# CMPUT 333
# Assignment 3 – Parts 1, 2

**Port Scanning and Packet Sniffing**

# Port Scanning

- Nmap Scanning Tool
  - Installed on the Linux VMs
    - Feel free to download and compile the latest version
  - Man page and http://nmap.org
  - Scan whole networks
    - Useful when you don't know the IP addresses of your targets
    - Pay attention to the "**host discovery**" options
  - Figure out what services are running on the targets
  - Detect which OS the target runs
    - More information: http://nmap.org/book/osdetect.html

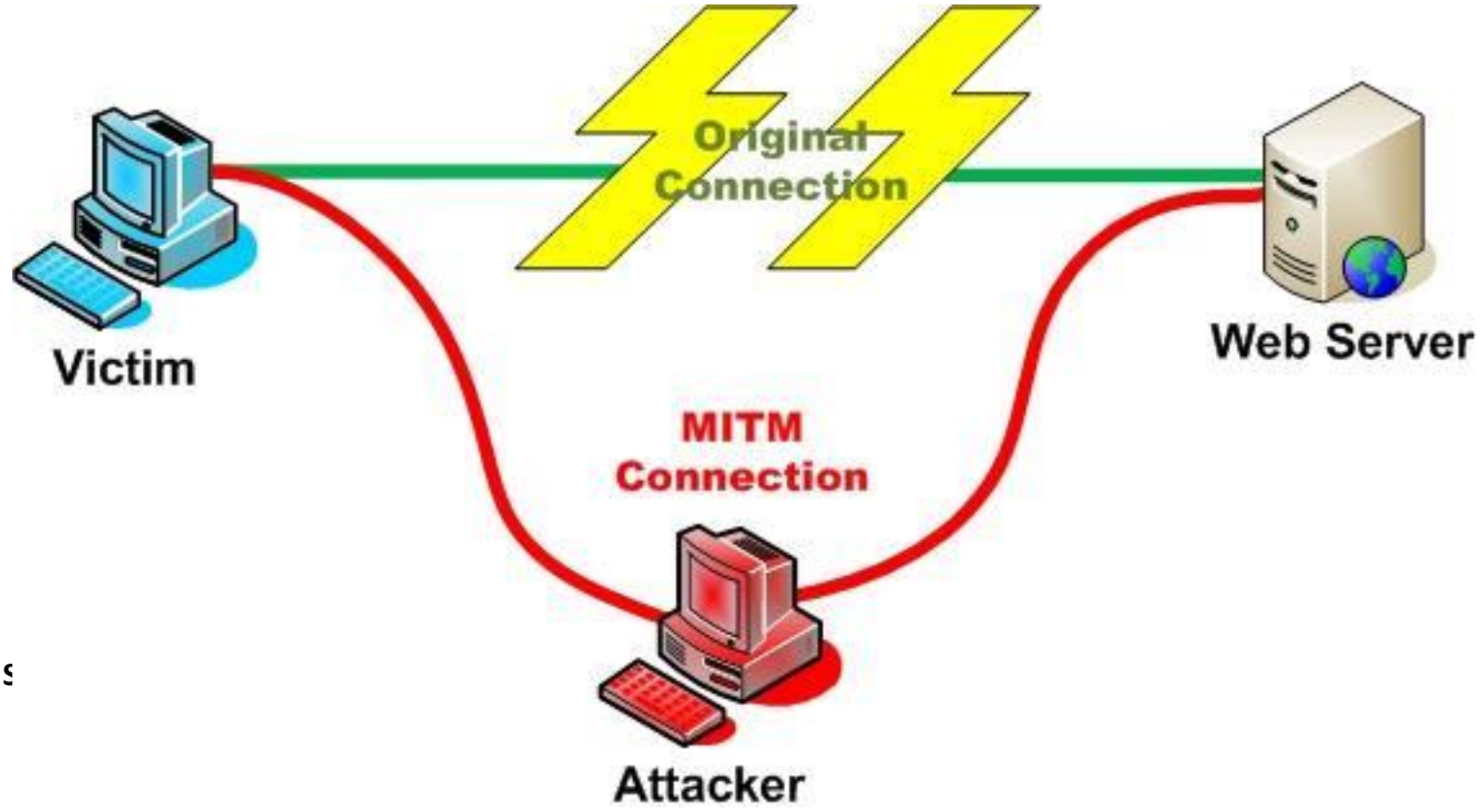
# Packet Sniffing

- On a shared medium you can just passively listen to all packets
  - Hubs
  - Wireless networks
- On switched networks you normally only receive packets sent to you
  - This includes the virtual network that connects your VMs
- You can perform a man-in-the-middle attack to insert yourself between the targets
  - One such attack is called "arp poisoning" and is the one you are advised to employ
  - Make sure you terminate the man-in-the-middle attacks when you have captured and saved the necessary traffic

# Packet Sniffing

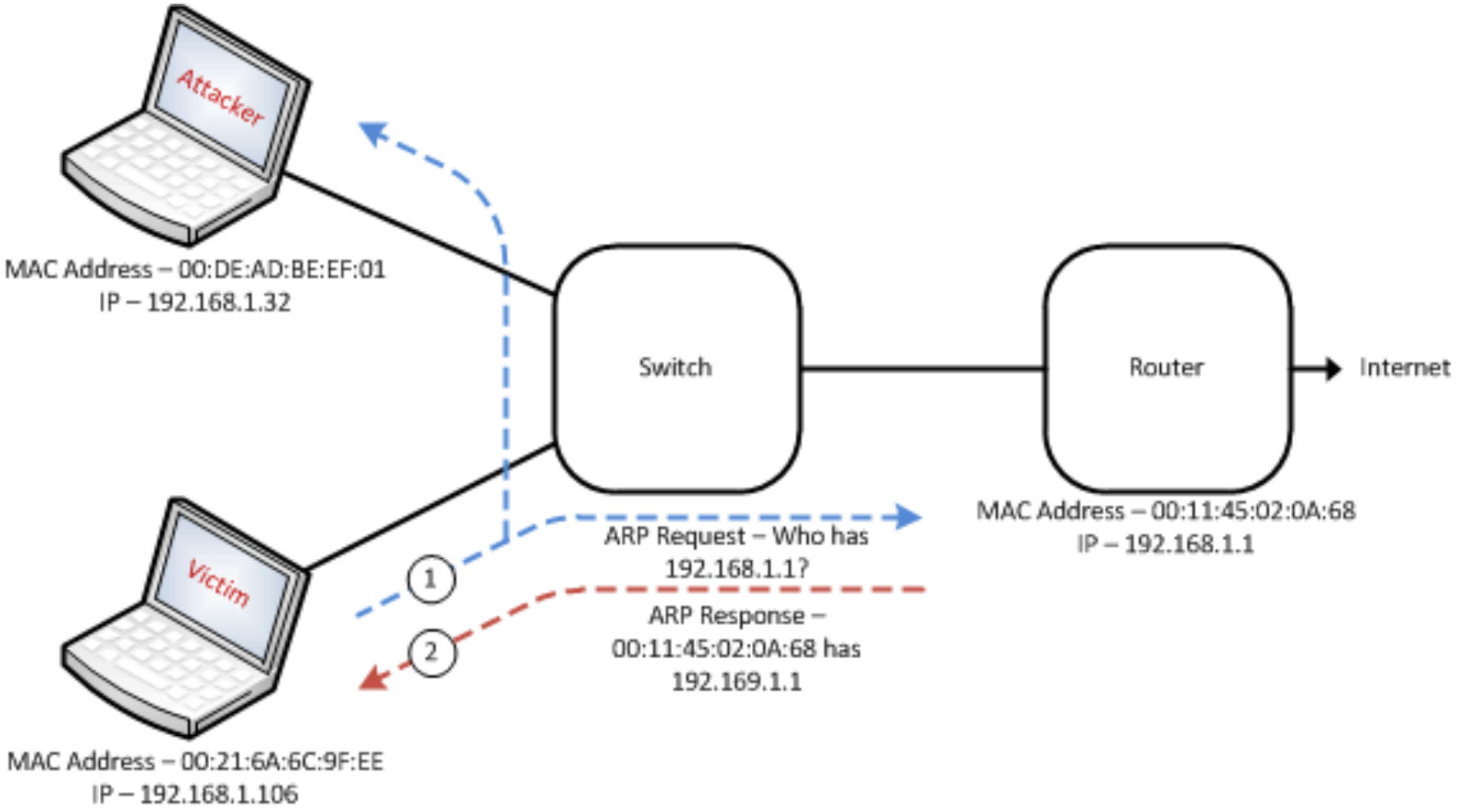
- On a shared medium you can just passively listen to all packets
  - Hubs
  - Wireless networks
- On switched networks you normally only receive packets sent to you
  - This includes the virtual network that connects your VMs
- You can perform a man-in-the-middle attack to insert yourself between the targets
  - One such attack is called "arp poisoning" and is the one you are advised to employ
  - Make sure you terminate the man-in-the-middle attacks when you have captured and saved the necessary traffic

# Man in the Middle Attack (MITM)



# MITM - ARP Poisoning

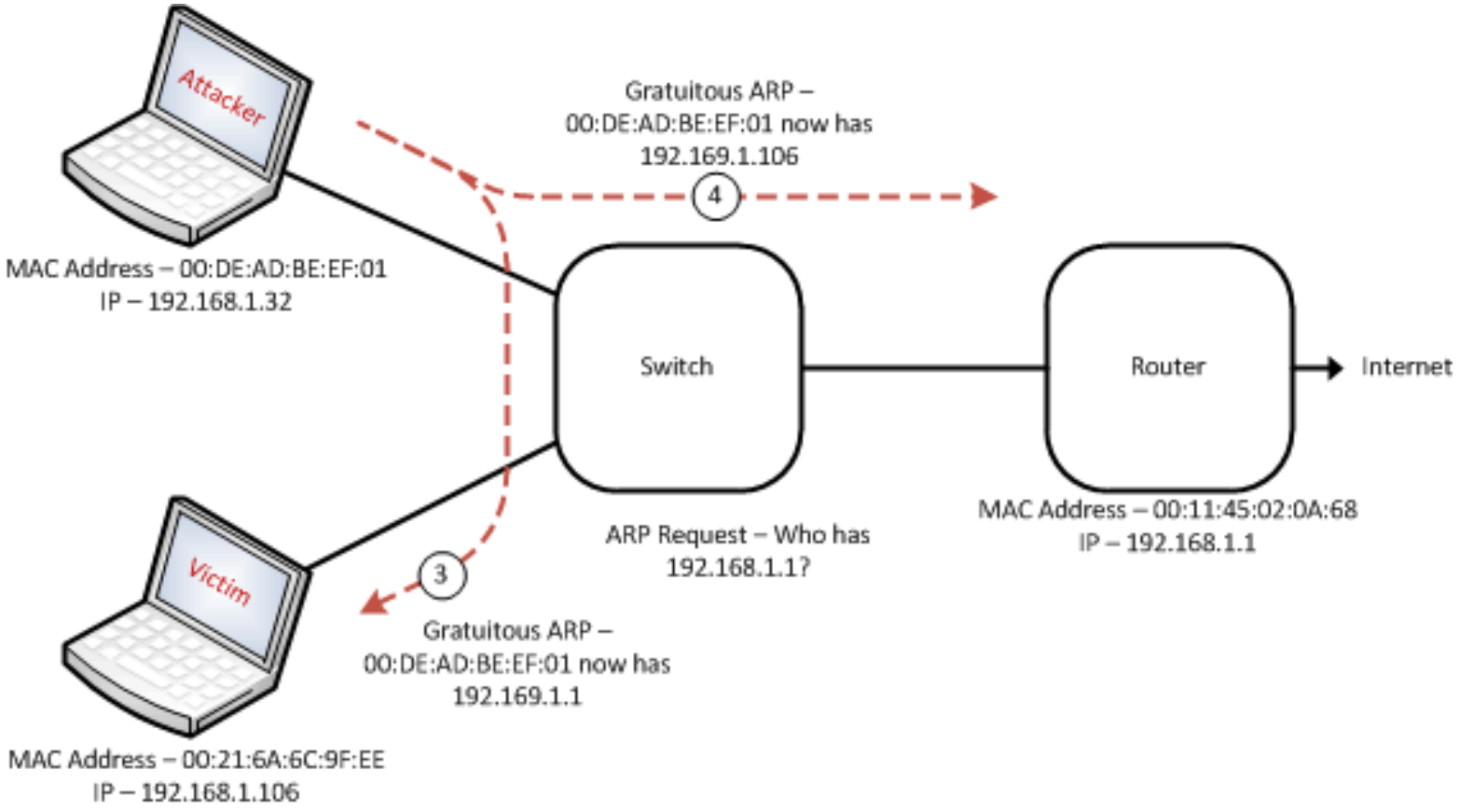
Before the ARP poisoning




**Source:** http://www.shortestpathfirst.net/2010/11/18/man-in-the-middle-mitm-attacks-explained-arp-poisoining/

# MITM - ARP Poisoning

During the ARP Poisoning




**Source:** http://www.shortestpathfirst.net/2010/11/18/man-in-the-middle-mitm-attacks-explained-arp-poisoining/

# Packet Sniffing and MITM Tools

- ettercap
  - Used to perform a variety of man-in-the-middle attacks as well as to do the actual sniffing
  - Man page
  - http://ettercap.sourceforge.net/
  - Installed on the Linux VMs
  - Can read/write pcap files
- tcpdump
  - Command line tool that can perform packet sniffing
  - You will need to first perform the man-in-the-middle attack before tcpdump sees the traffic
  - Installed on the Linux VMs
  - Can read/write pcap files

# Packet Sniffing and MITM Tools

- Wireshark
  - Another tool for packet sniffing
  - Has a large number of protocol dissectors
    - Useful for decoding the captured data
  - Can read/write pcap files
  - Again, you will first need to perform the man-in-the-middle attack with another tool
  - You can also run wireshark on your local machine and use it to analyze the capture files that you have collected on the VM
  - Can be downloaded from: https://wireshark.org/download.html

# Questions?