Attack a computer network

Lecture 3

Data and Network Security

Information Gathering

- Find out initial information
  - Open Source: general information about a company that anyone can obtain
  - whois (unix), sam spade (third-party tool for windows)
  - nslookup
- Find out address range of the network
  - ARIN (American registry for Internet numbers) http://www.arin.net
    - whois -h rs.arin.net arin-net
  - Traceroute
- • Find active machines:
  - ping

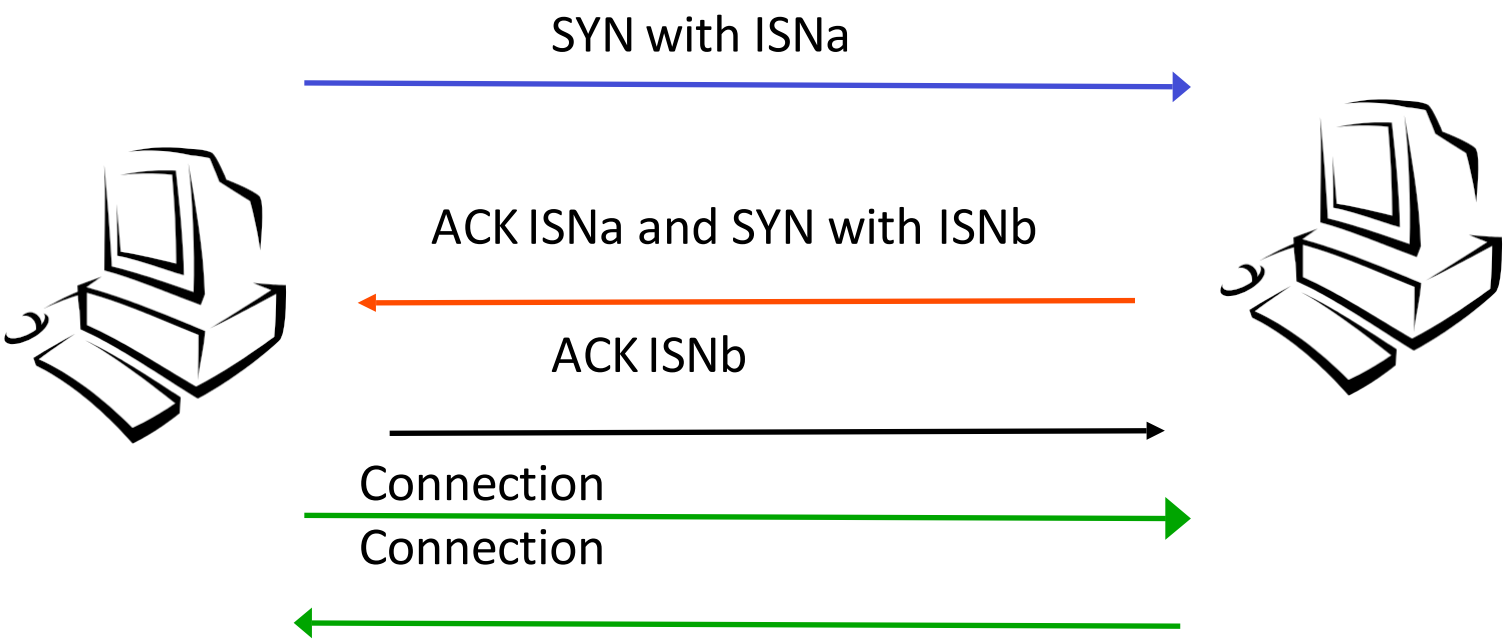
Information Gathering cont.

- Find open ports or access points:
  - Nmap http://www.insecure.org/nmap for UNIX
  - ScanPort http://www.dataset.fr/eng/scanport.html for Windows
  - War Dialers: Programs that find modems on a network
    - THC-Scan for Windows
- Figure out the operating system
  - Queso
  - Nmap

Information Gathering cont.

- Map out the network
  - Cheops http://www.marko.net/cheops/
  - Visual ping http://www.visualware.com/visualroute/
  - Traceroute
- Figure out which services are running on each port
  - Default port and OS
  - Telnet
  - Vulnerability scanners: programs that can be run against a site that give a hacker a list of vulnerabilities on the target host
    - SAINT http://www.wwwdsi.com/saint/
    - NESSUS http://www.nessus.org

TCP three-way handshake

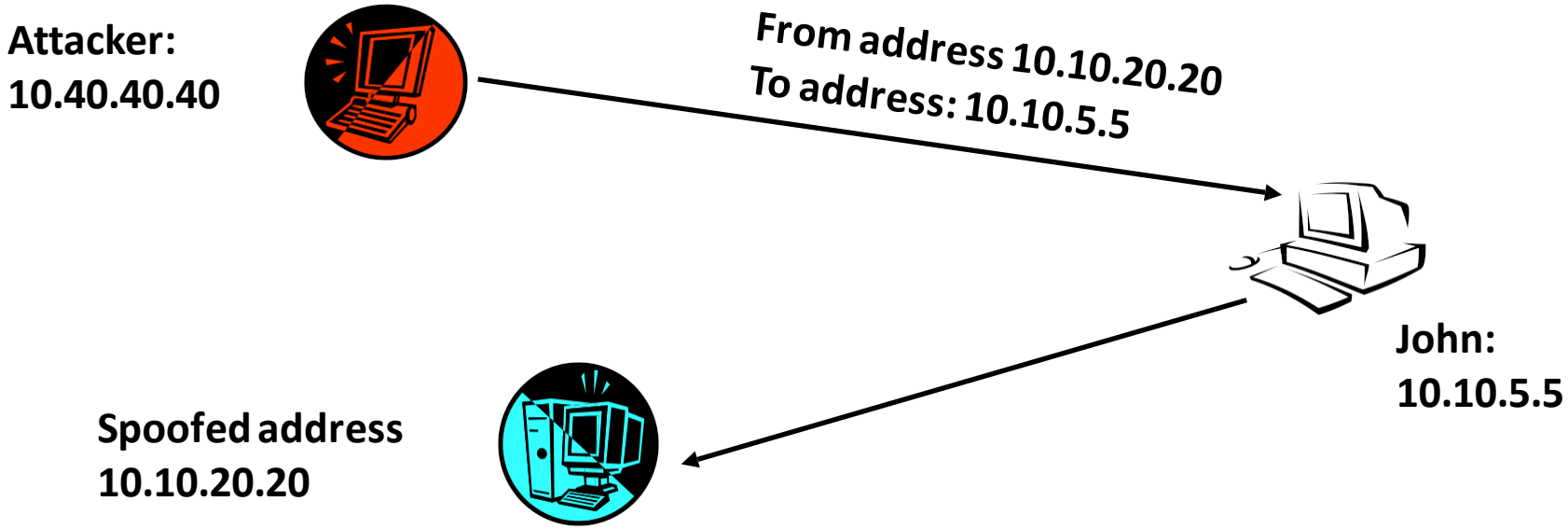


Types of Nmap scans

- **TCP Connect Scan:**
  - Attempts to complete the TCP three-way handshake and set up a connection
  - Easy to detect
- **TCP SYN Scans: "half-open scans"**
  - Sends a SYN to each target port. Target sends SYN-ACK if the port is open. The attacker send a RESET packet to abort the connection.
  - Hard to detect, only routers or firewalls will log (if enabled) the attackers IP.
- **FIN Scan:**
  - Violate the TCP specification by sending unexpected packets at the start of a connection
  - Attacker sends FIN packet, if the target port is closed a RESET packet is sent back, if open nothing is sent back.
- **Ack Scan:**
  - Sends an ACK packet to targets port. If RESET comes back from target Nmap will classify the port as "*unfiltered*" otherwise "*filtered*"

IP Spoofing.

- The intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- A hacker must find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.



Types of Spoofing

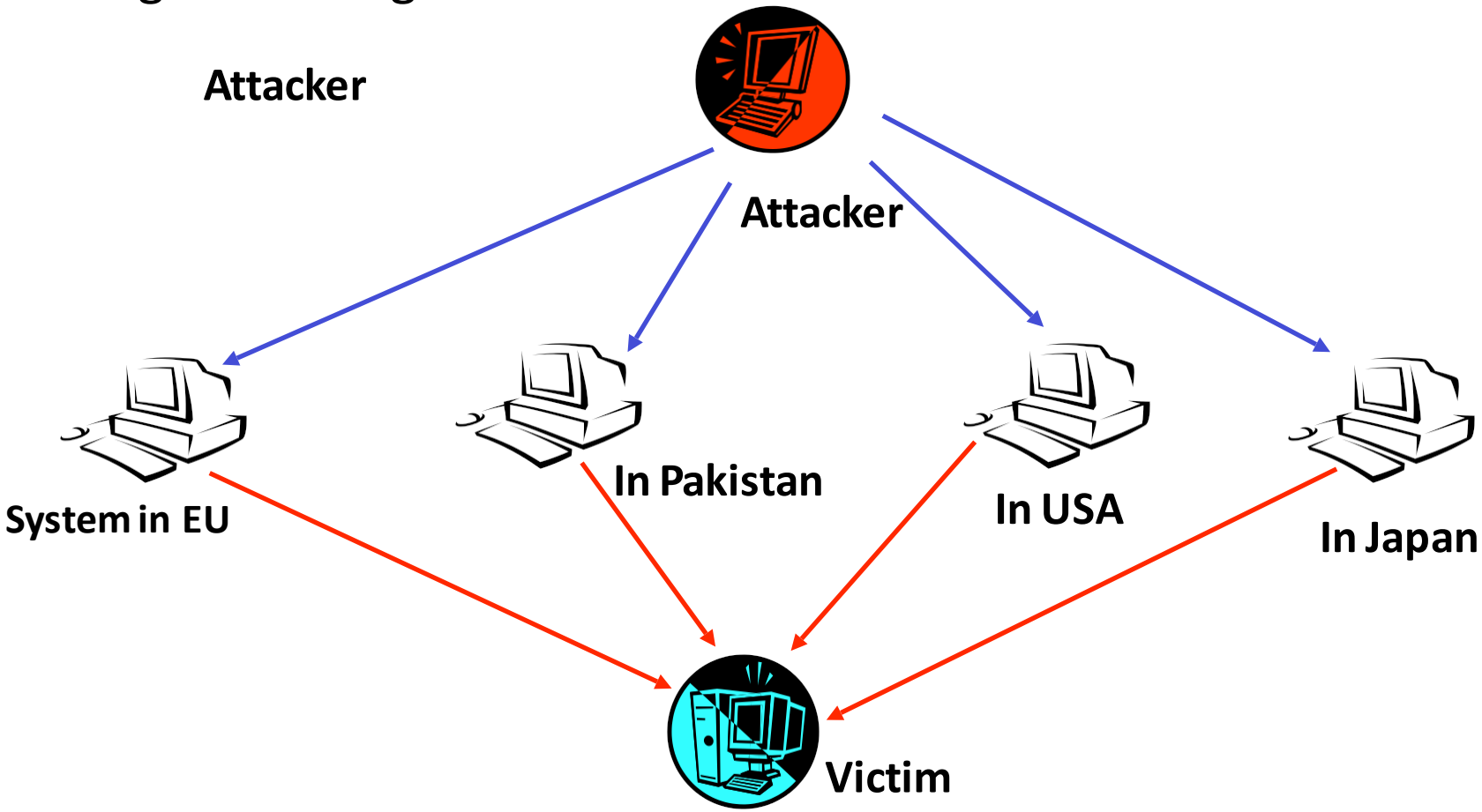
- **IP spoofing:** An attacker uses an IP address of another computer to acquire information or gain access
- **Email spoofing:** In essence, the email looks like it came from John, but in reality, John didn't send the email. Someone who was impersonating John send it.
- **Web spoofing:** Whenever an entity has to be trusted, the opportunity for spoofing arises.
- **Non-technical spoofing:** These types of attacks concentrate on compromising the human element of a company. This is done through social engineering techniques.

Denial of Service Attack.

- **DoS:** A type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.
  - Two general types of DoS attacks:
    1. **Crashing a system or a network:**
       - The attacker can send a data or packets which is not expected by victim
       - This attack requires little traffic to perform and human interaction to fix
    2. **Flooding the system or network** with so much information that it cannot respond:
       - This attack requires more energy from the attacker, recovering requires minimal human intervention

Distributed Denial of Service Attack.

- **DDoS:** Several machines are coordinated to launch an attack against a target machine or network at the same time



DoS

- Ping of Death
- SSPing
- Land
- Smurf
- Win Nuke
- CPU Hog
- SYN Flood

Buffer Overflow Attack

- A buffer overflow attack is when an attacker tries to store too much information in an undersized receptacle.
- Most of the newest exploits are based on buffer overflow attack
- Takes advantage of applications that do not adequately parse input by stuffing too much data into undersized receptacles
- Can cause attacks against all three areas to security:
  1. Attack against availability
  2. Attack against integrity
  3. Attack against confidentiality

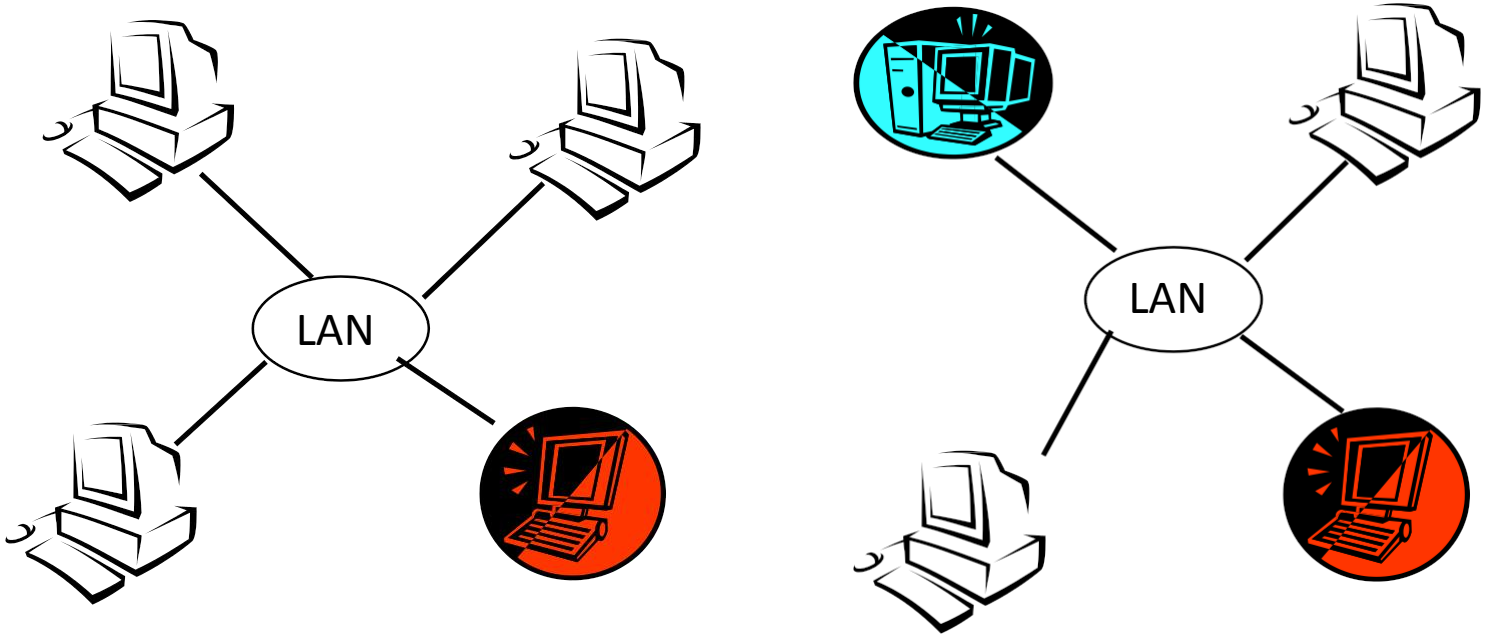
Example

- Some different buffer overflow attacks:
  - NetMeeting Buffer Overflow
  - Outlook Buffer Overflow
  - Linuxconf Buffer Overflow
  - IIS 4.0/5.0 Phone Book Server Buffer Overflow

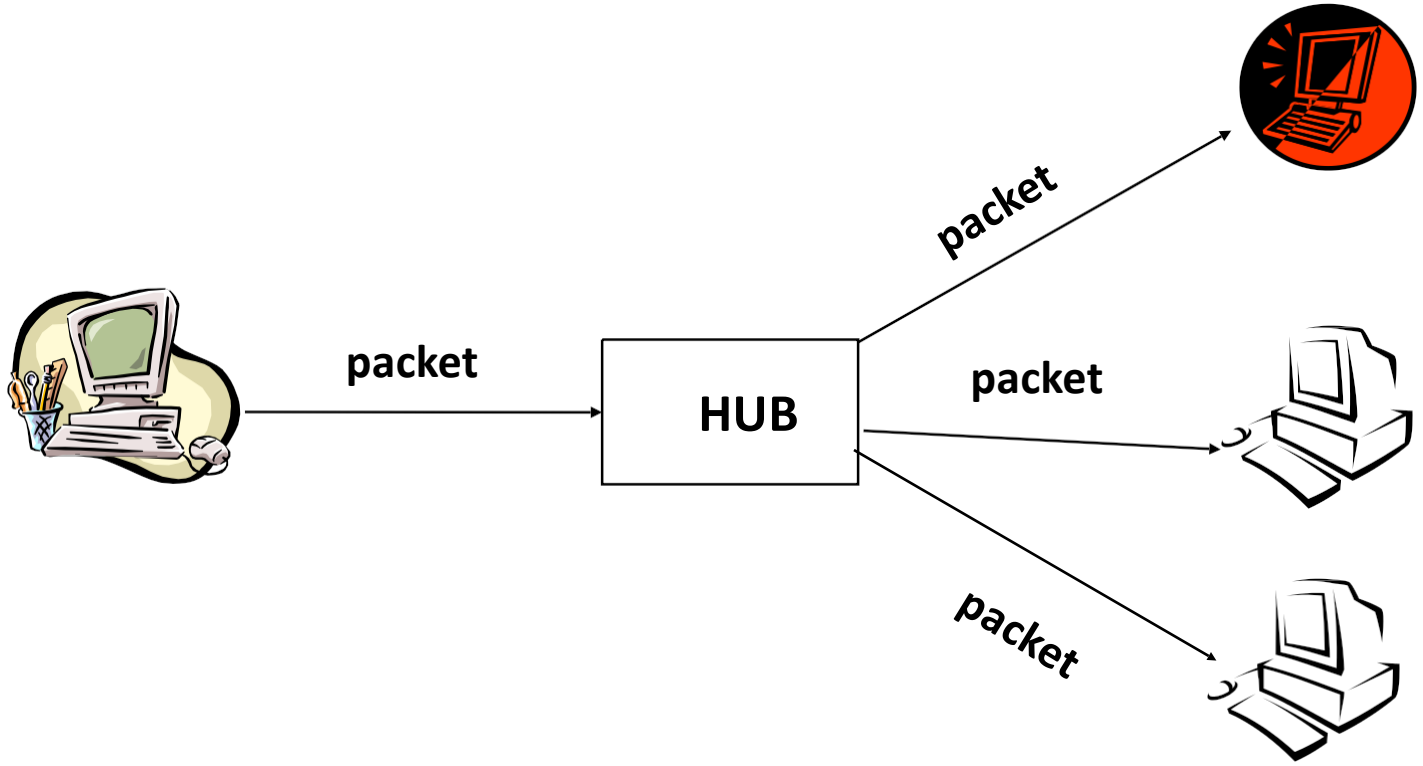
Sniffing

- A program that gather traffic from the local network
- Used by both attackers and network administrators
- Gathers packets at the Data Link layer
- An attacker must haven account on a machine in order to run the sniffer program.
- Sniffing tools available:
  - tcpdump http://www.tcpdump.com
  - windump netgroup-serv.polito.it/windump
  - Wireshark (ethereal)
  - Dsniff

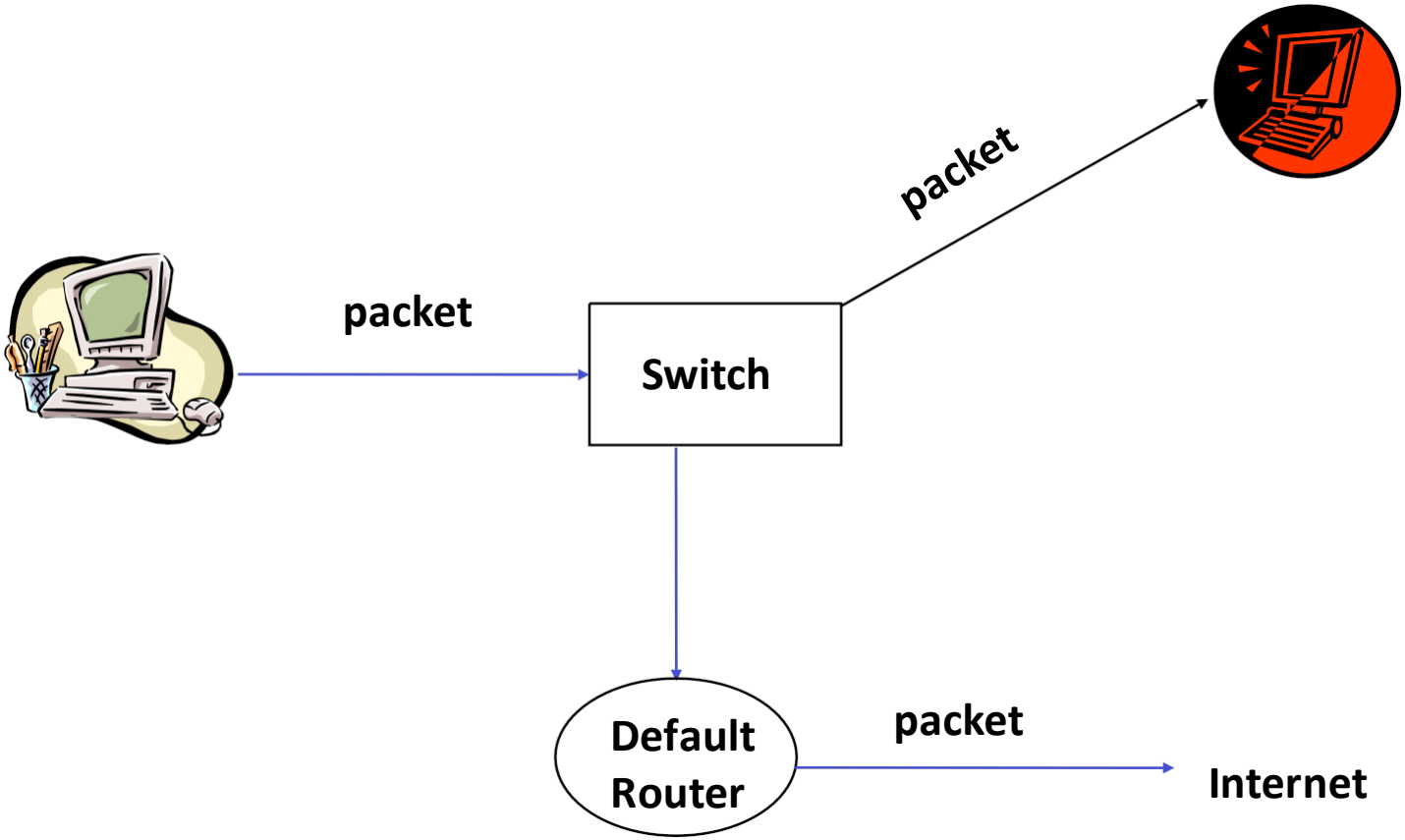
Island hopping attack



Passive Sniffing



Active Sniffing



Spoofed ARP Message