Introduction to Computer Security

Project II: Phishing Attacks in Wi-Fi Networks

Chi-Yu Li (2020 Spring)
Computer Science Department
National Chiao Tung University

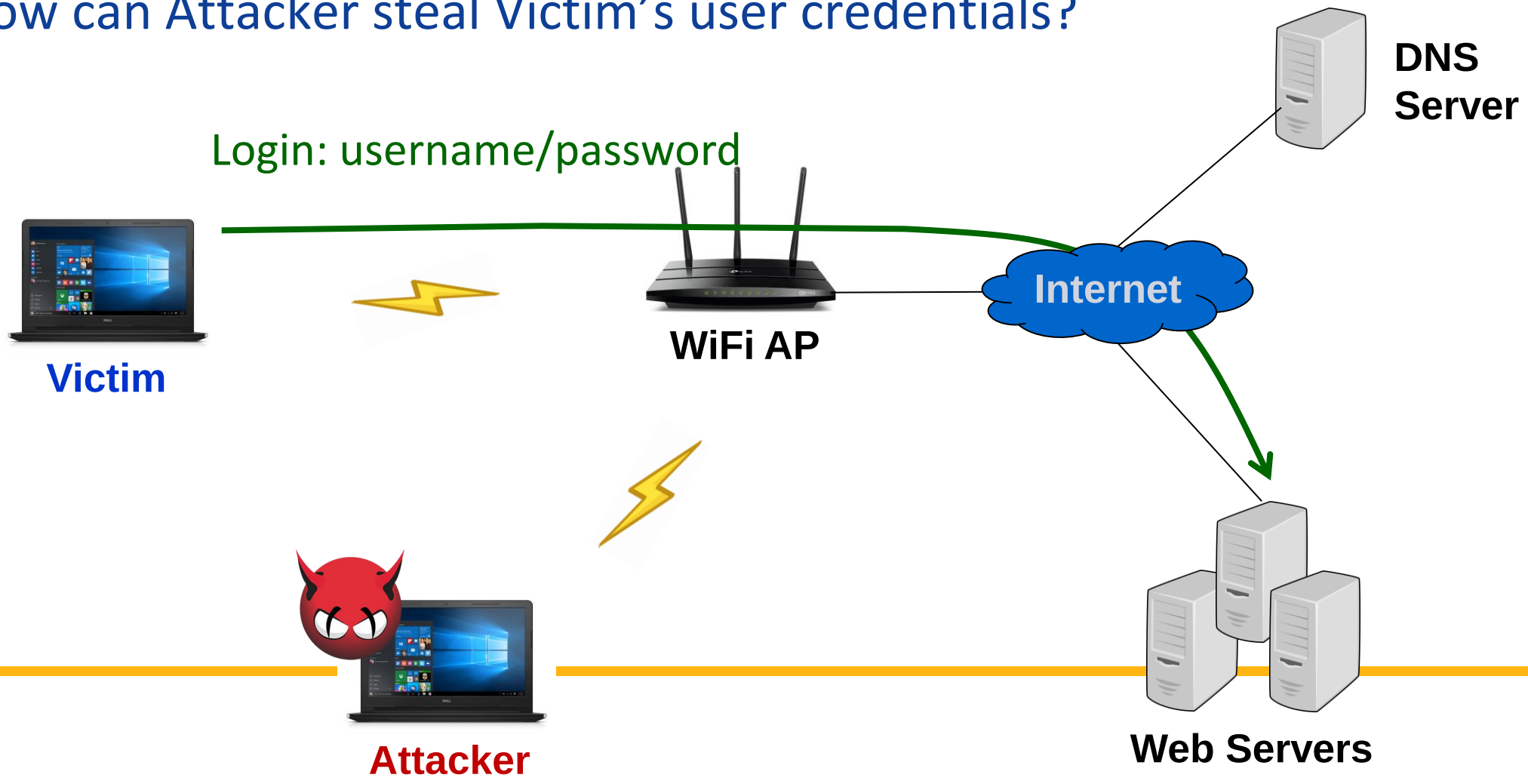
Goal

- Understand how user credentials can be leaked by a man-in-the-middle attack over Wi-Fi networks

- You will learn how to
  - scan IP/MAC addresses of the devices in a Wi-Fi network
  - launch an ARP spoofing attack
  - launch a pharming attack
  - launch a man-in-the-middle attack

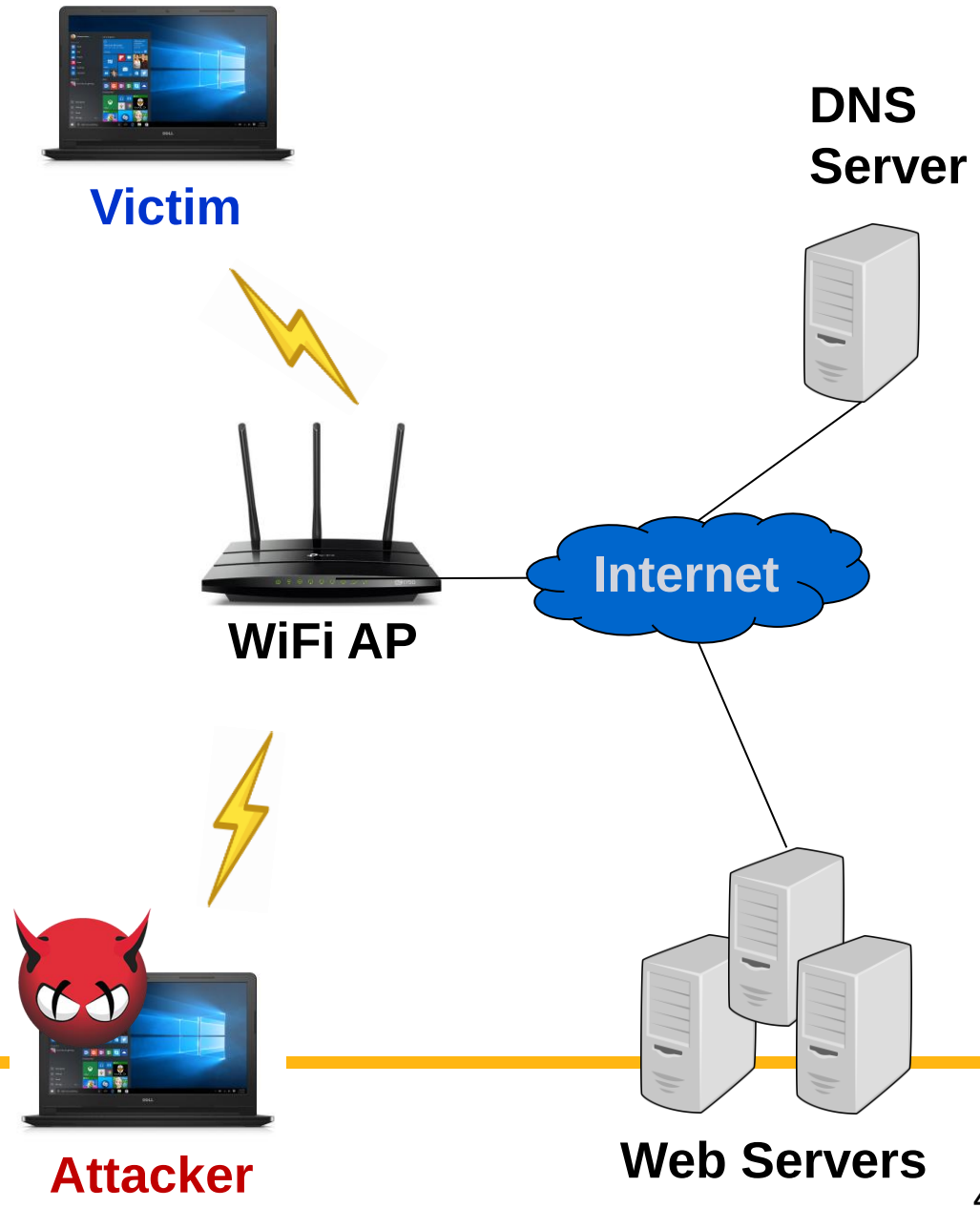
Attack Scenario

- How can Attacker steal Victim's user credentials?



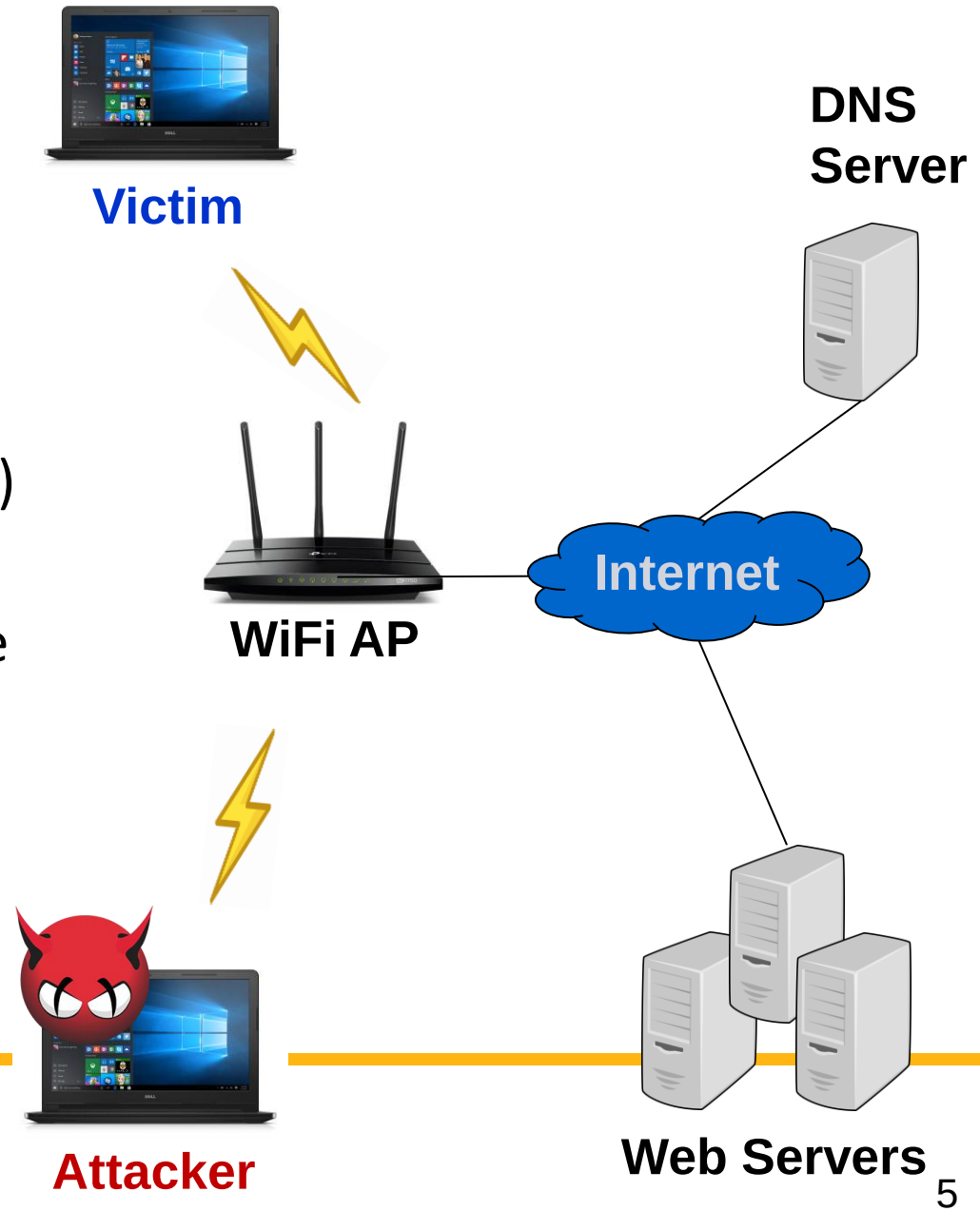
Major Ideas

- Redirect Victim's traffic to Attacker
  - Man-in-the-middle based on ARP spoofing
  - How to know Victim's IP/MAC address?
- Unencrypted sessions
  - Parse HTTP messages
- How about encrypted sessions?
  - Pharming attack: redirect an HTTP request to a phishing web page



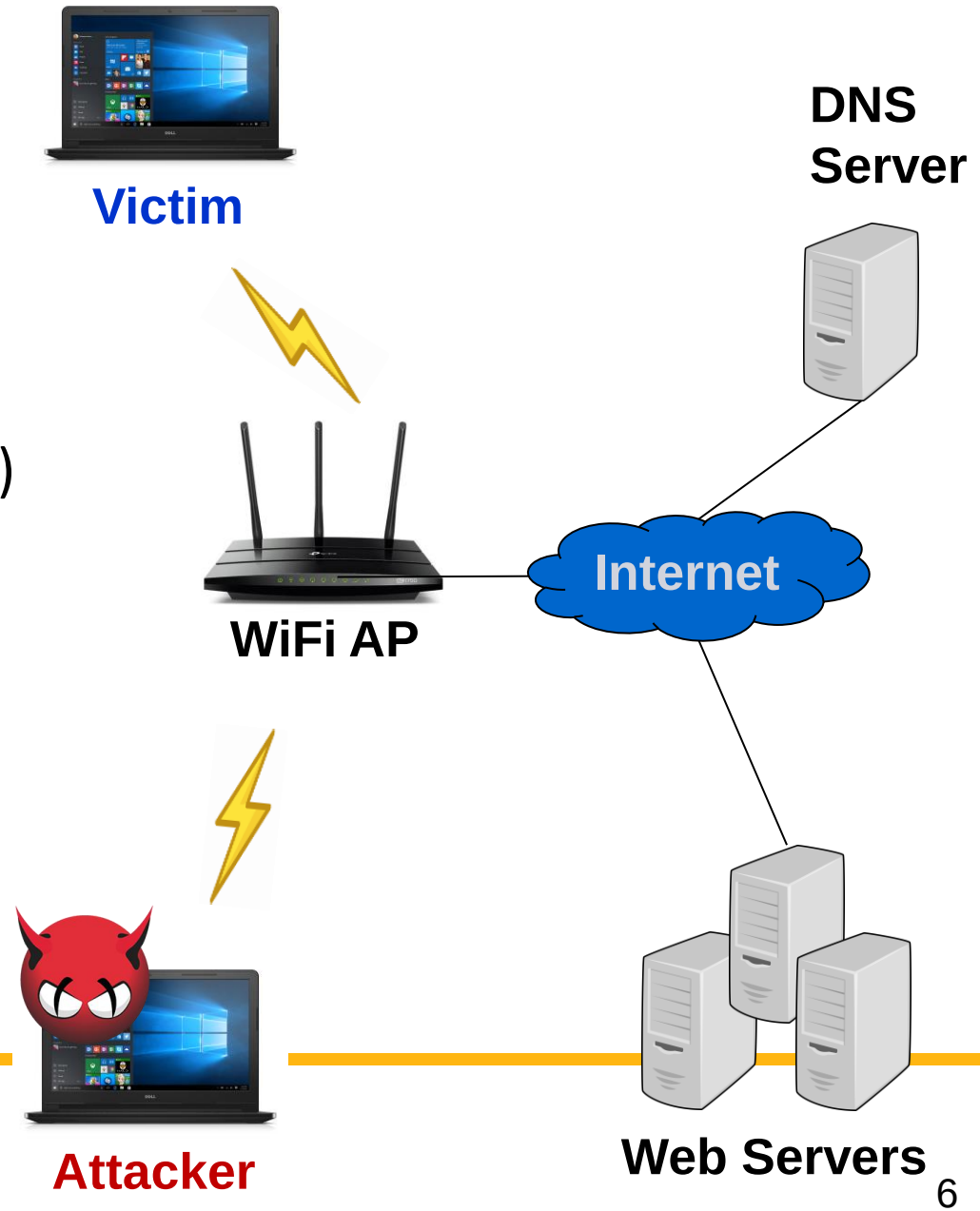
Tasks: Two Attacks and One Report

- Man-in-the-middle Attack (40%)
  - Obtain all other client devices' IP/MAC addresses in a connected Wi-Fi network (Task I)
  - ARP spoofing for all other client devices in the Wi-Fi network (Task II)
  - Fetch all the inputted username/password strings on a specified web page



Tasks: Two Attacks and One Report

- Pharming Attack (30%)
  - Obtain all other client devices' IP/MAC addresses in a connected Wi-Fi network (Task I)
  - DNS spoofing attack on a specified web page (Task III)
- Report (30%)



Task 1: Obtain Other Client Devices' IP/MAC Addresses in a Wi-Fi Network

- Scan all the devices' IP/MAC addresses in the Wi-Fi network
  - You can use 'Scapy' library in Python or commands 'nmap', 'arp', and 'route'

```
➜  project 2 cat scan_result
Available devices
------------------------------------------
IP                          MAC Address
------------------------------------------
192.168.1.1                 fc:f5:28:67:dd:db
192.168.1.101               cc:2f:71:fe:45:7f
192.168.1.104               54:35:30:73:c1:87
```

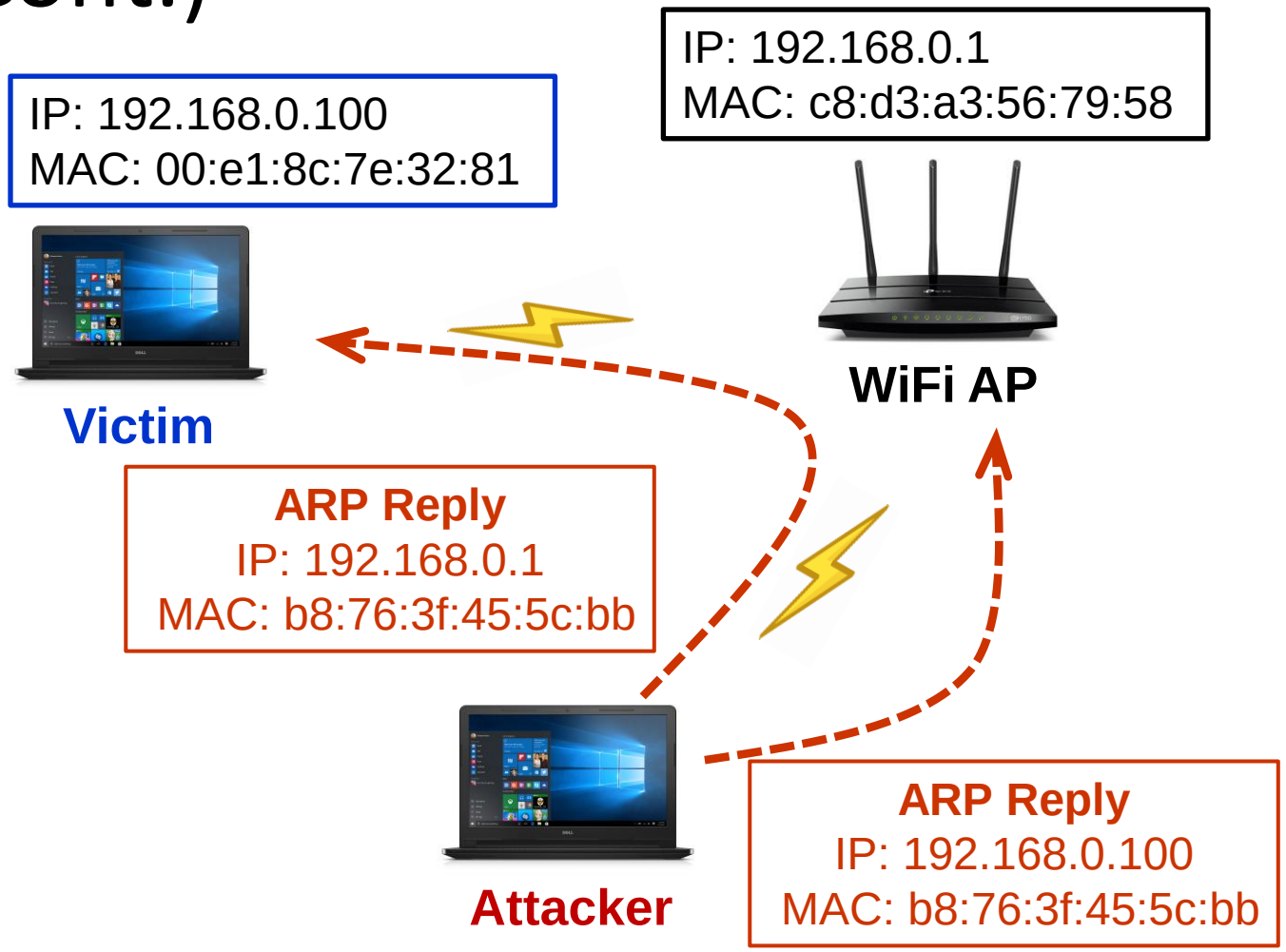
- Fetch the IP/MAC addresses of all the other client devices

Task II: ARP Spoofing

- What is ARP (Address Translation Protocol)?
  - A communication protocol: discovering the link layer (or MAC) address associated with a given IP
  - A request-response protocol: messages are encapsulated by a link-layer protocol
    - ARP request: broadcast
    - ARP response: unicast
  - Never routed across internetworking nodes

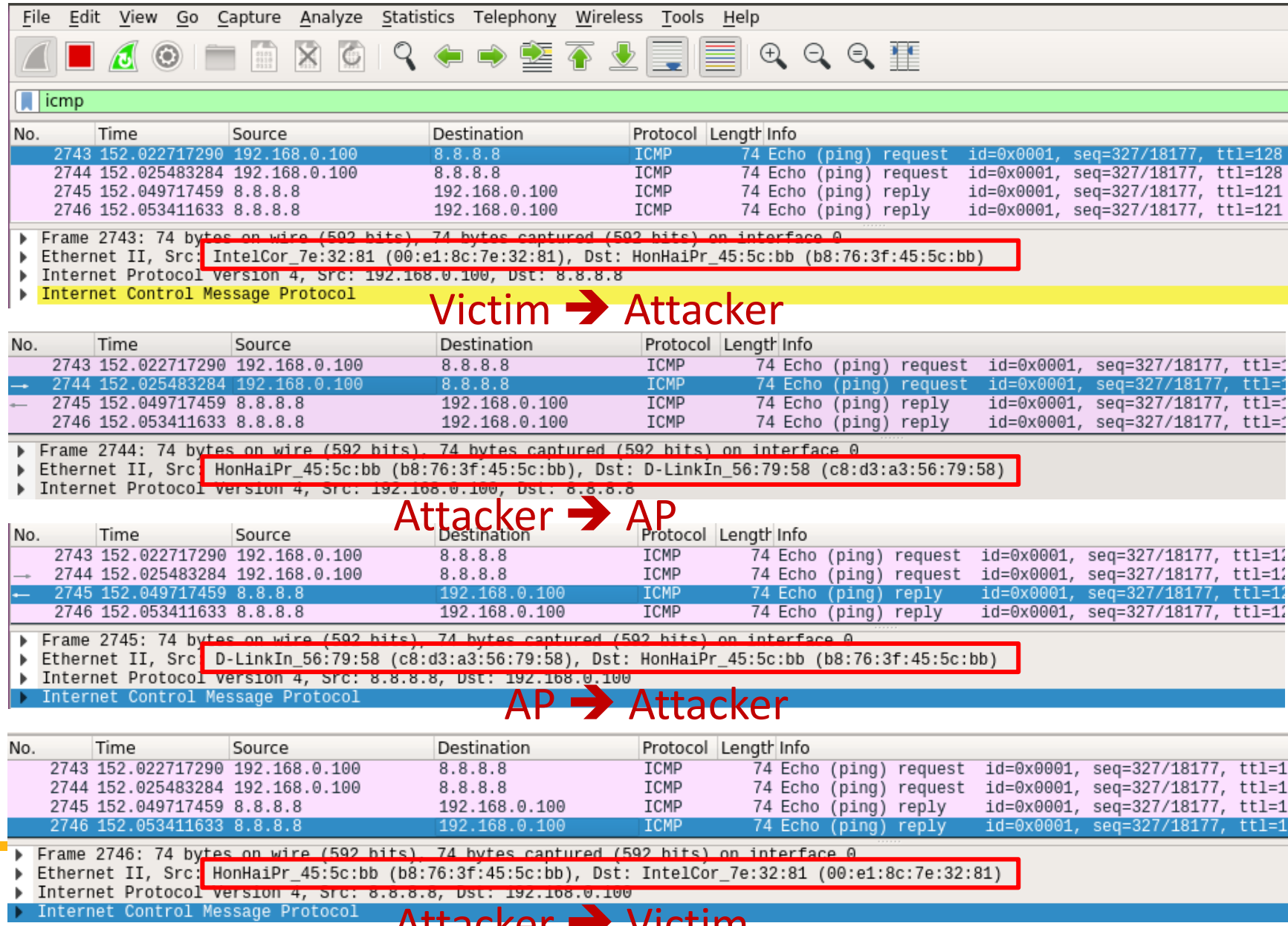
Task II: ARP Spoofing (Cont.)

- Generate spoofed ARP replies for all other client devices
  - You can use 'Scapy' library in Python
- Both uplink and downlink should be considered
  - Other client devices' network services can work normally



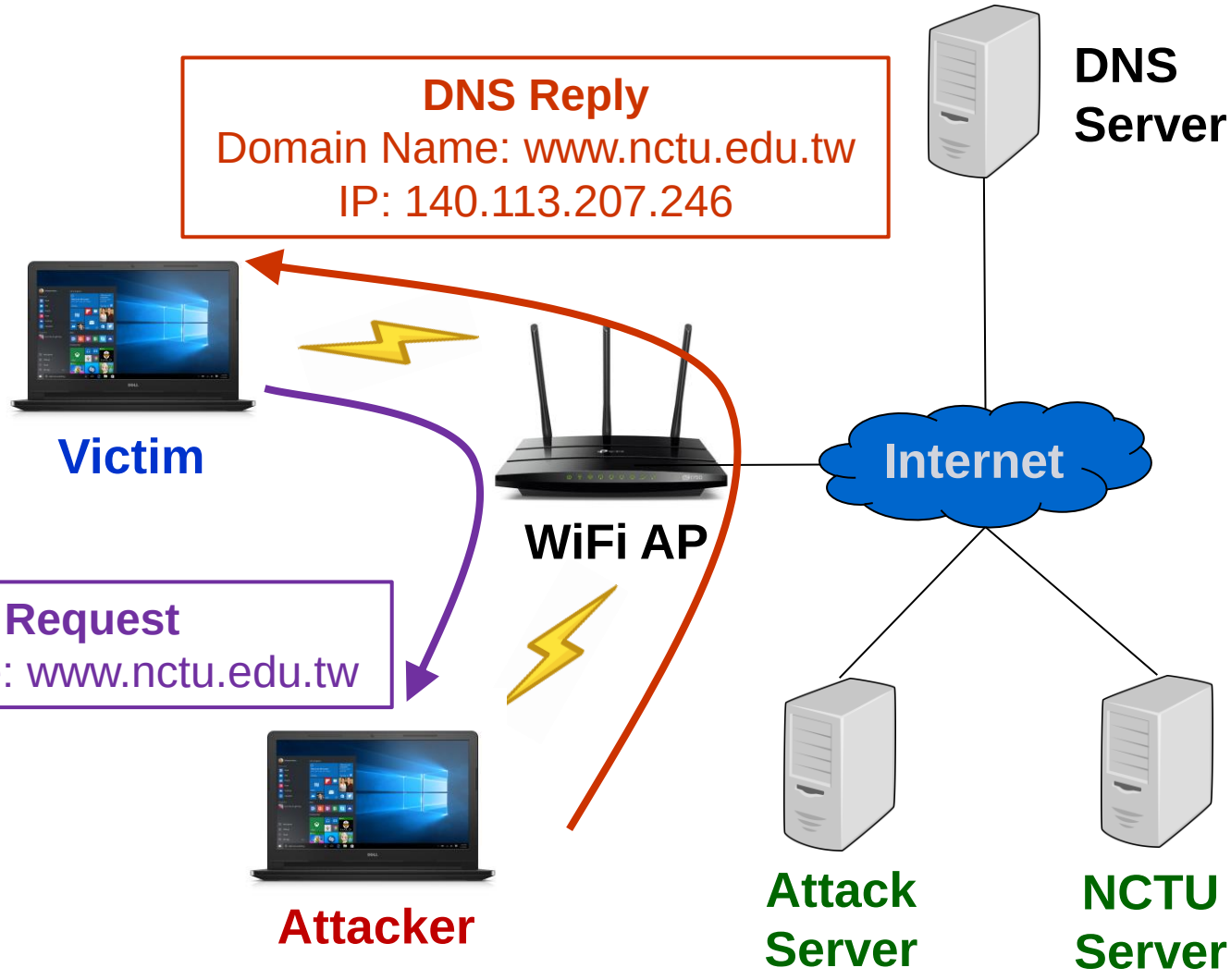
Task II: ARP Spoofing (Cont.)

- An example trace of the successful ARP spoofing at Attacker



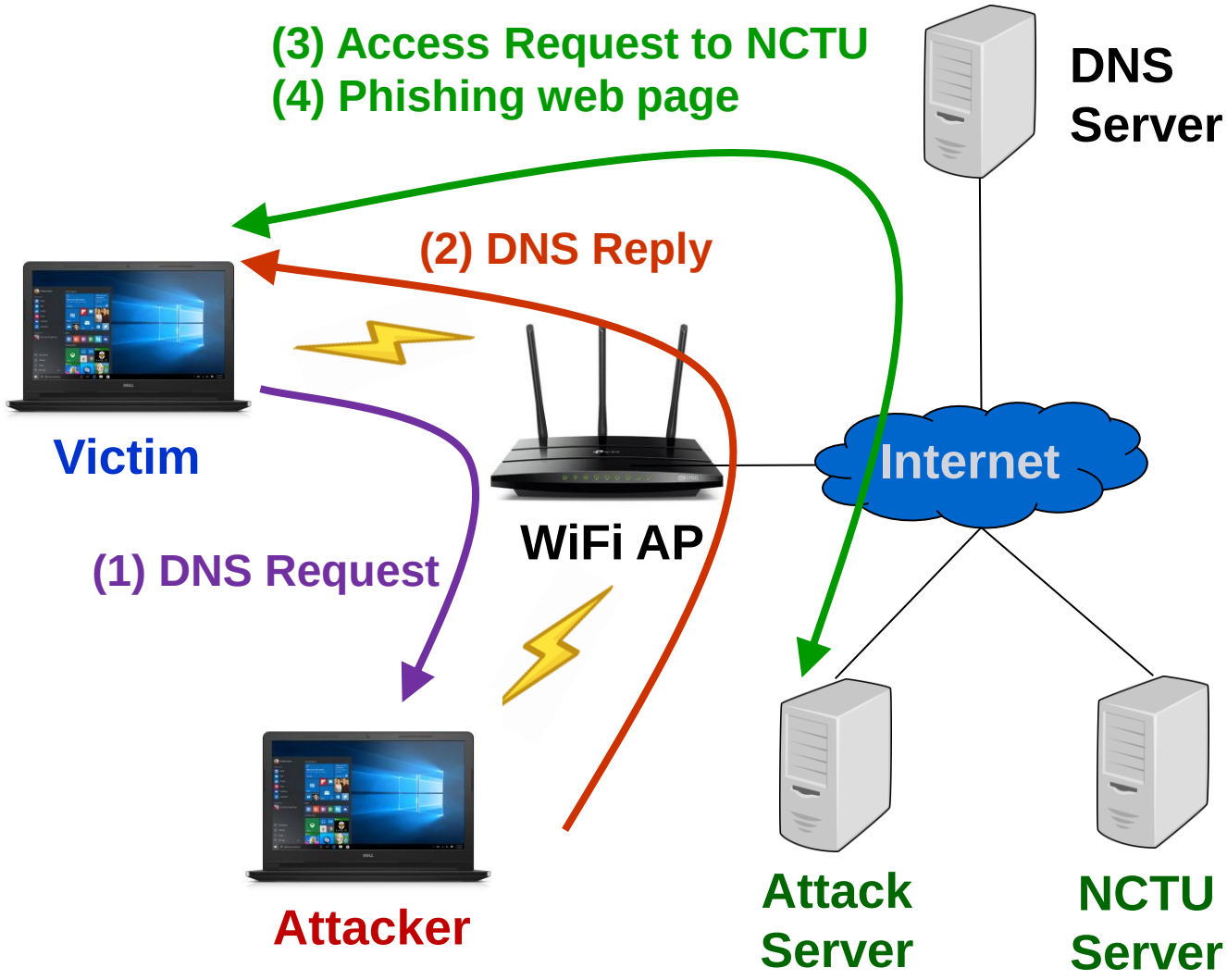
Task III: DNS Spoofing

- Intercept DNS requests for a specific web page and generate spoofed DNS replies with the attack server's IP
  - You can use 'Scapy' and 'NetfilterQueue' library in Python



Task III: DNS Spoofing

- Successful attack
  - An access request to NCTU home page will be redirected to the attack server (140.113.207.246)
  - A phishing web page will be shown to Victim

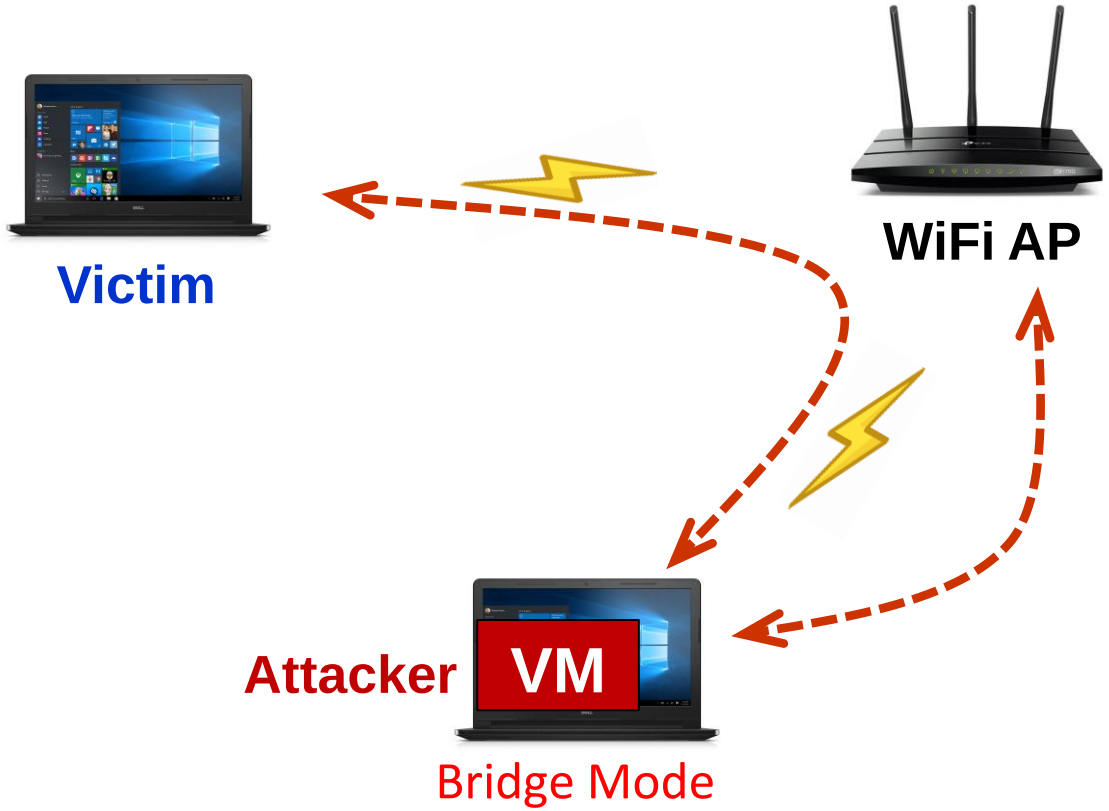


Requirements

- You need to develop/run your program in a given virtual machine
  - VM image: Please download it from Link
    - Username/password: cs2020/cs2020
- You are allowed to use C/C++ and Python
- You are allowed to team up. Each team has at most 2 students
  - Teams: discussions are allowed, but no collaboration
- Please submit your source codes and report to E3

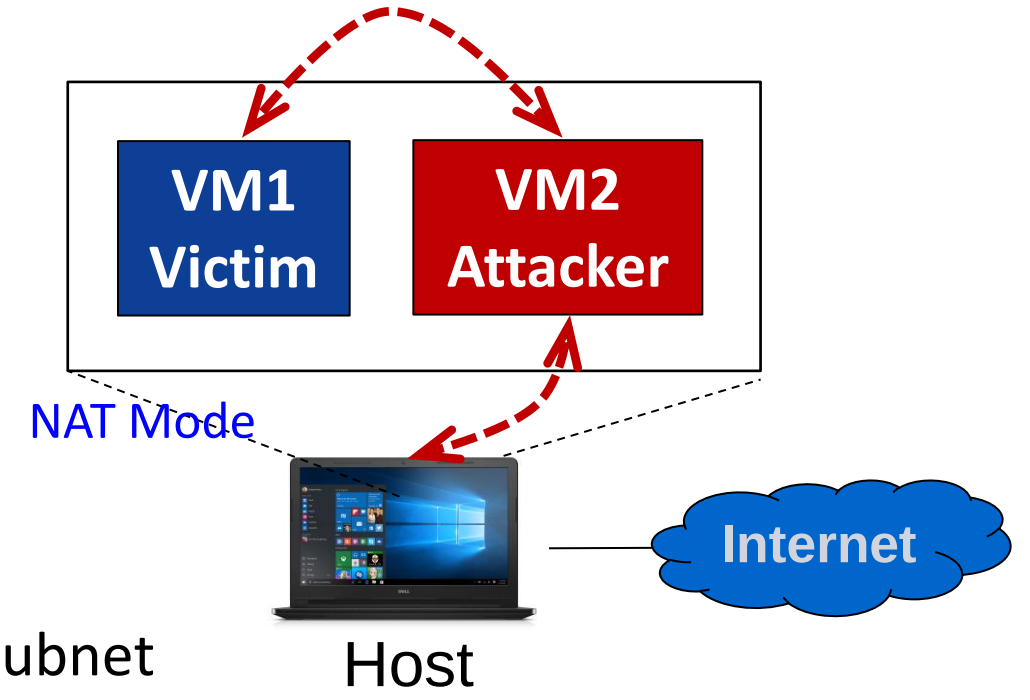
Test Scenario I: Target Scenario

- However, this scenario does not work for all the combinations of OS and VM software
  - Working: Linux + VirtualBox/VMware
  - Not working properly
    - Windows + VirtualBox/Vmware
    - MacOS + VirtualBox
- You can choose Test Scenario II



Test Scenario II: Alternative Scenario

- VM2 (Attacker) launches attacks on VM1 (Victim)
  - NAT mode shall be used for VMs
- Host is similar to the role of the AP in Test Scenario I
  - Scenario I: The Wi-Fi devices are in the same subnet
  - Scenario II: The VMs are in the same subnet
- Host can be connected to the Internet via Wi-Fi or wired Ethernet



Important: How to Prepare Your Attack Programs?

- Must provide a **Makefile** which compiles your source codes into two executable files, named **mitm_attack** and **pharm_attack** (Missing: -20%)
- Test requirements for the programs
  - Must be run in the given VM without any additional tools or libraries
  - Must use the following parameters
    - Test web page in the man-in-the-middle attack: http://140.113.207.246/login.php
    - DNS spoofing for the NCTU home page: http://www.nctu.edu.tw
    - Attacker server IP in the DNS spoofing: 140.113.207.246
  - Must work for the test commands: ./mitm_attack and ./pharm_attack

Important: How to Prepare Your Attack Programs?

- Results from the MitM attack (./mitm_attack)
  - Print out the IP/MAC addresses of all the Wi-Fi devices or VMs except for Attacker and AP/Host
  - Print out the username and password which a user submits to the website http://140.113.207.246/login.php using any of the Wi-Fi devices or VMs
- Results from the pharming attack (./pharm_attack)
  - Print out the IP/MAC addresses of all the Wi-Fi devices or VMs except for Attacker and AP/Host
  - Redirect the NCTU home page (www.nctu.edu.tw) to the phishing page (140.113.207.246)
- Notes
  - TA will verify the MitM attack by giving inputs on the website using one Wi-Fi device or VM
  - TA will verify the pharming attack by accessing the NCTU page on one Wi-Fi device or VM

Important: How to Prepare Your Report?

- Item 1 (10%): please give evidence that you have finished the MitM attack
  - Specify your scenario (I or II) and Illustrate your results based on some snapshots
- Item 2 (10%): please give evidence that you have finished the pharming attack
  - Specify your scenario (I or II) and Illustrate your results based on some snapshots
- Item 3 (10%): please propose a solution that can defend against the ARP spoofing attack
  - No more than 200 English words
- Note: the report must be written in English with font size 11 or 12 in Times New Roman. It must be submitted in one PDF file with a name “report.pdf.”

Project Submission

- Due date: 5/7 11:55pm
  - Makeup submission: 5/21 11:55pm (75 points at most)
- Submission rules
  - Put all your files into a directory and name it using your student ID(s)
    - If your team has two members, please concatenate your IDs separated by "-"
  - Zip the directory and upload the zip file to New E3
  - A sample of the zip file: 01212112-02121221.zip
    - Makefile
    - mitm_attack.cpp
    - report.pdf
    - mitm_attack.h
    - ….