Lab-2: ARP Attack

Task 0: Setting up SEED labs

Overview: Set up the SEED Lab environment

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 Intel macOS. If you run the latest macOS on the M1 chip, you must choose Option A.

If your computer cannot run the VMs, your total cost will not exceed $30 for this semester if you use DigitalOcean(approximately $10/ month).

If you're a new GitHub user, you may be qualified for free $100 DigitalOcean credits. See this link.

Steps to prepare network environment:

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.

Note:

1. Explain and attach the screenshots for all tasks performed (not required for Task 0).
2. Attach the code snippet and explain wherever necessary. Simply attaching code without any explanation will not earn many points.

Task 1: ARP Cache Poisoning (20 points)

- Follow the steps in Section 3 from- https://seedsecuritylabs.org/Labs_20.04/Files/ARP_Attack/ARP_Attack.pdf

- **Task 1.A (using ARP request)**. (6 points)
  On host M, construct an ARP request packet to map B's IP address to M's MAC address. Send the packet to A and check whether the attack is successful or not.

- **Task 1.B (using ARP reply)** (7 points)

On host M, construct an ARP reply packet to map B's IP address to M's MAC address. Send the packet to A and check whether the attack is successful or not. Try the attack under the following two scenarios, and report the results of your attack:
– Scenario 1: B's IP is already in A's cache.
– Scenario 2: B's IP is not in A's cache. You can use the command "arp -d a.b.c.d" to remove the ARP cache entry for the IP address a.b.c.d.

- **Task 1.C (using ARP gratuitous message)** (7 points)
  On host M, construct an ARP gratuitous packet, and use it to map B's IP address to M's MAC address. Please launch the attack under the same two scenarios as those described in Task 1.B. ARP gratuitous packet is a special ARP request packet. It is used when a host machine needs to update outdated information on all the other machine's ARP cache.

Task 2: MITM Attack on Telnet using ARP Cache Poisoning

(30 points)

NOTE: (Make sure to save the code somewhere on your computer, but not in SEED Labs. Once you shut down a container, your files will be deleted.)

Hosts A and B are communicating using Telnet, and Host M wants to intercept their communication, so it can make changes to the data sent between A and B. The setup is depicted in Figure 2. We have already created an account called "seed" inside the container, the password is "dees". You can telnet into this account.

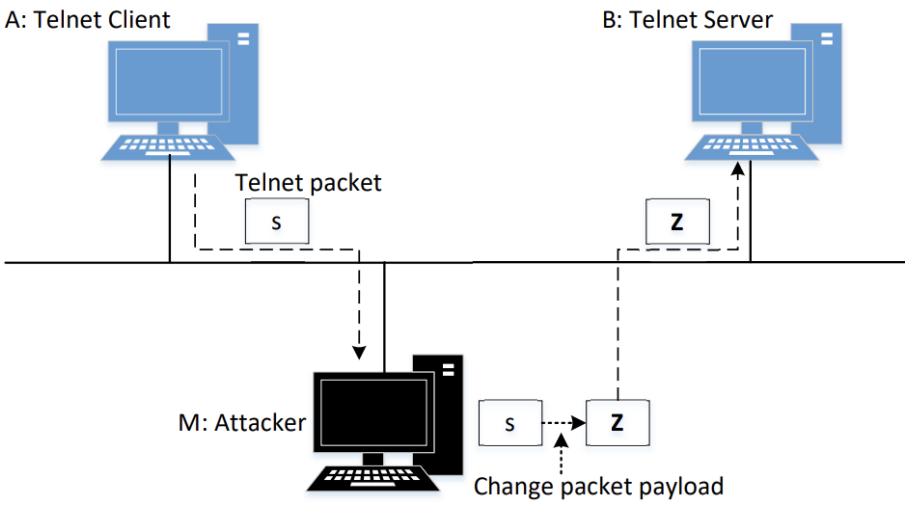

Figure 2: Man-In-The-Middle Attack against telnet

- **Task 2.1** (Launch the ARP cache poisoning attack) (6 points)
- **Task 2.2** (Testing) (6 points)

- **Task 2.3** (Turn on IP forwarding) (6 points)
- **Task 2.4** (Launch the MITM attack) (12 points)

Follow the steps in Section 4 to complete the above tasks:
https://seedsecuritylabs.org/Labs_20.04/Files/ARP_Attack/ARP_Attack.pdf

Task 3: MITM Attack on Netcat using ARP Cache Poisoning (30 points)

This task is similar to Task 2, except that Hosts A and B are communicating using netcat, instead of telnet. Host M wants to intercept their communication, so it can make changes to the data sent between A and B.

Follow the steps in Section 5 from:
https://seedsecuritylabs.org/Labs_20.04/Files/ARP_Attack/ARP_Attack.pdf

Task 4: Write-Up (20 points)

Provide a write-up explaining what you learned at a high level about the ARP attacks. Provide an explanation for the observations that are interesting or surprising. Mention any challenges that you faced in the lab.