

Network Sniffing


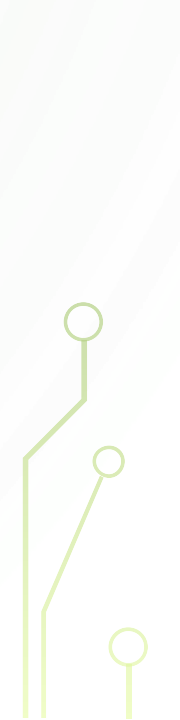
MODULE TOPICS

- Sniffing Concepts
- Sniffing Attacks
- Detection and Countermeasures





WIRETAPPING


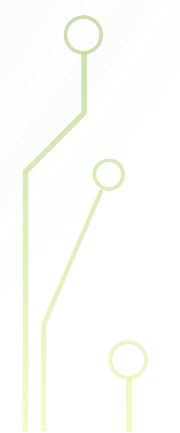
- Process of monitoring telephone and Internet conversations by a 3rd party
 - Attacker connects a listening device (hardware or software) to the information path
 - Allows monitoring, interception and recording of information in a data flow
- 
- 

WHAT IS PACKET SNIFFING?

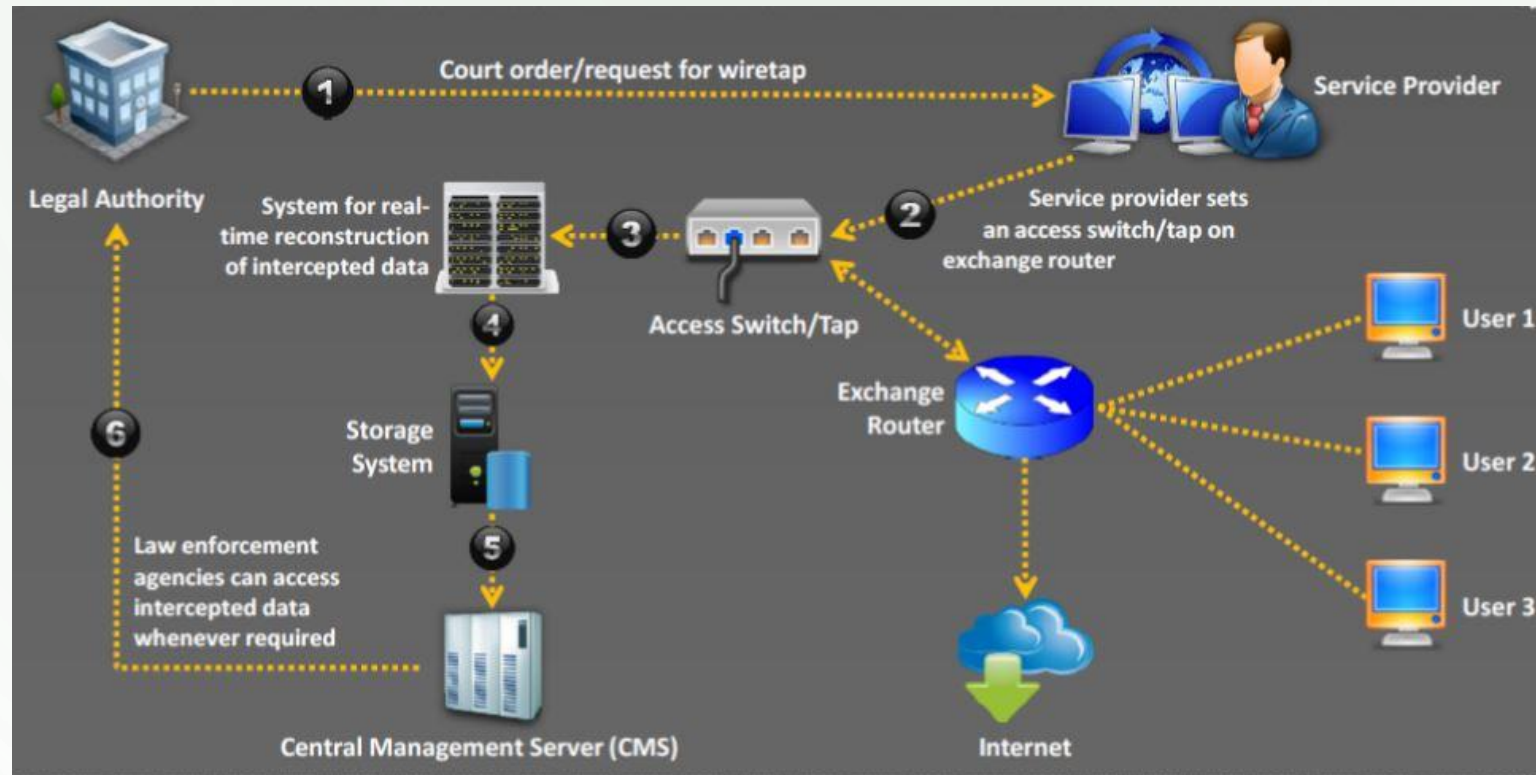
- It is a form of wire tapping done on a data network
- Process of monitoring and capturing data packets over the network using software or hardware tools
- An attacker can use sniffing to
 - Capture sensitive information
 - Gains information in reading unencrypted data
- Methods
 - Passive - monitor and record only
 - Active - monitor, record, **alter**, and **inject**



LAWFUL INTERCEPTION

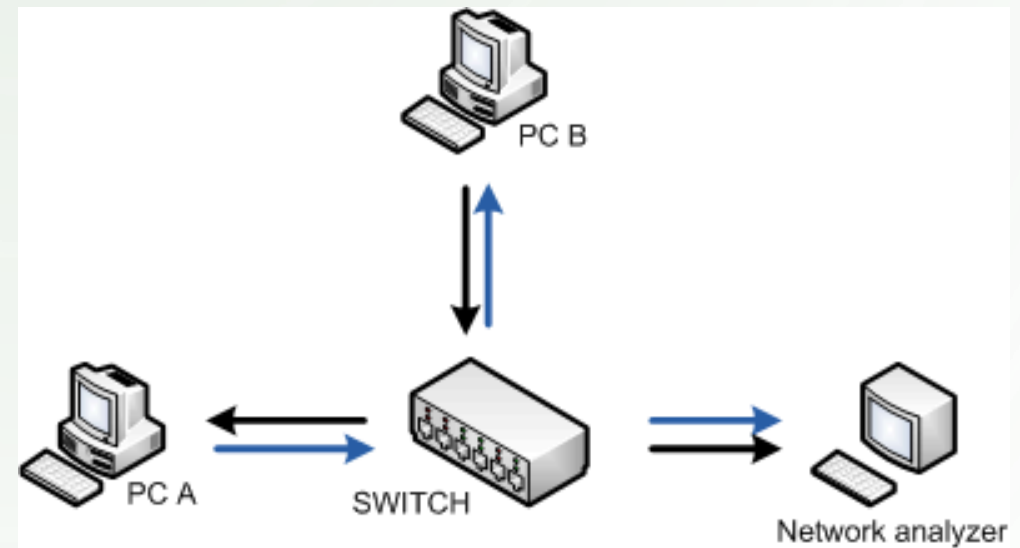
- Form of obtaining data from the communication network by lawful authority for analysis or evidence
 - Useful in infrastructure management and protection
 - Also used in cyber-security related issues
 - Remember that this should be **legally sanctioned**
- 
- 

LAWFUL INTERCEPTION PROBABLE INFRASTRUCTURE




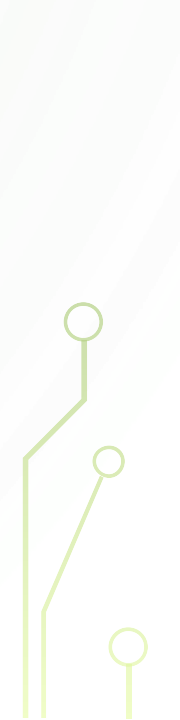
HOW SNIFFING WORKS

- Using NIC in promiscuous mode so that it listens to all data transmitted in a segment
- A sniffer monitors the network traffic in a computer using the NIC by decoding packets
- Sniffer connects using a switch, hub or tap





PACKET SNIFFING IN HUBS

- Very easy since all packets are transmitted on all ports
 - Even if it is not a broadcast packet
 - This is because of the collision domain in an Ethernet networks
 - Obsolete technology
- 
- 


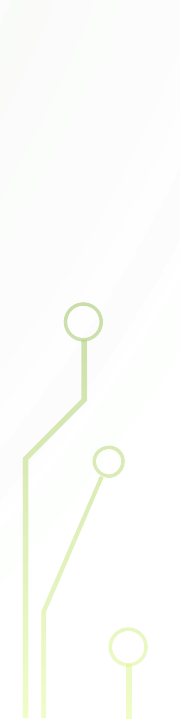
PACKET SNIFFING IN NETWORK TAP

- A hardware device which provides a way to access the data flowing across a computer network
- Analogous to a phone tap or vampire tap




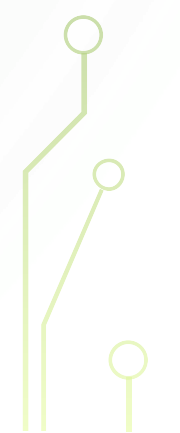


PACKET SNIFFING IN A SWITCH

- Only broadcast packets are transmitted on all ports
 - For unicast packets, a port mirror or SPAN port is needed
 - Very limited to the capability of the switch
 - Attacks can be done through
 - MAC flooding
 - ARP poisoning
- 
- 



WHAT INFORMATION CAN ATTACKERS GET?


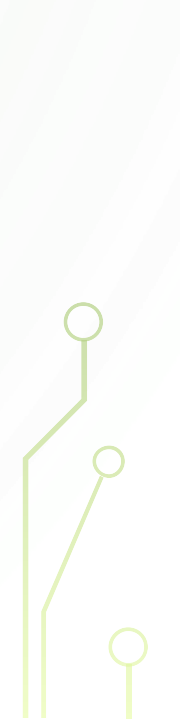
- Telnet passwords
 - Router configurations
 - DNS traffic
 - Web traffic (HTTP and FTP)
 - Email traffic (POP and IMAP)
 - Syslog traffic
 - Chat sessions
- 
- 

The image features a light green background with faint, concentric circular patterns. In the four corners, there are decorative elements resembling circuit board traces or fiber optic paths, with small circles at the end of the lines. The title "SNIFFING ATTACKS" is centered in a bold, black, serif font.

SNIFFING ATTACKS



PASSIVE SNIFFING METHODS

- Monitor and record only without sending additional data
 - More stealthy
 - aka snooping or eavesdropping
 - Easily done if network uses a hub
 - If network uses a switch
 - Inject a Trojan to record traffic from the victim
 - Compromise physical security to plug in directly to the network
- 
- 

ACTIVE SNIFFING METHODS

- Monitor, record, **alter**, and **inject**
- Usually involves injects packets to the network to manipulate network hosts

MAC
Flooding

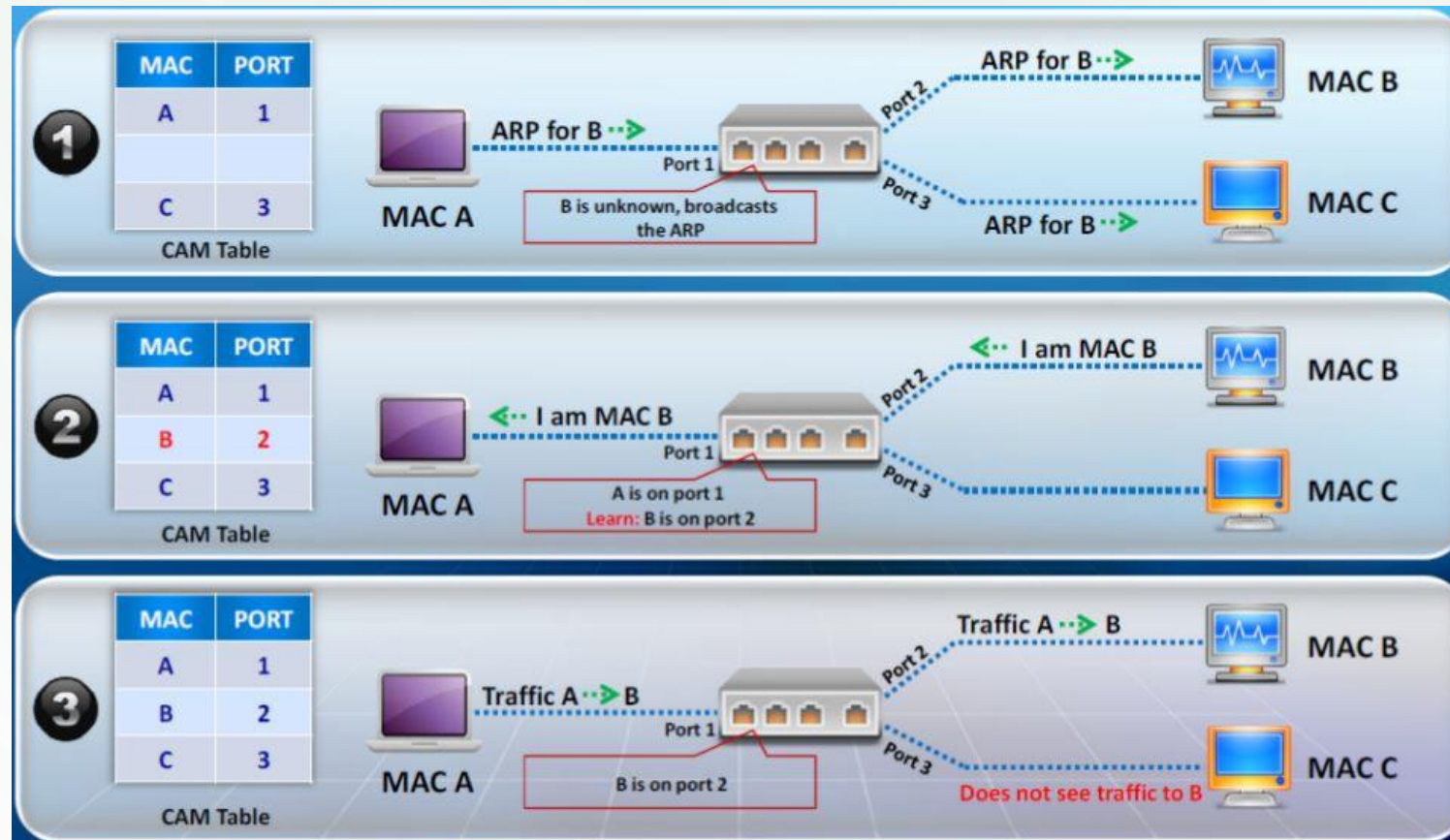
ARP
Poisoning

DHCP
Attacks

DNS
Poisoning


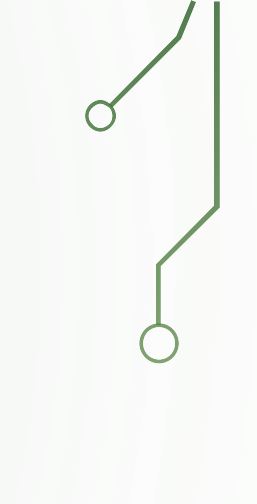
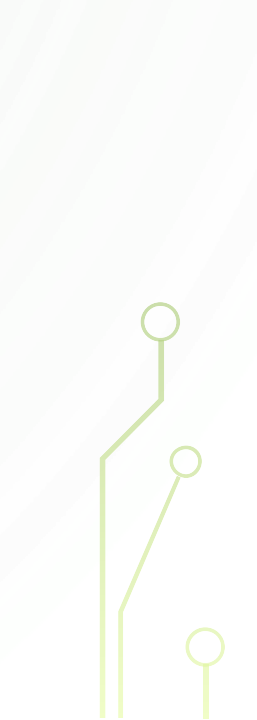
Spoofing
Attacks

RECALL : HOW THE SWITCH CAM TABLE WORKS

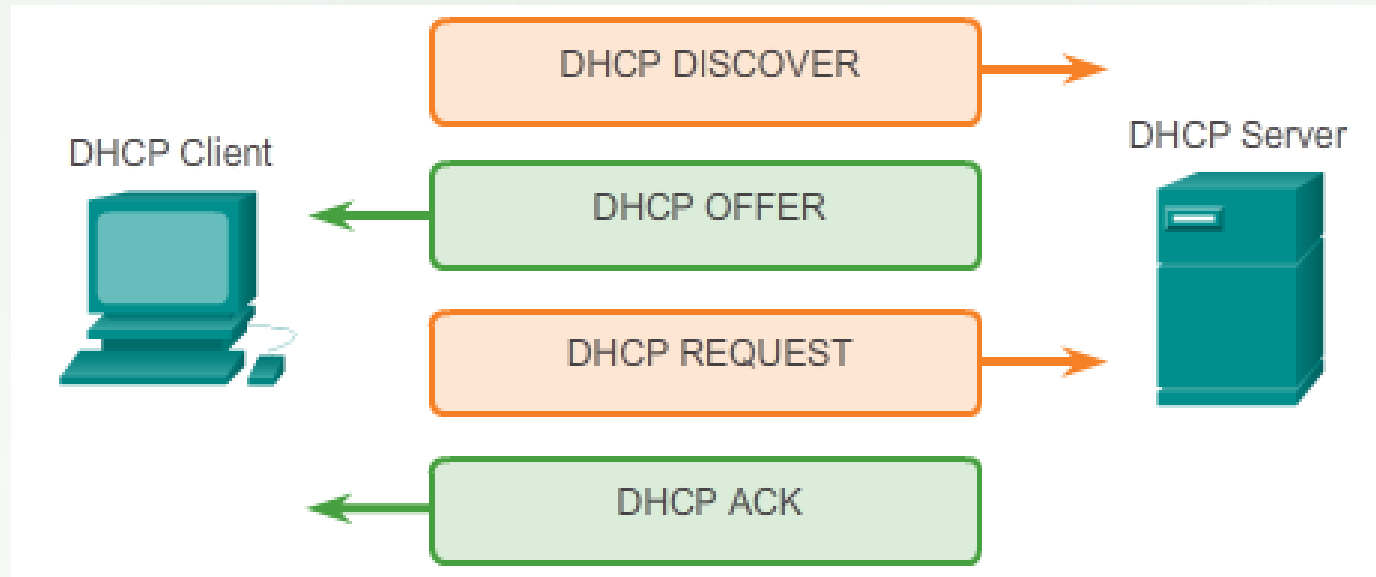




MAC FLOODING

- Exploits the vulnerability of how the CAM works
 - Floods the CAM table with fake MAC addresses until it is full
 - Done with numerous request
 - When the CAM is full, the switch acts as a hub
 - Can be prevented using port security
- 
- 
- 


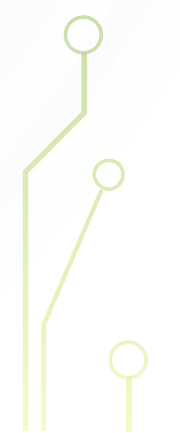
RECALL : HOW DHCP WORKS



- DHCP attacks usually done in 2 steps:
 - DHCP starvation
 - Rouge DHCP server



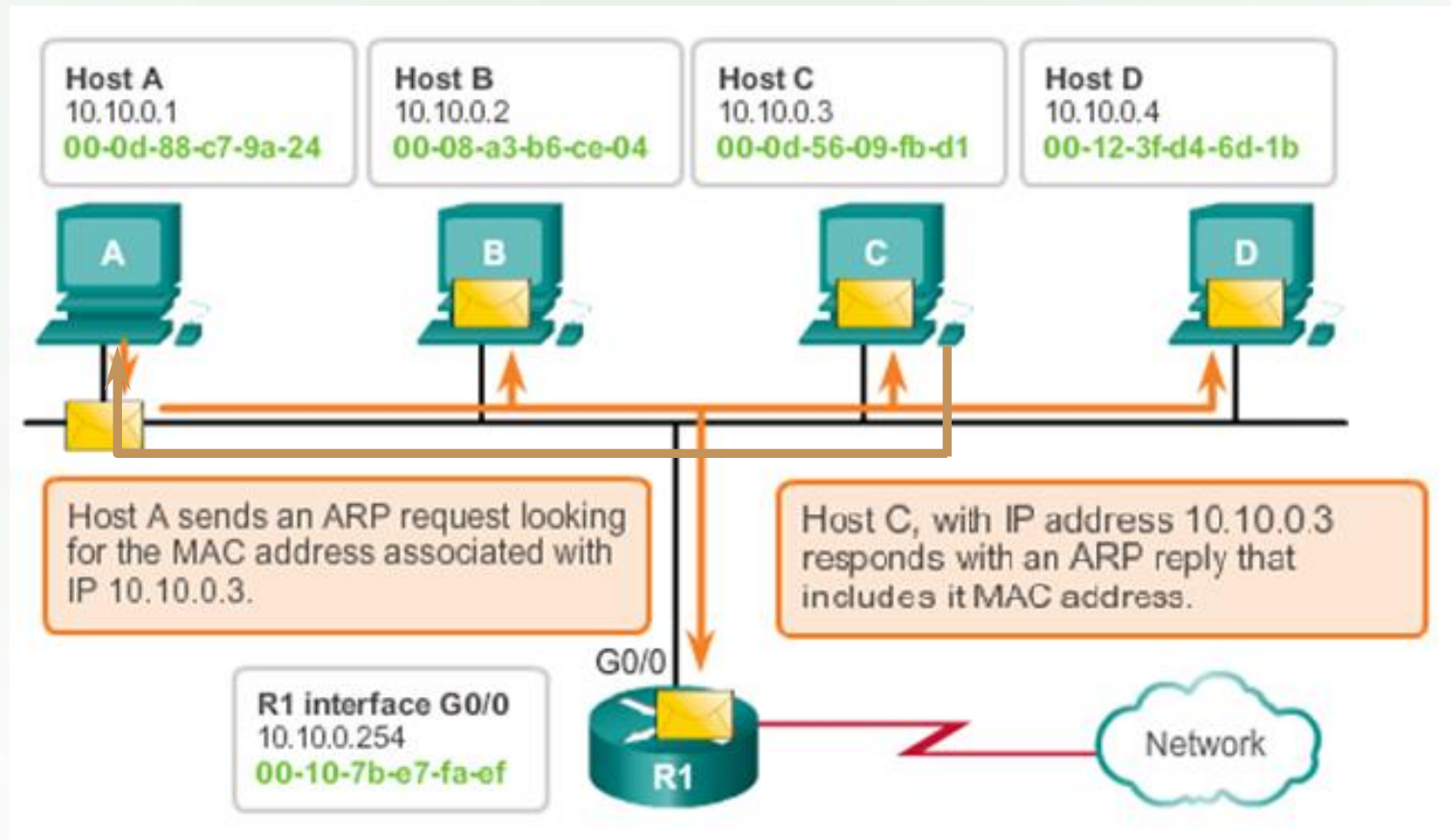
DHCP STARVATION

- Attacker forges DHCP request and tries to lease all of the DHCP addresses available in the DHCP pool
 - This results to legitimate users not being able to obtain or renew an IP address failing to get network access
 - Form of DOS attack
- 
- 

ROGUE DHCP SERVER

- Attacker sets rogue DHCP server in the network
- Responds to DHCP requests with bogus IP addresses
 - Send incorrect gateway – attacker is the gateway
 - Send wrong DNS server – attacker is the server
 - Send wrong IP address – DoS with spoofed address
- Can be prevented using DHCP snooping

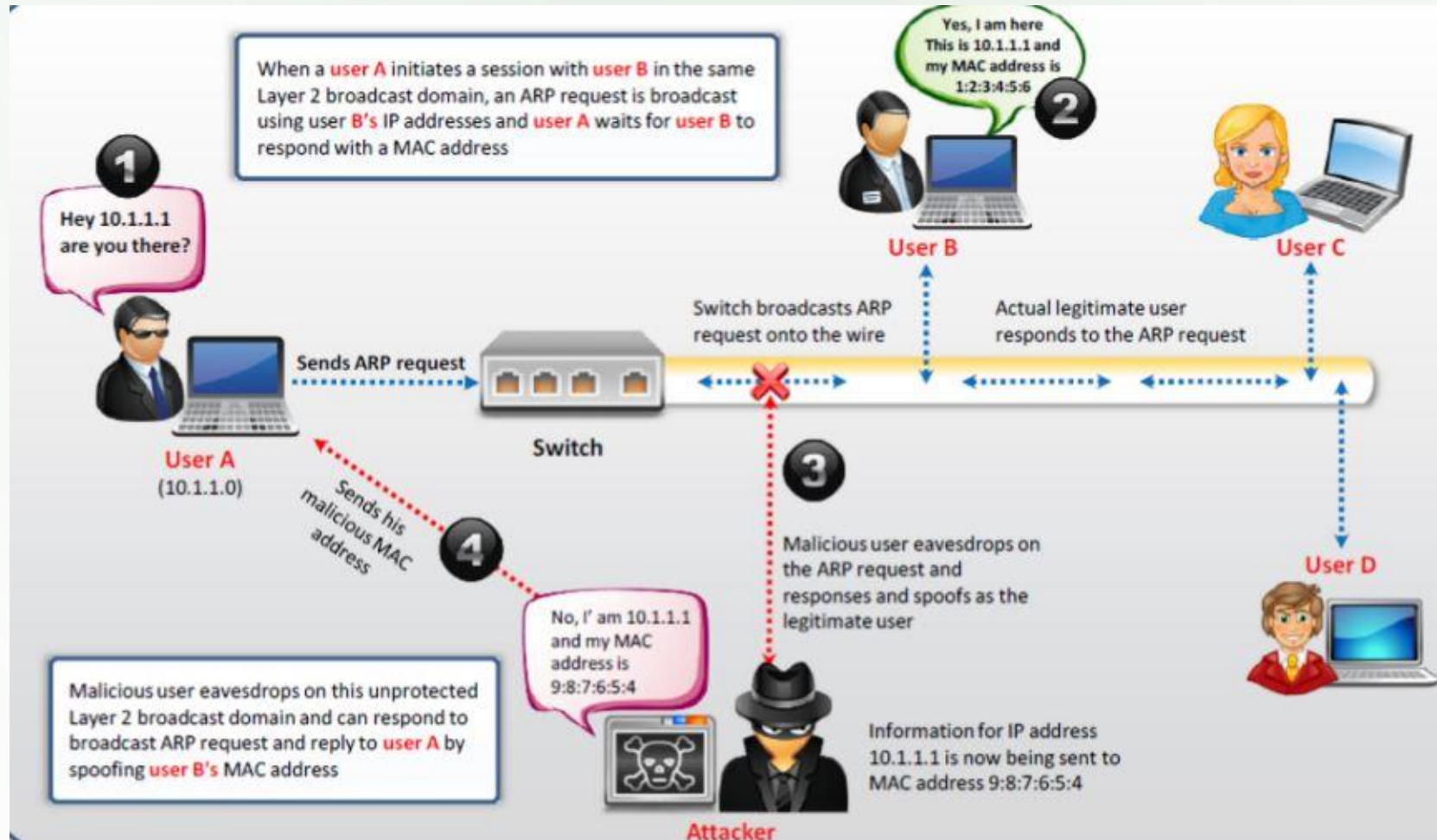
RECALL : HOW ARP WORKS



ARP POISONING / SPOOFING

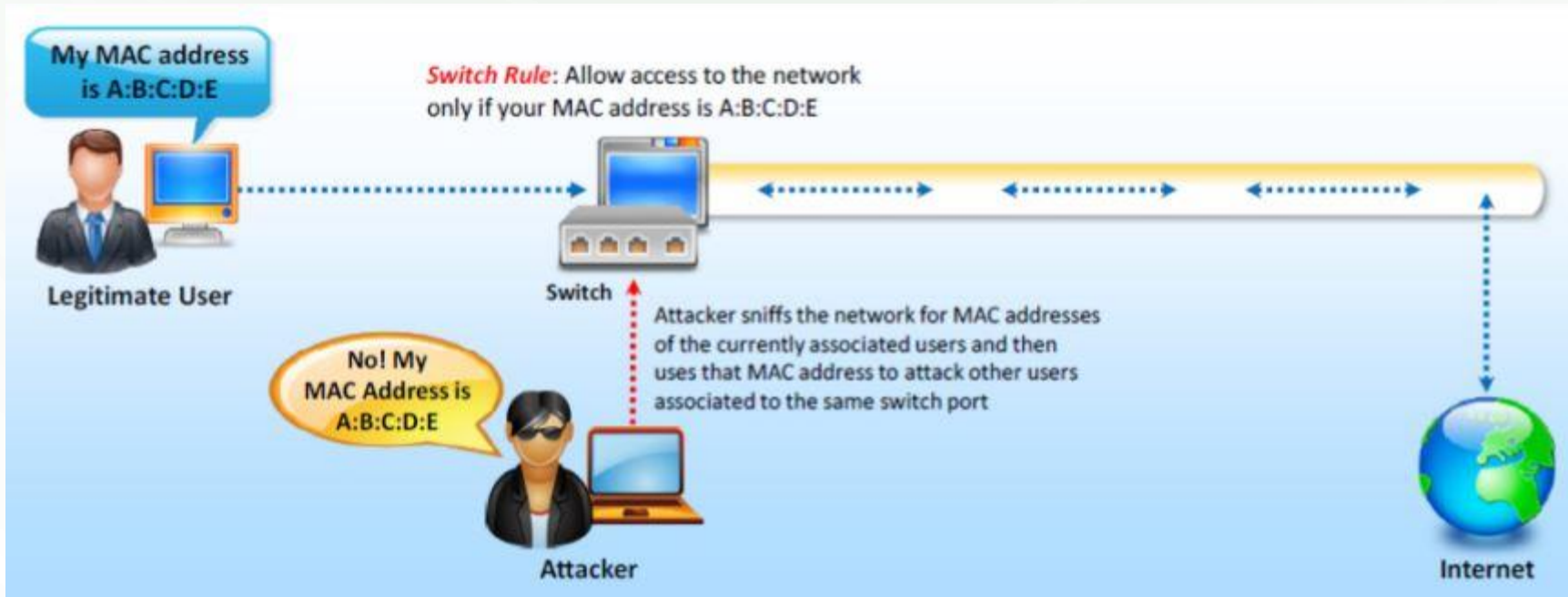
- Computers usually accept any ARP reply even if not requested
- When an attacker replies to an ARP request by sending fake ARP replies
 - Carried out by changing the MAC address of the attacker's computer to the MAC address of the target computer
- Can be used to perform man-in-the-middle attack
- Can be prevented using DHCP snooping binding and Dynamic ARP Inspection

ARP POISONING / SPOOFING




MAC SPOOFING / DUPLICATING

- Launched by sniffing the network MAC addresses of legitimate hosts
- Attacker duplicates a target's MAC address to use the target's identity and intercept traffic meant for it





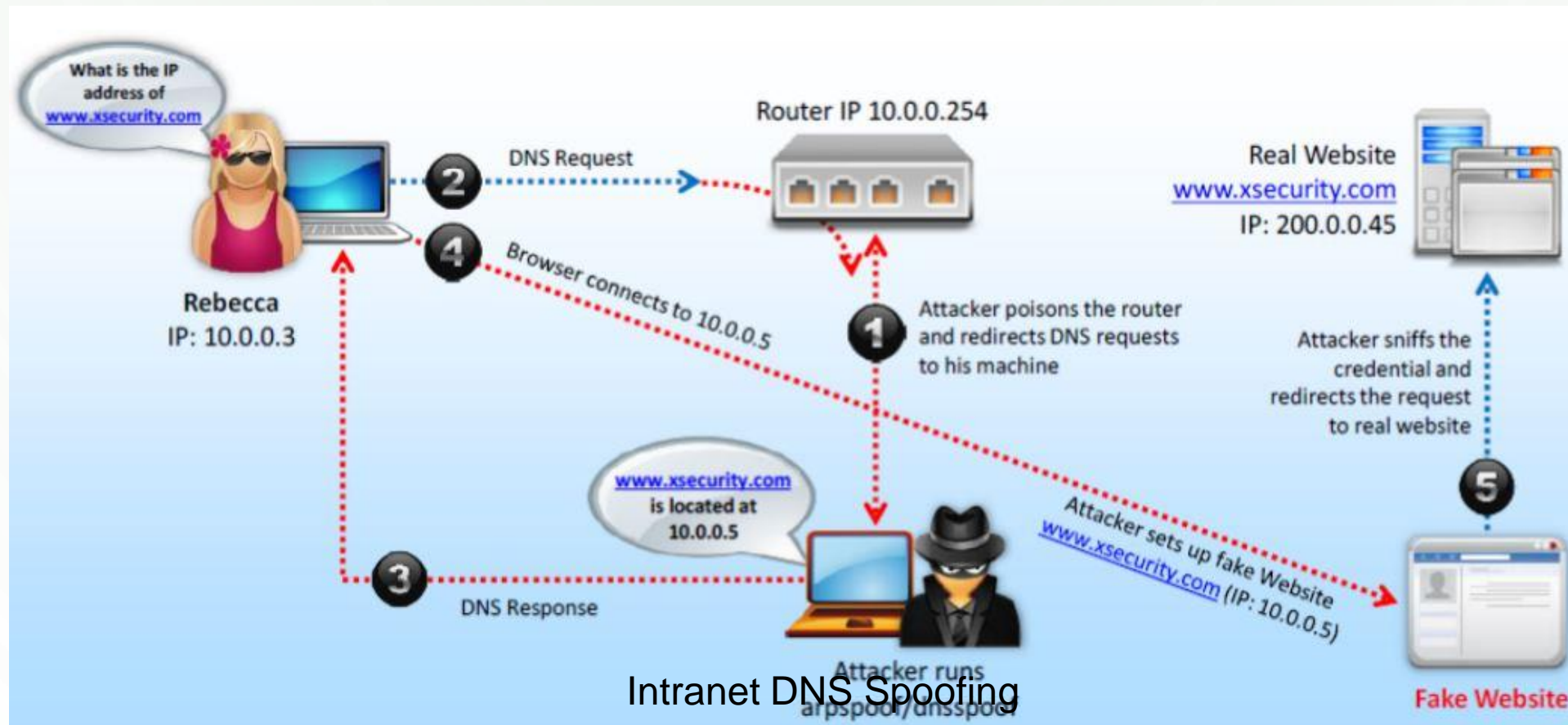
DNS POISONING

- Intranet DNS spoofing
 - Internet DNS spoofing
 - Proxy Server DNS poisoning
 - DNS cache poisoning
- 



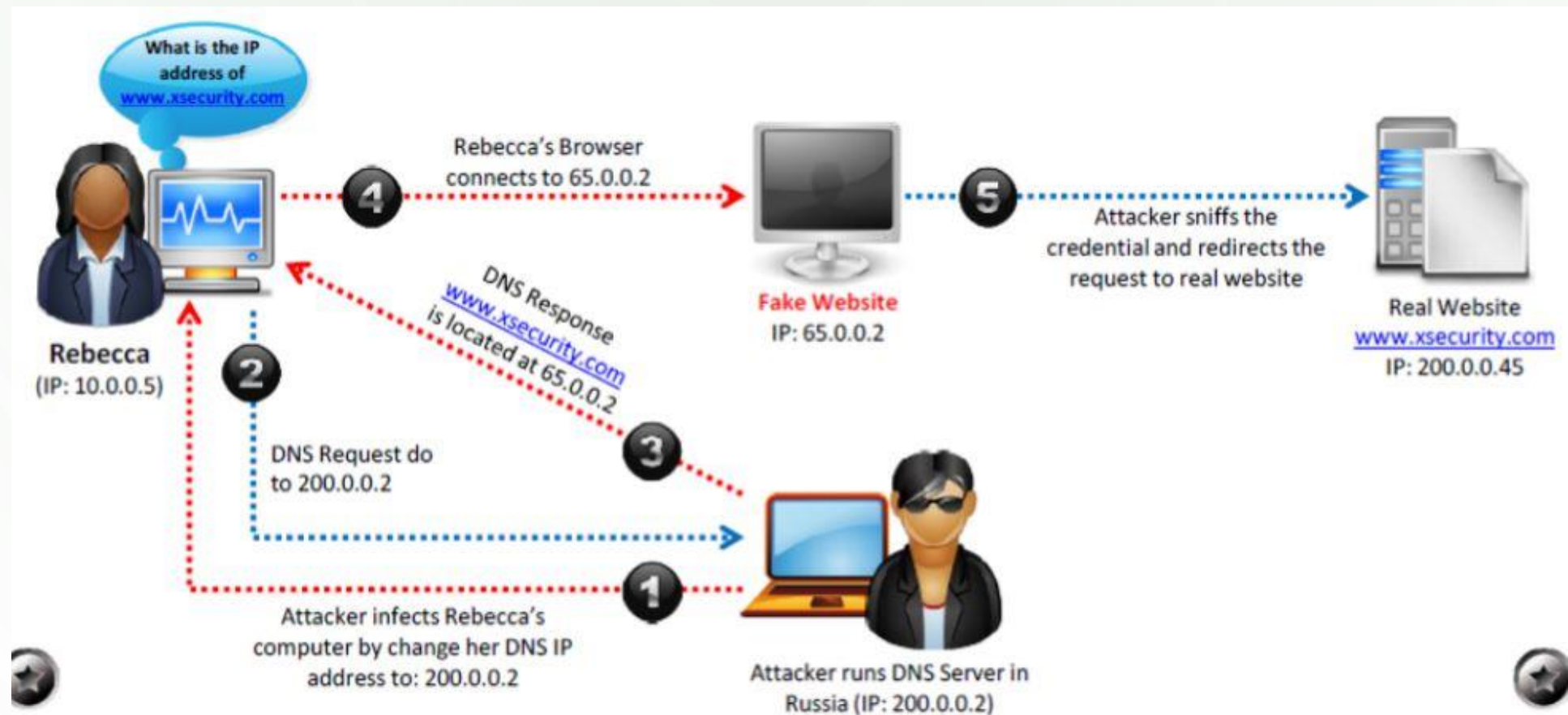
INTRANET DNS SPOOFING

- Rouge DNS catches DNS client request and replies with a diff. IP address from the original



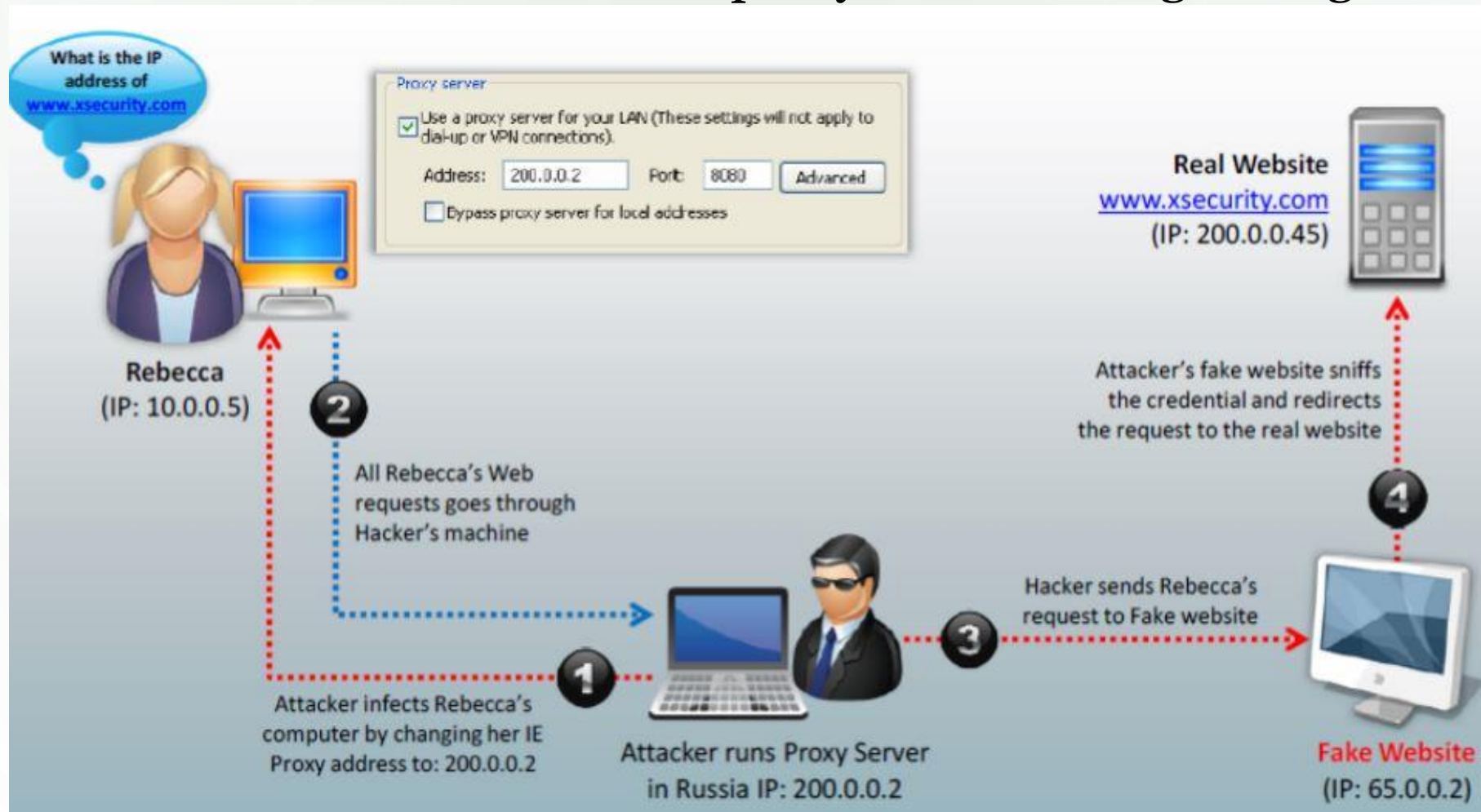
INTERNET DNS SPOOFING

- Infects the victim with a Trojan to change DNS results




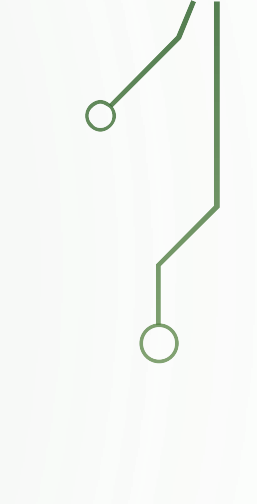
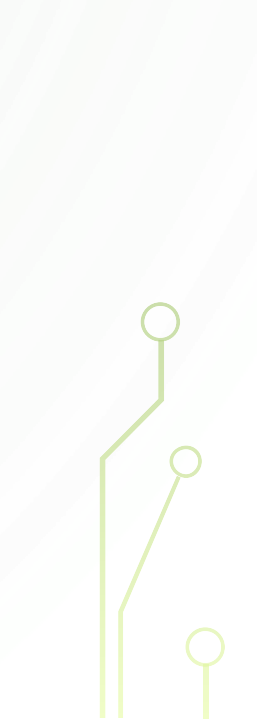
PROXY SERVER DNS SPOOFING

- Infects the victim's proxy server setting through a Trojan

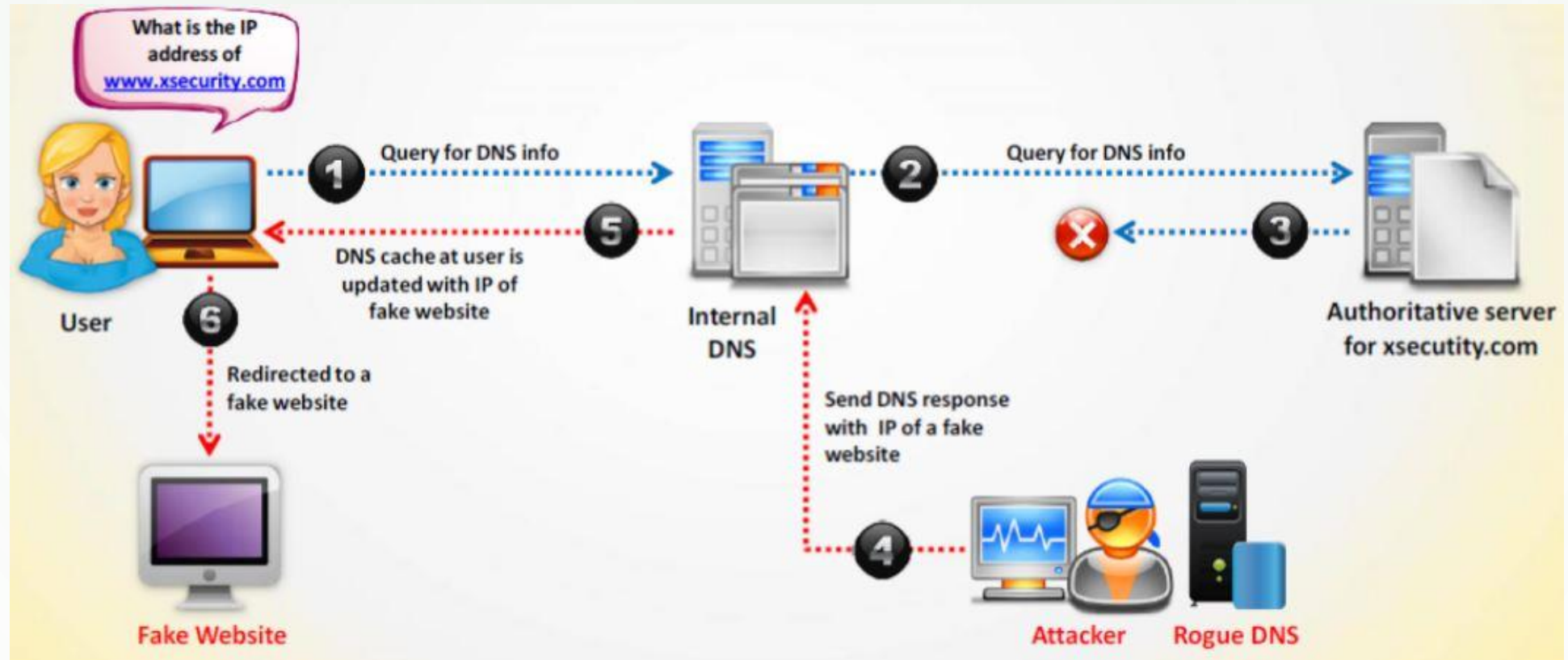




DNS CACHE POISONING

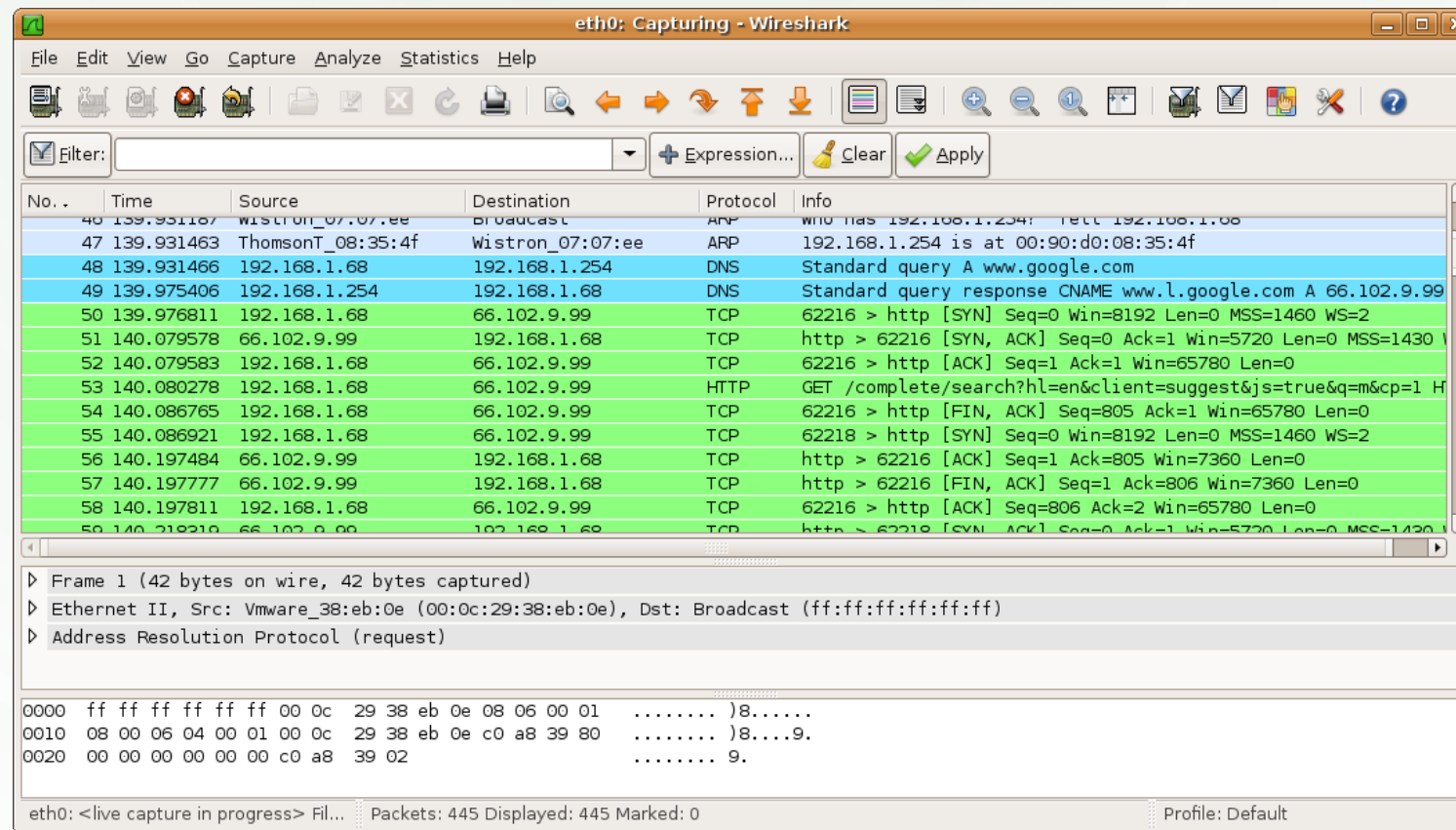
- Alters or adding forged DNS records into the DNS resolver cache so that DNS query is directed to a malicious site
 - If DNS resolver cannot validate that the DNS responses have come from an authoritative source, it will cache the incorrect entries locally and serve them to users who make the same request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

DNS CACHE POISONING



SNIFFING TOOLS

- Wireshark



HOW A HACKER SNIFFS USING TOOLS

Connect laptop to a switch port

Run discovery tools to learn network topology

Identify victim to target

Poison victim machine to set up MITM

Extract passwords and data from victim traffic

COUNTERMEASURES

- Restrict physical access to switches
- Use encryption when possible
 - HTTPS instead of HTTP
 - SSH instead of telnet
- Set the default gateway MAC address as a static ARP cache entry
- Use static IP addresses and ARP cache entries if you can