ECE-GY 9383 Network Security LAB 2 - ARP Spoofing
Credit to: Prof. Danny Y. Huang, Vaibhav Jain

What to Return: A zip file that contains the following uploaded to the course Gradescope site

1. **A PDF file that contains all the answers to the question,**
2. **Task 3 Code**

Task 0. Setting up SEED labs (5 points)

Overview: Set up the SEED Lab environment

Steps: Follow either Option A or Option B, but not both Options.

- Option A: Creating SEED labs on DigitalOcean.
    - Follow this guide. I strongly recommend using DigitalOcean as the cloud provider as the cost is predictable (i.e., $10/month). Follow Step 1, Step 2, and Step 3B of the guide; ignore Step 3A.
- Option B: Creating SEED labs on VirtualBox.
    - Follow this guide only if your personal computer runs Linux, Windows 10, or the Intel macOS. If you run the latest macOS on the M1 chip, you have to choose Option A.

My recommendation is to go for Option A. It is the easier way to set up the environment. Now the DigitalOcean has a good deal for new users. New users will have $100 credit for 2 months so it will cover all the fees throughout this whole semester. For Option B, you need to make sure that the host machine (which runs VirtualBox) should have good performance (at least 4 core cpu and 8gb mem).

Also note, if your computer is Macbook 2021 or Macbook 2020 with M1 chip (M1, M1 pro, M1 Max) You have to go to Option A because the Virtual Machine File only works on X86 architecture.

Question 0.1:

- Include a screenshot of your terminal when you run the following command: `su seed`

[Your response goes here.]

Task 1. Prepare the network environment. (5 points)

Overview: Set up the network environment for Hosts A, B, and M.

Steps:

1. Switch to the "seed" user: `su seed`
2. Go to https://seedsecuritylabs.org/Labs_20.04/Networking/ARP_Attack/.
3. Download the Lab setup file "Labsetup.zip" into the SEED Lab (created in Task 0).
4. Read Sections 1 and 2 only of the instructions.

Question 1.1:

- Use `dockps` to list the IP addresses of Hosts A, B, and M. Paste your screenshot below. Make sure to include your input (i.e., the `dockps` command) and the output — not just for this question but for all questions in this lab.

[Your response goes here.]

Question 1.2:

- Use `docksh` to access Host A's shell. Ping Host B from A's shell. Do not kill the ping process yet.
- Open a new window. Access Host B's shell. Run tcpdump for about five seconds. Paste the screenshot below.
- Go back to A's shell where A is pinging B. Kill the ping after about 5 seconds. Show Host A's ARP table with `arp -n`. Paste the screenshot below.

[Your response goes here.]

Question 1.3:

- Use `docksh` to access Host M's shell. Do not ping any hosts from M. Show M's ARP table. Paste the screenshot below.
- Compare M's ARP table with A's ARP table (Question 1.2). Explain the similarities and/or differences.

[Your response goes here.]

Task 2. Intercept A's packets from M. (10 points)

Overview: Let M be the adversary who intercepts all packets from A to B.

Steps:

1. Go to Host B's shell. Start a web server: `cd /; python3 -m http.server`

2. Go to Host A's shell. Visit B's web server: `curl http://10.9.0.6:8000`
3. Go to Host M's shell. Intercept the communication between A and B with the `arpspoof` command.
4. Use `tcpdump -A` to view the packet payload as observed by M.
5. Repeat Steps 1 and 2.
6. Observe the output of the tcpdump process.

Question 2.1:

- Include a screenshot of Host B's HTTP response (i.e., payload), along with the corresponding packet headers from M's perspective.
- Why do you see duplicated packet contents in Step 6?

[Your response goes here.]

Task 3. Implement ARP spoofing in Python (10 points)

Overview: Instead of using Linux's `arpspoof` tool, you could implement it in Python using the "scapy" package.

Steps:

1. (Google it.)
2. (Make sure to save the code somewhere on your computer, but not in SEED Labs. Once you shut down a container, your files are gone forever.)

Question 3.1:

- Paste your code below.

Question 3.2:

- Repeat Task 2, replacing Step 2's `arpspoof` command with your Python code above. Include a screenshot of Host B's HTTP response (i.e., payload), along with the corresponding packet headers from M's perspective.

Bonus Question (3 points):

Think of a good quiz question for the material covered in Lecture 3, Lecture 4, and Lecture 5.