Networks Attacks

Dr. Asem Kitana

Network Traffic Basics

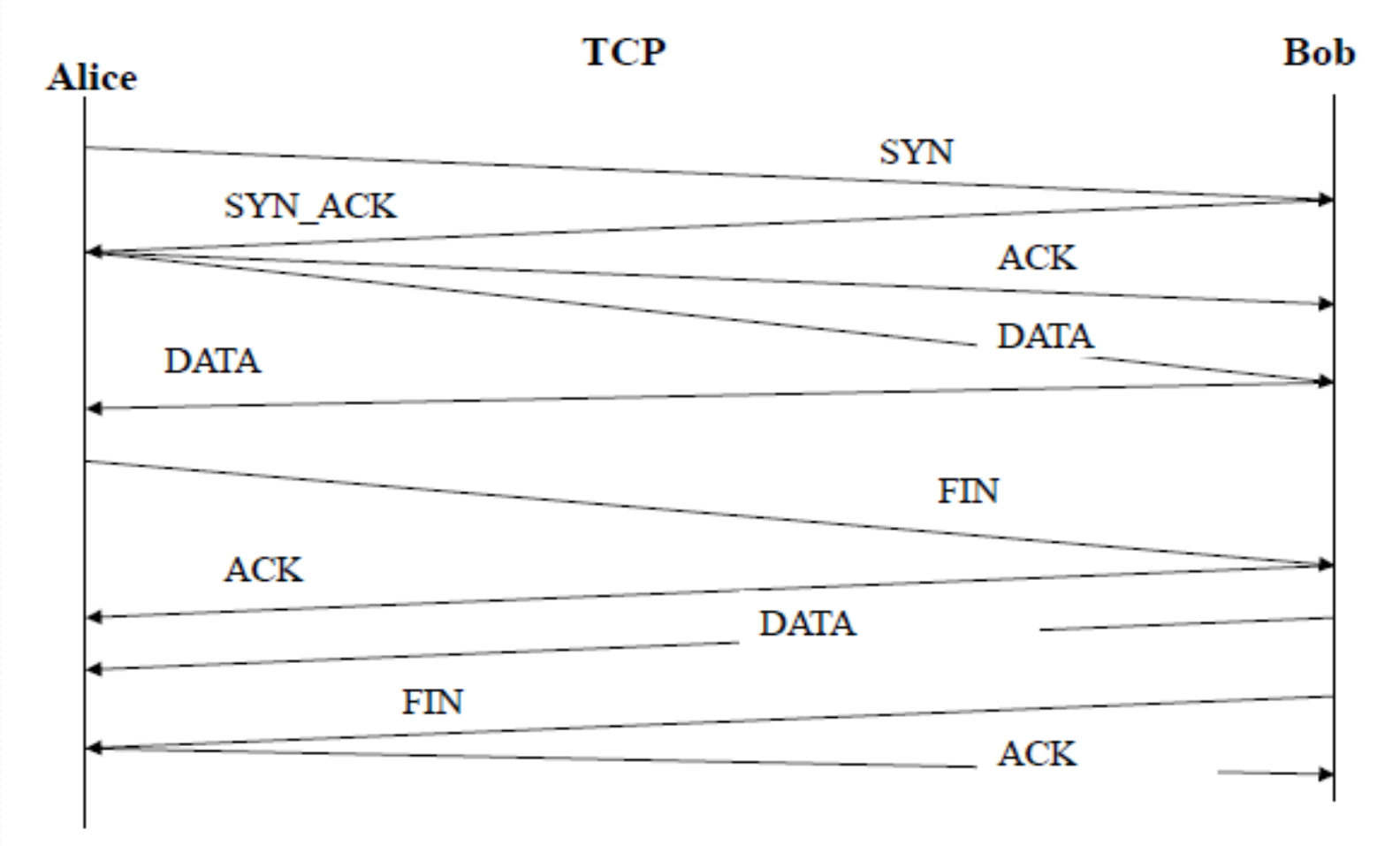
- The Internet Protocol (IP) and the Transmission Control Protocol (TCP) are the most commonly used protocols in network attacks.
- The IP protocol defines the rules for getting a packet from one point to another and the TCP protocol defines the rules ensuring that the data received at the destination is accurate and in the correct sequence.
- To achieve these capabilities, both the TCP and IP protocols attach headers to the data given by the application, before the data is actually dispatched to the recipient.

IP Protocol

Structure of an IP packet

- An IP packet can be a maximum of 64 Kb long:
  - The fields at the beginning of the packet, called the frame header, define the IP protocol's functionality and limitations.
  - 32 bits are allocated for encoding source and destination addresses (32 bits for each of these address fields).

TCP Protocol



Denial of Service

- A classic DOS attack was the SYN flood
  - The attacker computer sends a stream of TCP SYN messages to the victim's computer.
  - The victim computer responds to all of the SYN messages, starting up a connection for each one.
  - The attacker does not respond to the victim's ACK/SYN messages with ACKs.
  - The overhead from maintaining all of these open connections slows down the victim computer, disabling it or perhaps even causing it to crash.

Denial of Service

- There are many variations of the DOS attack.
- They exploit different weaknesses of the network protocols

The Ping of Death

ICMP

- The *Internet Control Message Protocol* (*ICMP*) allows routers to send error and control messages to other computers, especially routers, on the network.
- ICMP operates at the network (routing) layer of the TCP/IP stack.

Ping

- The most widely used ICMP message is the *ping*.
- Basically, ping is used to see if packets are reaching a particular computer.
- The client sends a ping request, and when it receives it, the server responds with a reply.
- A ping is normally 32 bytes in size.

Ping

- Maximum IPv4 packet size is 65,535 bytes.
- Ping of death attack indicates sending 65,536 bytes or more.
- A ping packet of this size is illegal to IP protocol.
- But if a ping packet is fragmented, then the target computer reassembles the ping packet. Resulting a buffer overflow which causes a system crash.

Ping

- The ping of death uses the ICMP ping to DOS a computer by crashing it.
- It does this by sending an illegally large ping packet.
  - In this case, more than 65,536 bytes.
- The packet causes a buffer overflow that crashes the computer.

The Smurf Attack

Broadcast

- Normally, packets are sent to a single recipient.
- But, they can be *broadcast* - sent to all computers on the local network

Smurf

- The Smurf attack broadcasts a ping to all of the machines on a local network.
- It *forges* (*spoofs*) the return address of the ping packet to be that of the victim.
- All of the machines receiving the broadcast ping then send reply packets to the victim.

Smurf

- If enough computers (possibly thousands) receive the forged ping request, the sheer number of reply packets can crash the victim computer, or clog the network.
- Computers and networks can help prevent themselves from being used as intermediaries in the attack.
  - Computers do not reply to broadcast pings.
  - Block broadcast packets at the router.
- This can help the potential intermediary, as they can also be a victim if the reply packets swamp their local network.

Denial of Service (DoS)

- Attempts to consume network resources so that the network or its devices cannot respond to legitimate requests
- **Distributed denial of service (DDoS)** attack
  - A variant of the DoS
  - May use hundreds or thousands of zombie computers in a botnet to flood a device with requests

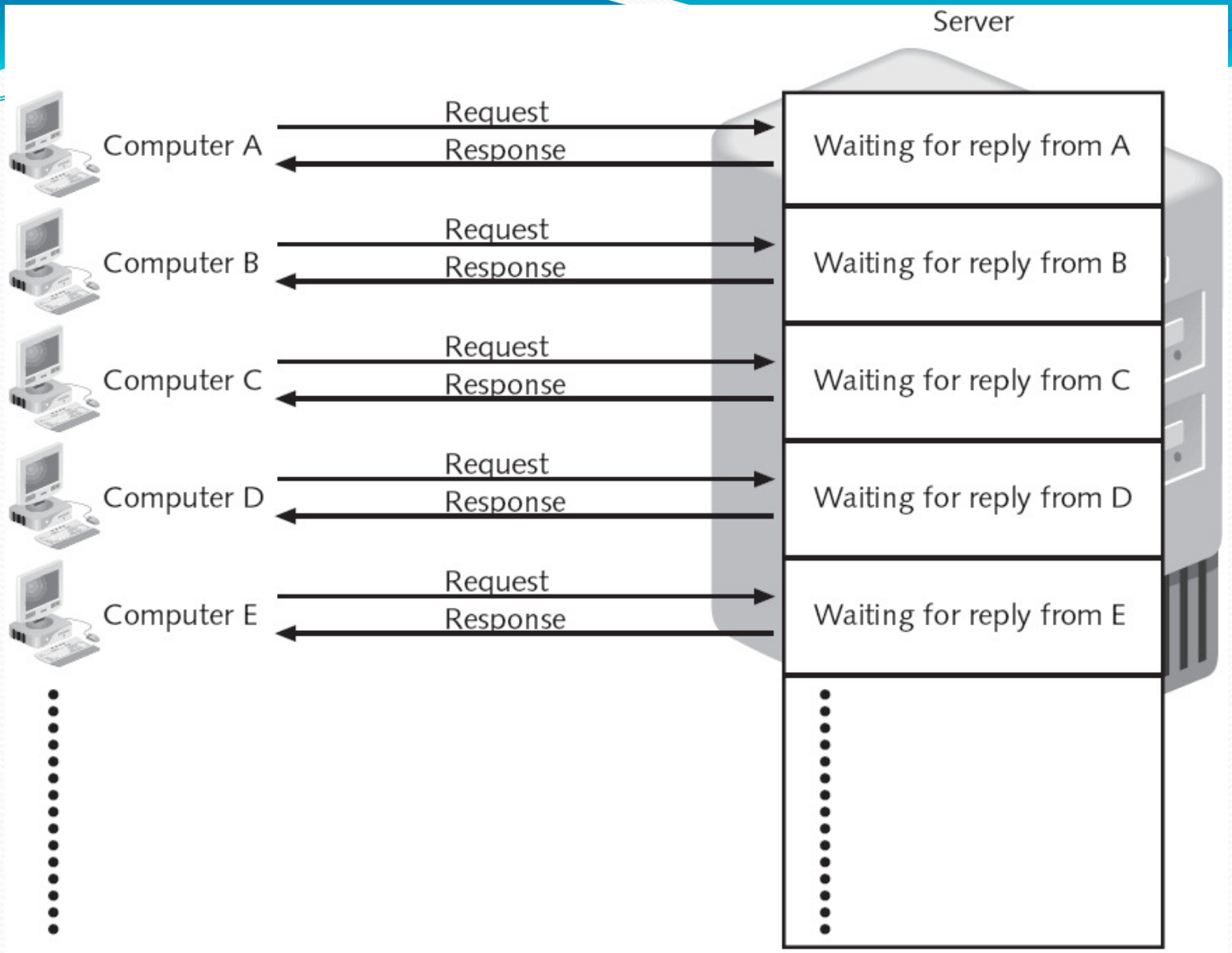


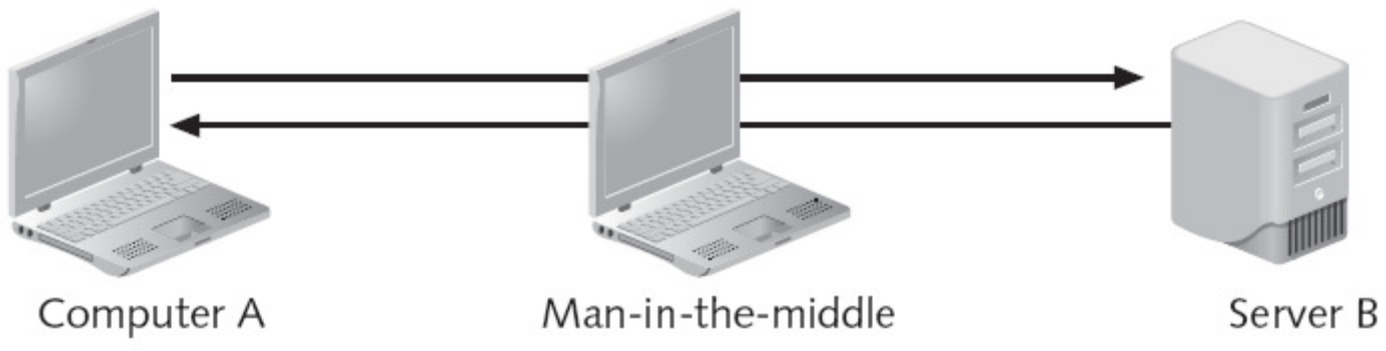
Figure 4-4 DoS attack

Spoofing

- **Spoofing** is impersonation
  - Attacker pretends to be someone else
- Malicious actions would be attributed to another user
- Spoof the network address of a known and trusted host
- Spoof a wireless router to intercept traffic

Man-in-the-Middle Attack

- **Passive**--attacker reads traffic
- **Active**--attacker changes traffic
- Common on networks



Replay Attack

- Attacker captures data
- Resends the same data later
  - A simple attack: capture passwords and save them

Sidejacking

- Records cookies and replays them
- This technique breaks into Gmail accounts
- Technical name: Cross Site Request Forgery
- Almost all social networking sites are vulnerable to this attack
  - Facebook, MySpace, Yahoo, etc.

New Tool Automates Webmail Account Hijacks

LAS VEGAS -- Logging into your **MySpace**, **Facebook**, **Yahoo!**, **Gmail** or **Hotmail** account over a wireless connection just got a lot more dicey, as researchers here at the **Black Hat** hacker conference today demonstrated a new set of tools that help automate the hijacking of those accounts.

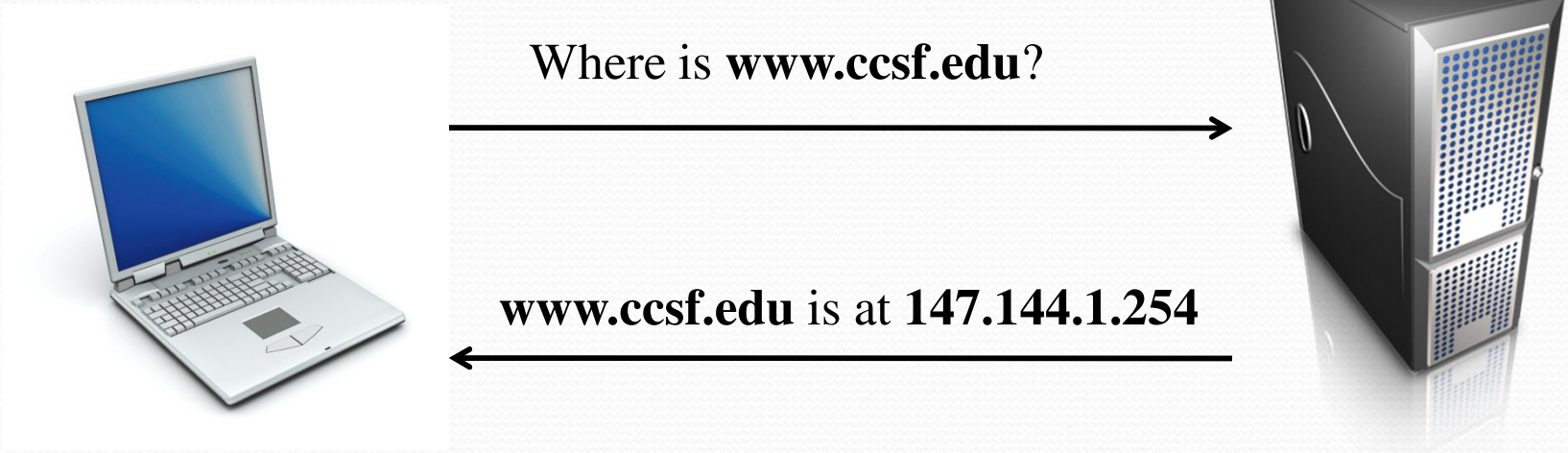
Methods of Network Attacks

SNMP (Simple Network Management Protocol)

- Used to manage switches, routers, and other network devices
- Early versions did not encrypt passwords, and had other security flaws
- But the old versions are still commonly used

DNS (Domain Name System)

- DNS is used to resolve domain names like **www.ccsf.edu** to IP addresses like **147.144.1.254**
- DNS has many vulnerabilities
  - It was never designed to be secure



DNS Poisoning

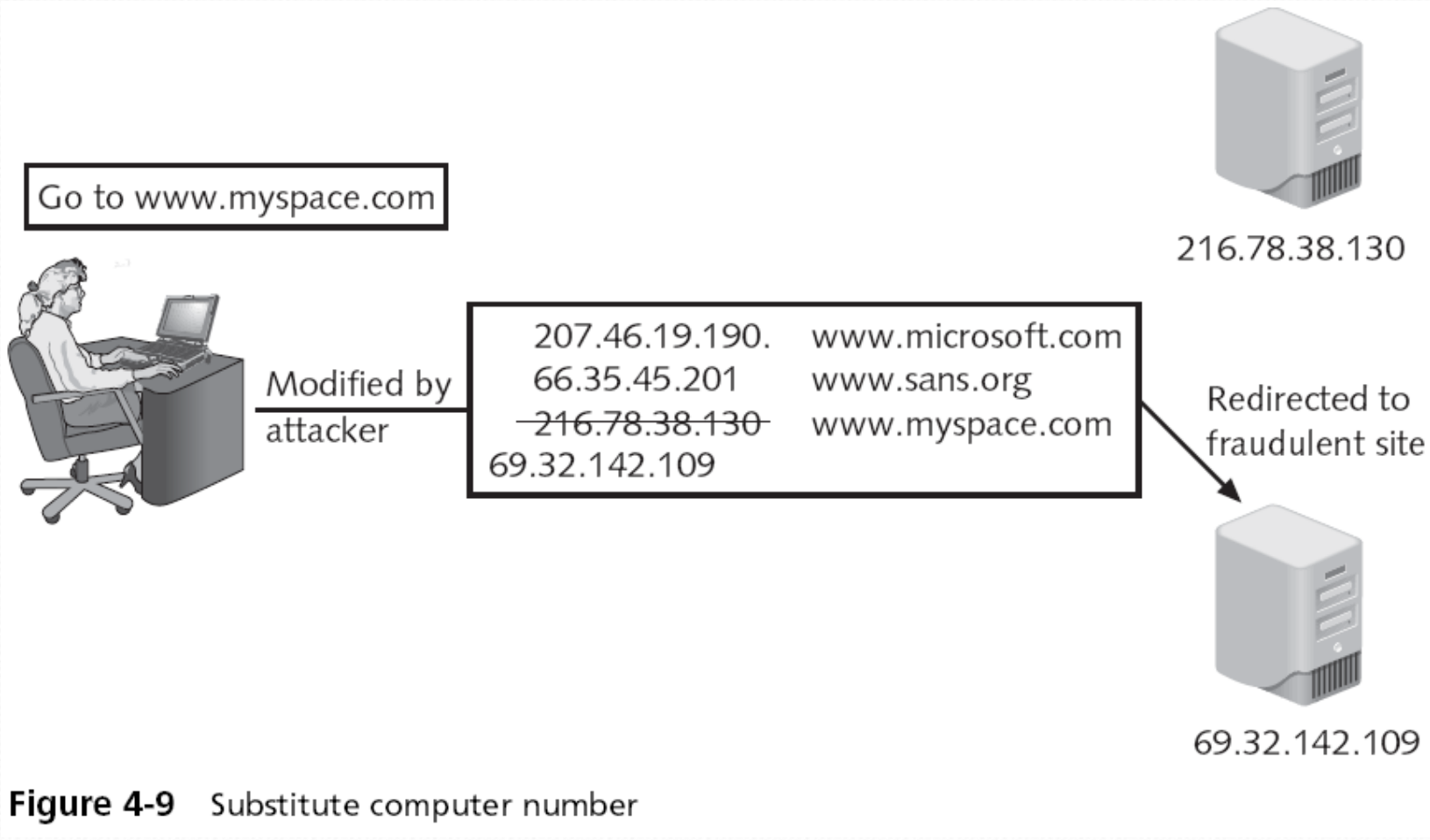
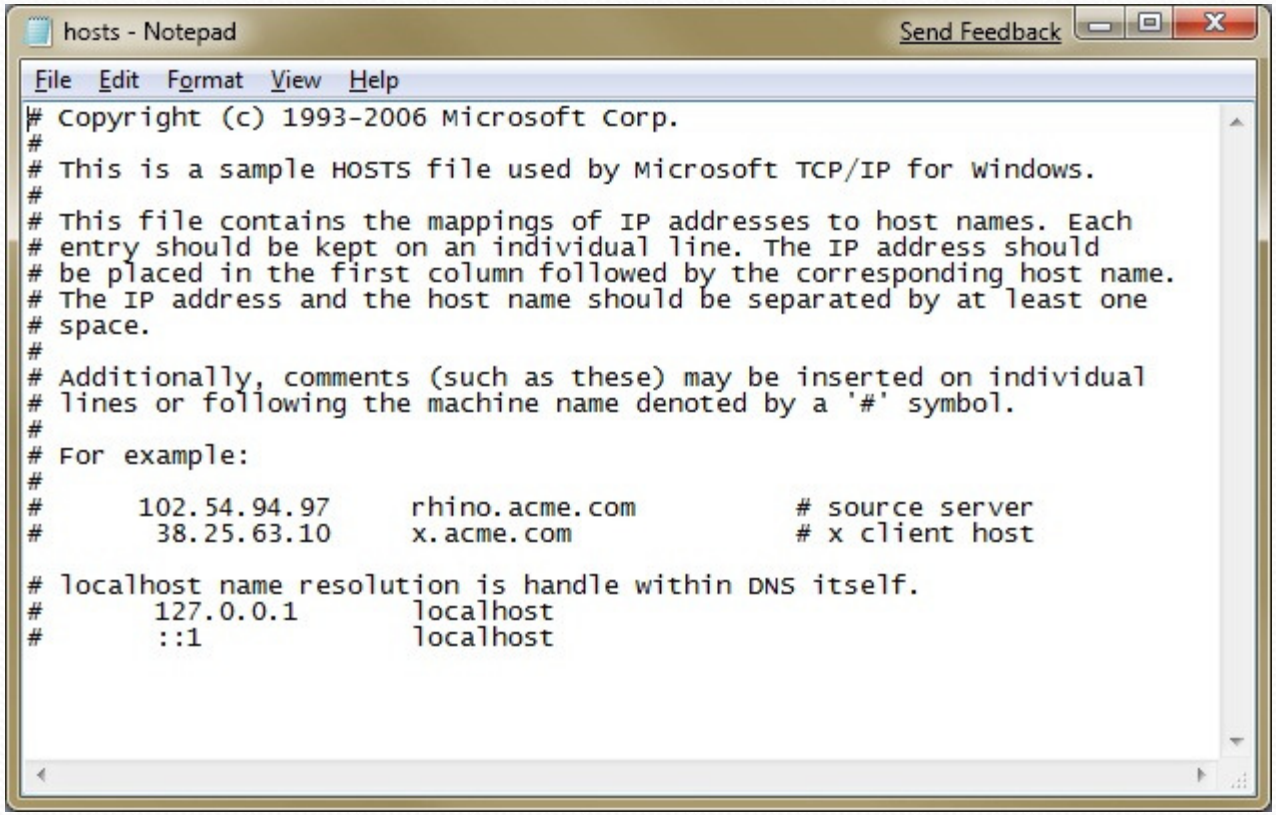


Figure 4-9 Substitute computer number

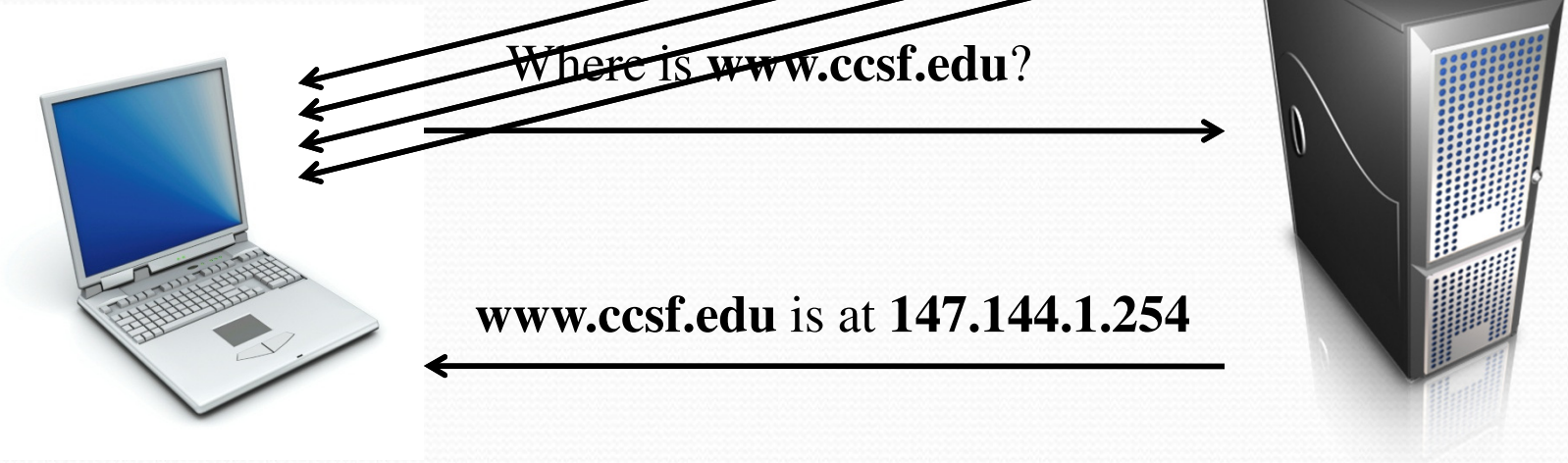
Local DNS Poisoning

- Put false entries into the Hosts file
- C:\Windows\System32\Drivers\etc\hosts



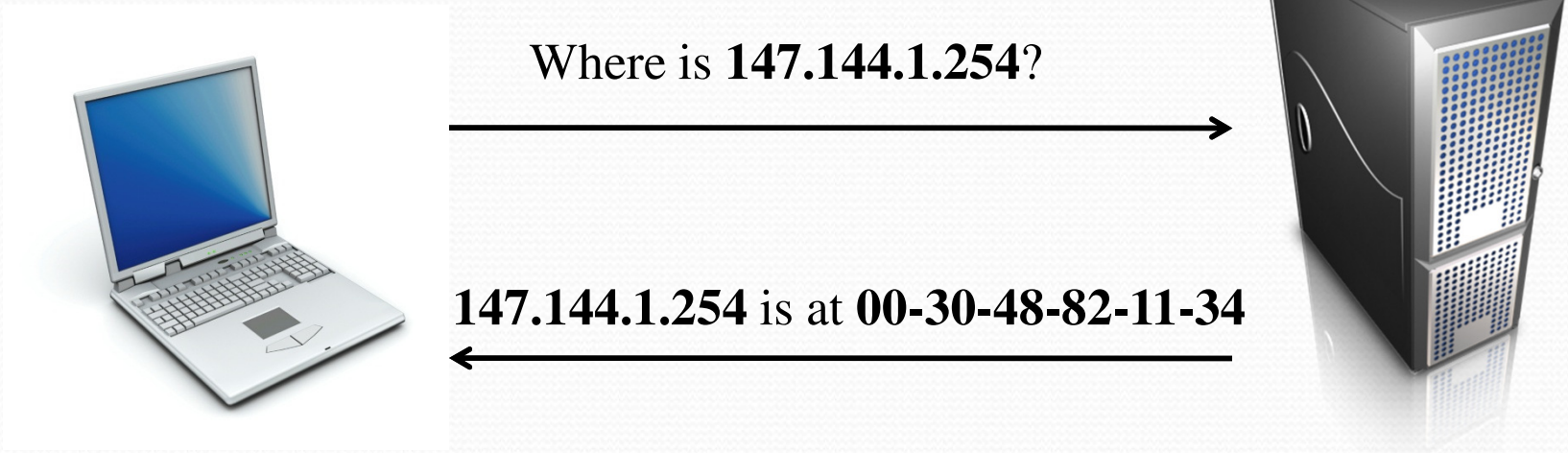
DNS Cache Poisoning

- Attacker sends many spoofed DNS responses
- Target just accepts the first one it gets



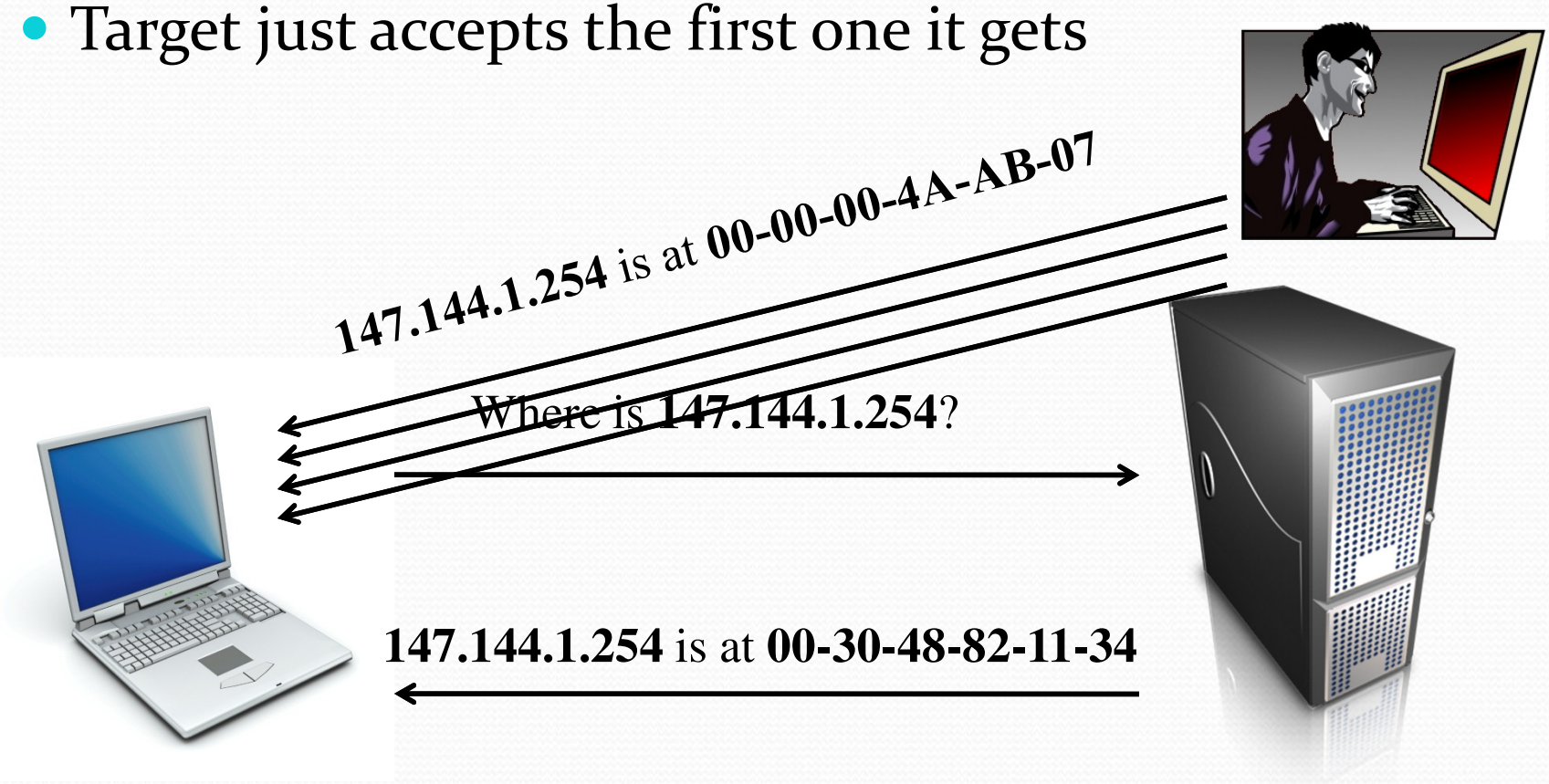
ARP (Address Resolution Protocol)

- ARP is used to convert IP addresses like **147.144.1.254** into MAC addresses like **00-30-48-82-11-34**



ARP Cache Poisoning

- Attacker sends many spoofed ARP responses
- Target just accepts the first one it gets



Results of ARP Poisoning Attacks

Result	Description
Steal data	An attacker could substitute his own MAC address and steal data intended for another device.
MAC flooding	Substituting the MAC address of the switch, an attacker could flood the switch with packets and force it to revert to a hub in order to use a protocol analyzer to view all traffic.
Prevent Internet access	An attacker could substitute an invalid MAC address for the network gateway so that no users could access external networks.
Man-in-the-middle	A man-in-the-middle device could be set to receive all communications by substituting that MAC address.

Table 4-3 Results of ARP poisoning attacks