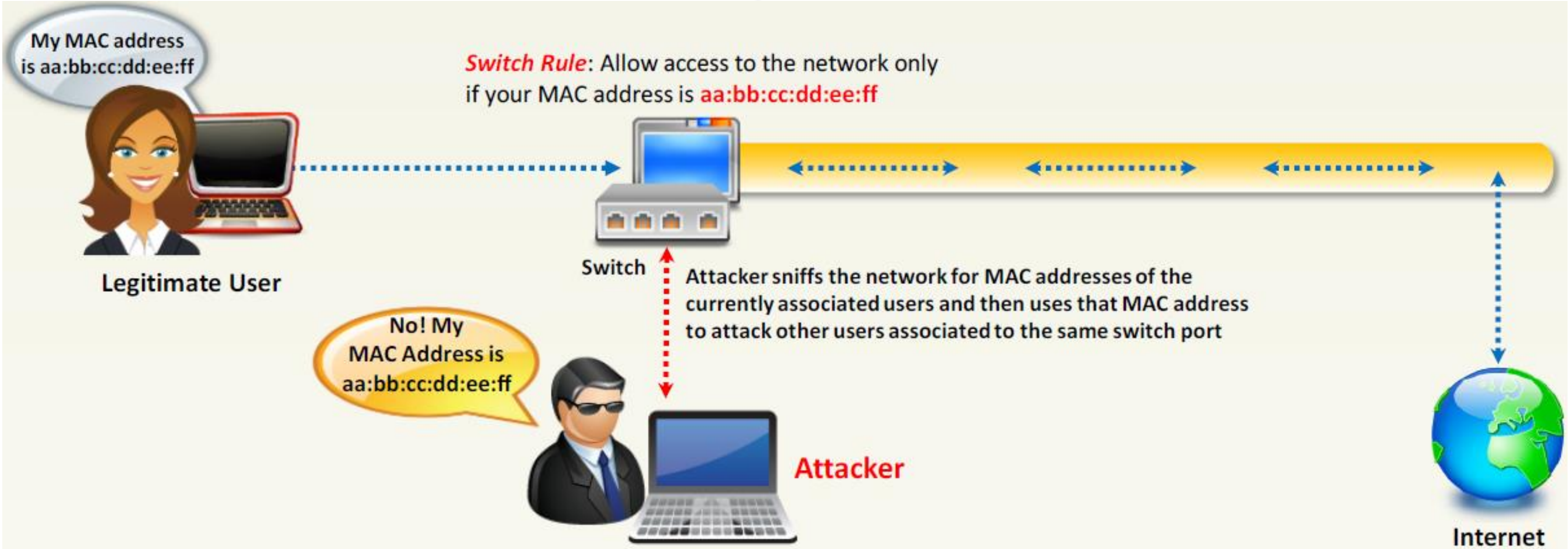
Module 10

Spoofing Attacks

MAC Spoofing/Duplicating

- MAC duplicating attack is launched by sniffing a network for MAC addresses of clients who are actively associated with a switch port and re-using one of those addresses.
- By listening to the traffic on the network, a malicious user can intercept and use a legitimate user's MAC address to receive all the traffic destined for the user.
- This attack allows an attacker to gain access to the network and take over someone's identity already on the network.
- **Defense**: Use DHCP Snooping Binding Table, Dynamic ARP Inspection, and IP Source Guard.

Spoofing Attacks



Switch Rule: Allow access to the network only if your MAC address is aa:bb:cc:dd:ee:ff

Attacker sniffs the network for MAC addresses of the currently associated users and then uses that MAC address to attack other users associated to the same switch port

My MAC address is aa:bb:cc:dd:ee:ff
Legitimate User
Switch
No! My MAC Address is aa:bb:cc:dd:ee:ff
Attacker
Internet

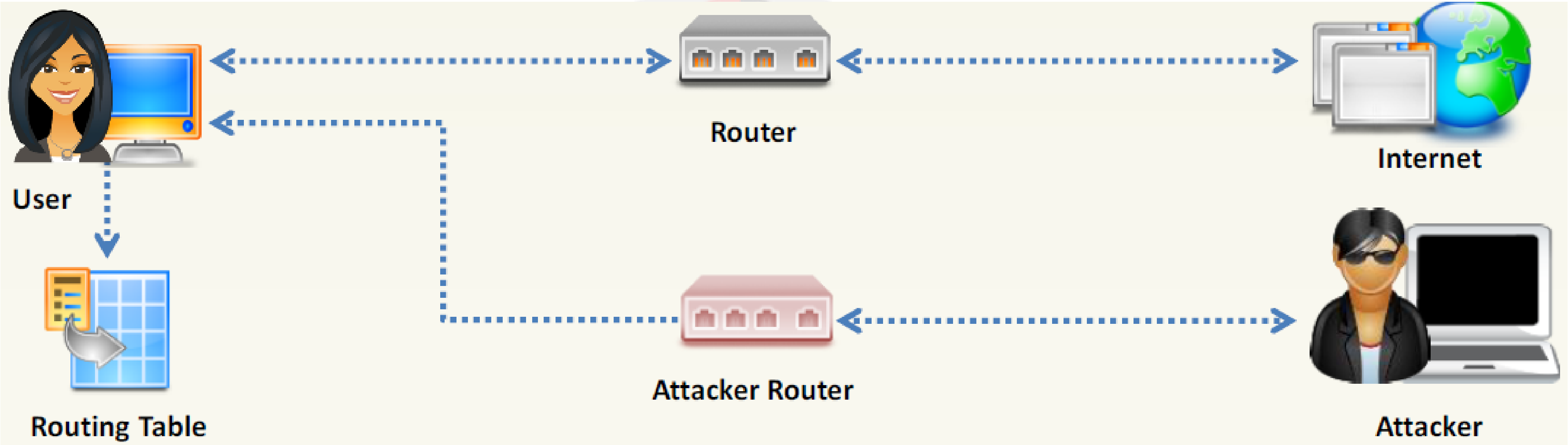
2. IRDP Spoofing

Module 10

Spoofing Attacks

- ICMP Router Discovery Protocol (IRDP) is a routing protocol that allows host to discover the IP addresses of active routers on their subnet by listening to router advertisement and solicitation messages on their network.
- Attacker sends spoofed IRDP router advertisement message to the host on the subnet, causing it to change its default router to whatever the attacker chooses.
- This attack allows attacker to sniff the traffic and collect the valuable information from the packets.
- Attackers can use IRDP spoofing to launch man-in-the-middle, denial-of-service, and passive sniffing attacks.

Spoofing Attacks



DNS Spoofing/ DNS Poisoning

Module 10

1. Introduction

Module 10

DNS Spoofing

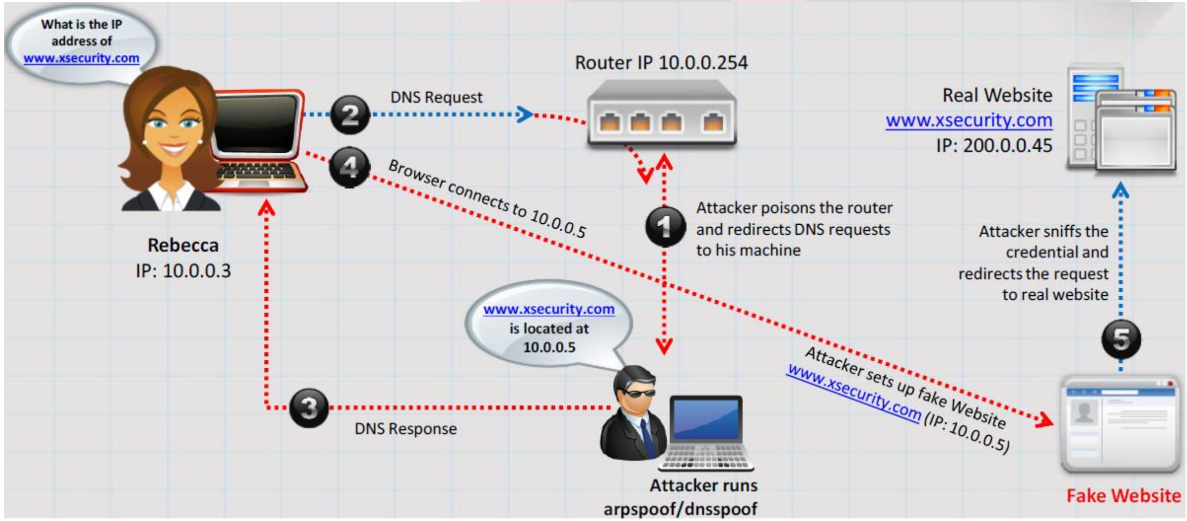
- DNS poisoning is a technique that tricks a DNS server into believing that it has received authentic information when, in reality, it has not.
- It results in substitution of a false IP address at the DNS level where web addresses are converted into numeric IP addresses.
- It allows attacker to replace IP address entries for a target site on a given DNS server with IP address of the server he/she controls.
- Attacker can create fake DNS entries for the server (containing malicious content) with same names as that of the target server.

2. Intranet DNS Spoofing

Module 10

DNS Spoofing

- For this technique, you must be connected to the local area network (LAN) and be able to sniff packets.
- It works well against switches with ARP poisoning the router.

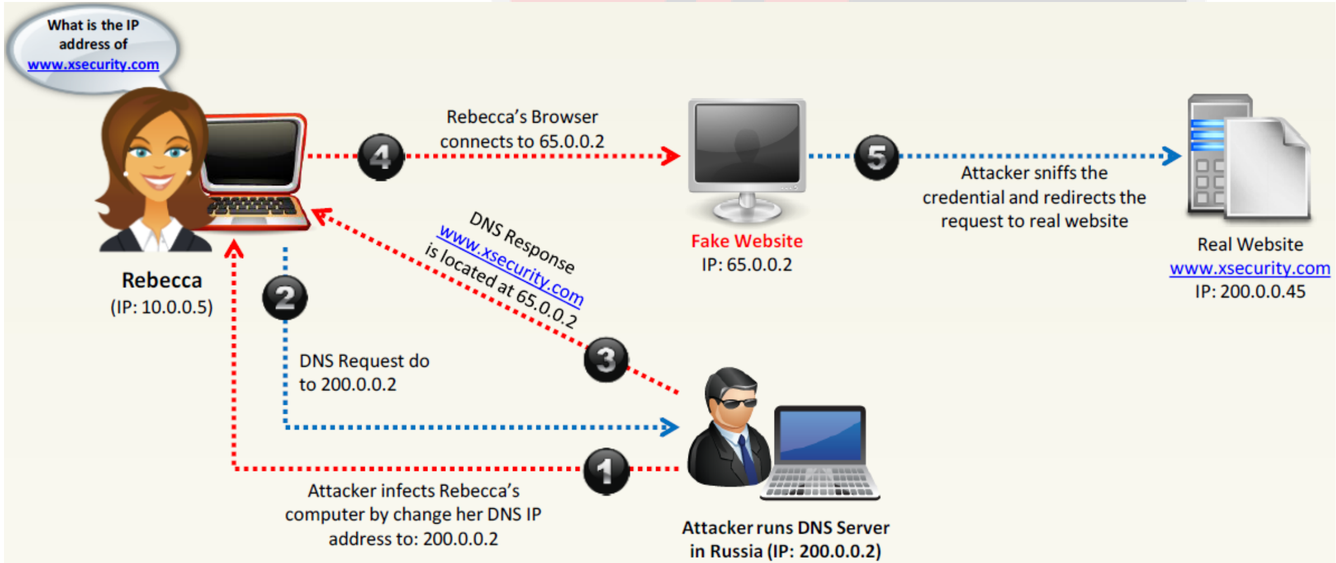

What is the IP address of www.xsecurity.com
Router IP 10.0.0.254
2 DNS Request
Real Website
www.xsecurity.com
IP: 200.0.0.45
4 Browser connects to 10.0.0.5
1 Attacker poisons the router and redirects DNS requests to his machine
Rebecca
IP: 10.0.0.3
Attacker sniffs the credential and redirects the request to real website
5
www.xsecurity.com is located at 10.0.0.5
Attacker sets up fake Website www.xsecurity.com (IP: 10.0.0.5)
3 DNS Response
Attacker runs arpspoof/dnsspoof
Fake Website

3. Internet DNS Spoofing

Module 10

DNS Spoofing

- Internet DNS Spoofing, attacker infects Rebecca's machine with a Trojan and changes her DNS IP address to that of the attacker's.

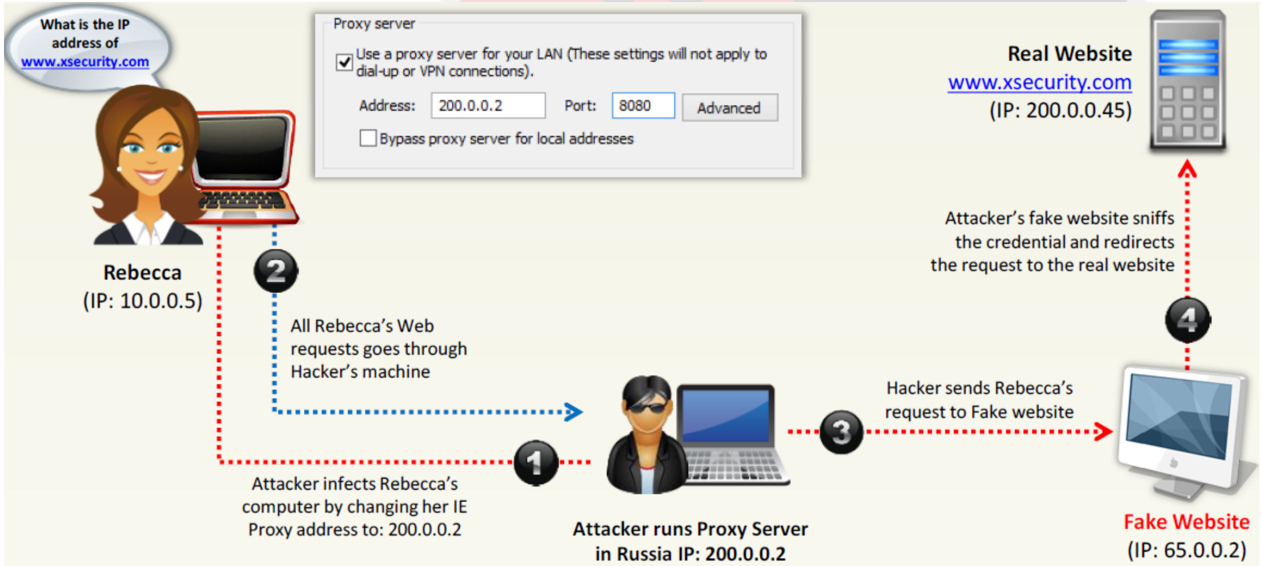

What is the IP address of www.xsecurity.com
Rebecca
(IP: 10.0.0.5)
4
Rebecca's Browser connects to 65.0.0.2
Fake Website
IP: 65.0.0.2
5
Attacker sniffs the credential and redirects the request to real website
Real Website
www.xsecurity.com
IP: 200.0.0.45
DNS Response
www.xsecurity.com
is located at 65.0.0.2
3
2
DNS Request do to 200.0.0.2
1
Attacker infects Rebecca's computer by change her DNS IP address to: 200.0.0.2
Attacker runs DNS Server in Russia (IP: 200.0.0.2)

4. Proxy Server DNS Poisoning

Module 10

DNS Spoofing

- Attacker sends a Trojan to Rebecca's machine that changes her proxy server settings in Internet Explorer to that of the attacker's and redirects to fake website.



What is the IP address of www.xsecurity.com

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 200.0.0.2 Port: 8080 Advanced

□ Bypass proxy server for local addresses

Rebecca
(IP: 10.0.0.5)

Real Website
www.xsecurity.com
(IP: 200.0.0.45)

1 Attacker infects Rebecca's computer by changing her IE Proxy address to: 200.0.0.2

2 All Rebecca's Web requests goes through Hacker's machine

3 Hacker sends Rebecca's request to Fake website

4 Attacker's fake website sniffs the credential and redirects the request to the real website

Attacker runs Proxy Server in Russia IP: 200.0.0.2

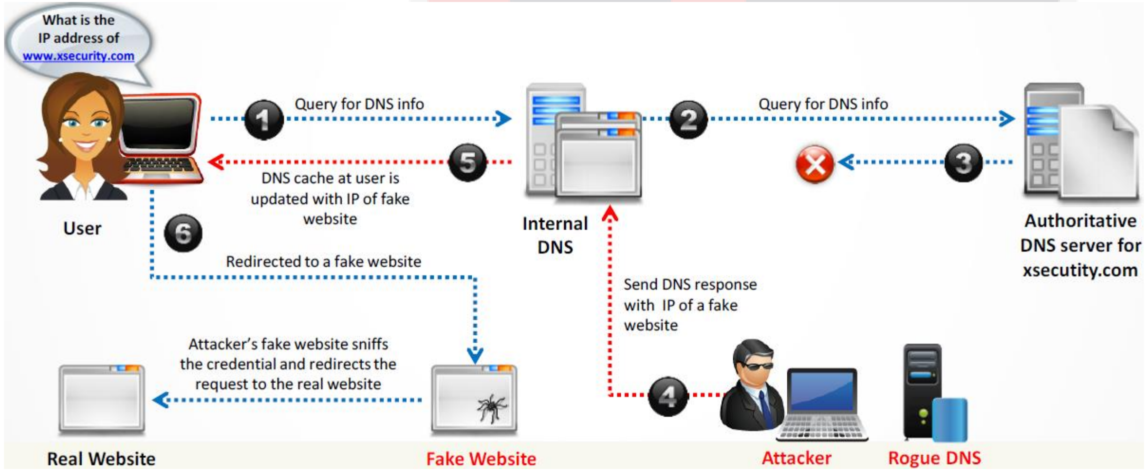
Fake Website
(IP: 65.0.0.2)

5. DNS Cache Poisoning

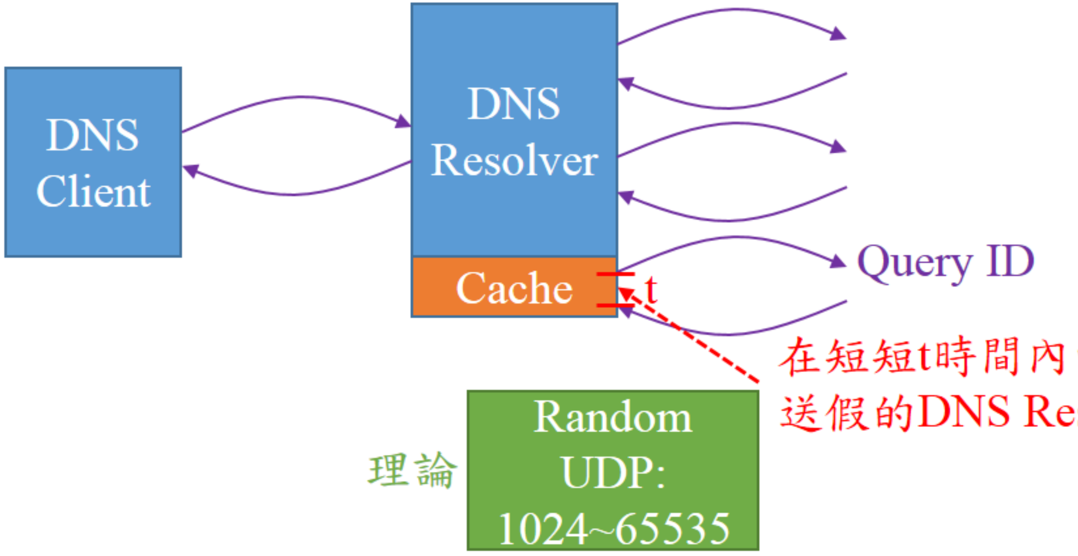
Module 10

DNS Spoofing

- DNS cache poisoning refers to altering or adding forged DNS records into the DNS resolver cache so that a DNS query is redirected to a malicious site.
- If the DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request.


What is the IP address of www.xsecurity.com
User
1 Query for DNS info
5 DNS cache at user is updated with IP of fake website
6 Redirected to a fake website
Internal DNS
2 Query for DNS info
3
Authoritative DNS server for xsecutity.com
Send DNS response with IP of a fake website
4
Attacker's fake website sniffs the credential and redirects the request to the real website
Real Website
Fake Website
Attacker
Rogue DNS

DNS Spoofing



理論

在短短t時間內向DNS Resolver 送假的DNS Response

實際做法只會從1024開始一小區間取random，因此才有機會被猜到使用的Port

6. How to Defend Against DNS Spoofing

Module 10

DNS Spoofing

- Resolve all DNS queries to local DNS server.
- Block DNS requests from going to external servers.
- Configure firewall to restrict external DNS lookup.
- Implement IDS and deploy it correctly.
- Implement DNSSEC.
- Configure DNS resolver to use a new random source port for each outgoing query.
- Restrict DNS recurring service, either full or partial, to authorized users.
- Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting.
- Secure your internal machines.

Sniffing Detection

Module 10

Sniffing Detection

- **Promiscuous Mode**:
  - You will need to check which machines are running in the promiscuous mode.
  - Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety.
- **IDS**:
  - Run IDS and notice if the MAC address of certain machines has changed (Example: router's MAC address)
  - IDS can alert the administrator about suspicious activities.

Sniffing Detection

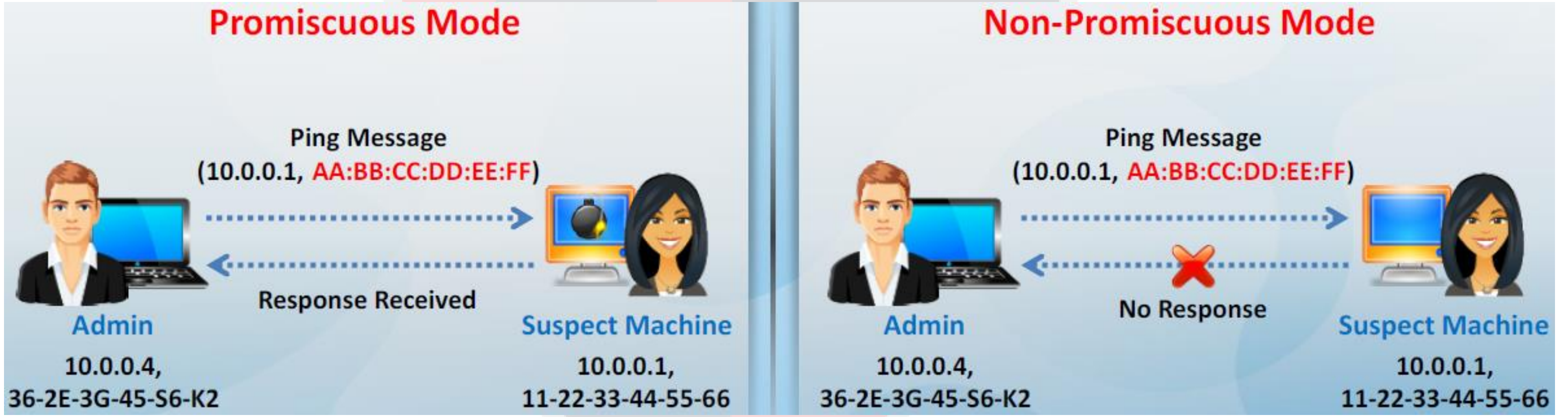
- **Network Tools**:
  - Run network tools such as Capsa Network Analyzer to monitor the network for strange packets.
  - It enables you to collect, consolidate, centralize and analyze traffic data across different network resources and technologies.

1. Ping method

Module 10

Sniffing Detection

- Send a ping request to the suspect machine with its IP address and incorrect MAC address. The Ethernet adapter reject it, as the MAC address does not match, whereas the suspect machine running the sniffer responds to it as it does not reject packets with a different MAC address.



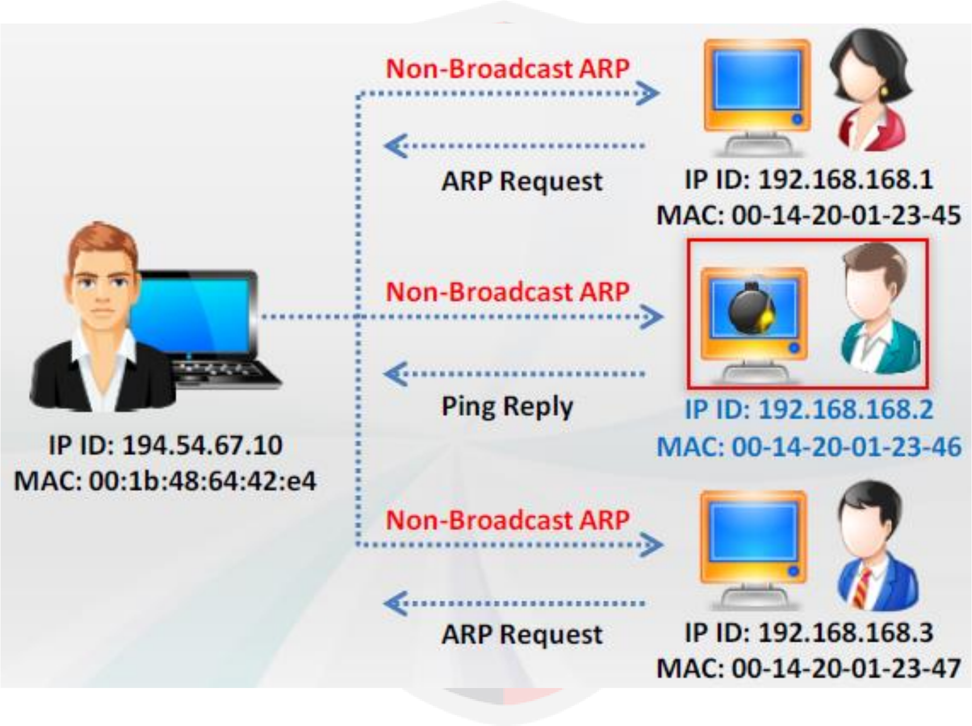
2. ARP method

Module 10

Sniffing Detection

- Only a machine in promiscuous mode (machine C) caches the ARP information (IP and MAC address mapping).
- A machine in promiscuous mode replies to the ping message as it has correct information about the host sending ping request in its cache; rest of the machines will send ARP probe to identify the source of ping request.

Sniffing Detection

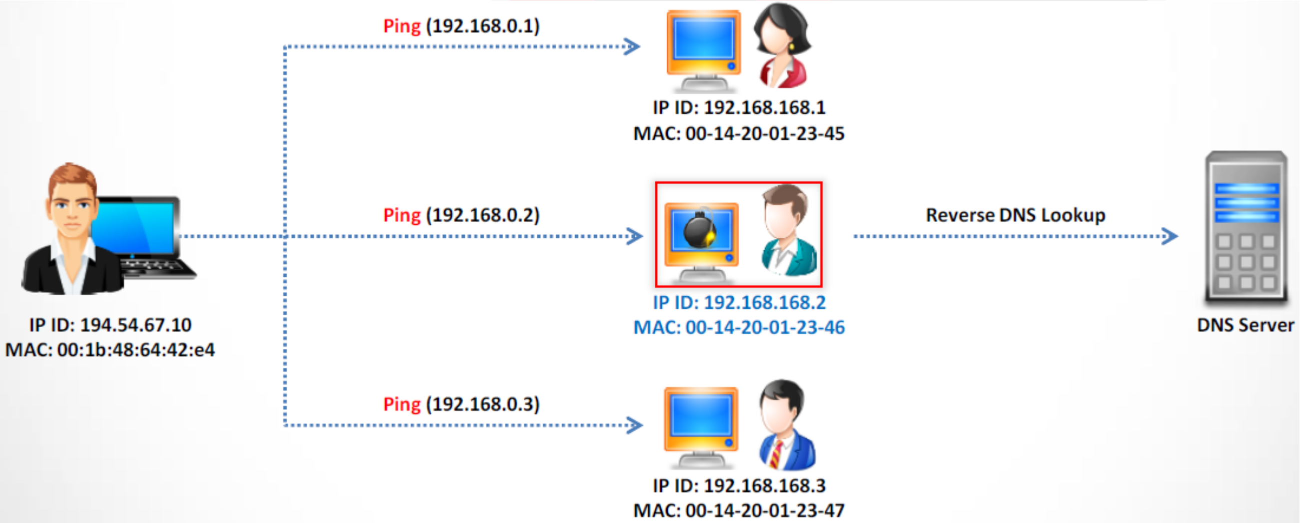


3. DNS method

Module 10

Sniffing Detection

- Most of the sniffers perform reverse DNS lookup to identify the machine from the IP address.
- A machine generating reverse DNS lookup traffic will be most likely running a sniffer.

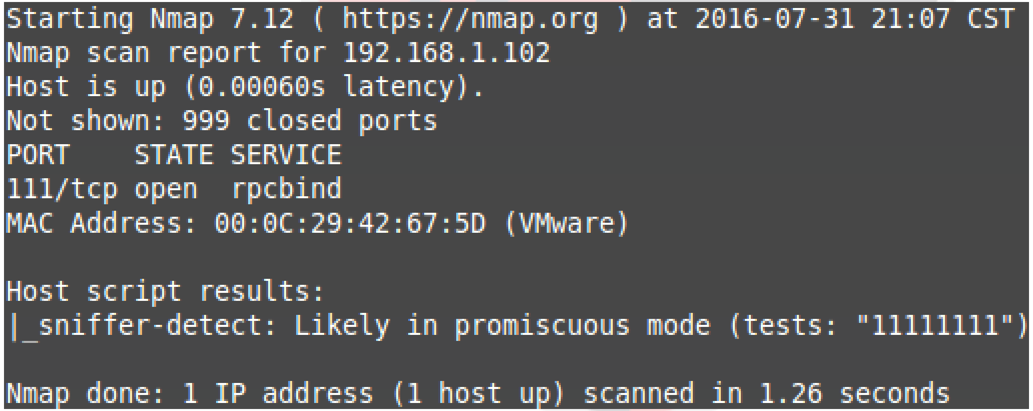


4. Nmap method

Module 10

Sniffing Detection

- Nmap's NSE script allows you to check if a target on a local Ethernet has its network card in promiscuous mode.
- Command to detect NIC in promiscuous mode:
  - nmap --script=sniffer-detect [Target IP Address/Range of IP addresses]



```
Starting Nmap 7.12 ( https://nmap.org ) at 2016-07-31 21:07 CST
Nmap scan report for 192.168.1.102
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind
MAC Address: 00:0C:29:42:67:5D (VMware)

Host script results:
|_sniffer-detect: Likely in promiscuous mode (tests: "11111111")

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

Countermeasures

Module 10

Countermeasures

- Restrict the physical access to the network media to ensure that a packet sniffer cannot be installed.
- Use encryption to protect confidential information.
- Permanently add the MAC address of the gateway to the ARP cache.
- Use static IP addresses and static ARP tables to prevent attackers from adding the spoofed ARP entries for machines in the network.
- Turn off network identification broadcasts and if possible restrict the network to authorized users in order to protect network from being discovered with sniffing tools.

Countermeasures

- Use tools to determine if any NICs are running in the promiscuous mode.
- Use IPv6 instead of IPv4 protocol.
- Use encrypted sessions such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, SSL for email connection, etc. to protect wireless network users against sniffing attacks.
- Use HTTPS instead of HTTP to protect user names and passwords.
- Use switch instead of hub as switch delivers data only to the intended recipient.

Countermeasures

- Use SFTP, instead of FTP for secure transfer of files.
- Use PGP and S/MIME, VPN, IPSec, SSL/TLS, Secure Shell (SSH) and One-time passwords (OTP).
- Always encrypt the wireless traffic with a strong encryption protocol such as WPA and WPA2.
- Retrieve MAC directly from NIC instead of OS; this prevents MAC address spoofing.

HACKING

Is an art, practised through a creative mind.