CS 449 Assignment 4

Release Nov 20th, 2023; Due Dec 11th, 2023

Instructions

This assignment is due on Dec 11th 23:59:59 EST. The whole assignment has been tested on a 64-bit Ubuntu 22.04 virtual machine. Using a Linux virtual machine to set up the environments and complete this assignment is recommended. If you have trouble running a Linux virtual machine on your own computer, you can go to the UNIX/PC Lab (M-3-731), Web Lab (M-3-732), or IT Lab (M-3-730) of our department where you can find computers pre-installed with virtualization software, including VMware Workstation Pro 17 and Oracle VirtualBox 7.

Your submissions will have two or three folders, depending on whether you complete the optional extra credit question. Place the files in the appropriate folders, using the exact names and conventions specified in the question text. Please zip these folders without encryption, rename the zip file as CS449A4.first_name.last_name.studentID.zip, and submit it on Blackboard.

Question 1 ARP Spoofing (20 points)

Given an IP address, Address Resolution Protocol (ARP) is a communication protocol used for discovering the corresponding MAC address. The ARP protocol is a simple protocol which does not contain any security mechanism. ARP Spoofing attack is a common attack against the ARP protocol where an attacker sends spoofed ARP messages to a local area network. Using such an attack, attackers can fool the victim into accepting forged IP-to-MAC mappings. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic. Often the attack is used as an opening for other attacks, such as denial of service, man-in-the-middle, or session hijacking attacks.

In this question, your goal is to launch an ARP spoofing attack against two machines in a network so that you can intercept any packets exchanged between them. You will use the `arpspoof` tool to launch the ARP spoofing attack.

Environment Setup

(a). (*You can skip this step if you have already done it in Assignment 2.*) Install `docker` on your computer. If you use Ubuntu, please refer to `https://docs.docker.com/engine/install/ubuntu/` for installation instructions, or visit `https://docs.docker.com/engine/install/` for instructions on installing `docker` on other operating systems.

(b). (*Optional*) Manage `docker` as a non-root user. Follow the instructions on `https://docs.docker.com/engine/install/linux-postinstall/#manage-docker-as-a-non-root-user` so that you can manage `docker` as a non-root user.

(c). The setup files for the evironment are given under the folder `LabsetupARP`. Go to that directory, and run

```
docker compose build
```

to build the container image, and then run

```
docker compose up
```

to start the containers. This will create the environment as shown in Figure 1. There are three hosts in the `10.9.0.0/24` network. Host A has the IP address of `10.9.0.5`, Host B has the IP address of `10.9.0.6`, and Host M, which is the attacking machine, has the IP address of `10.9.0.105`.

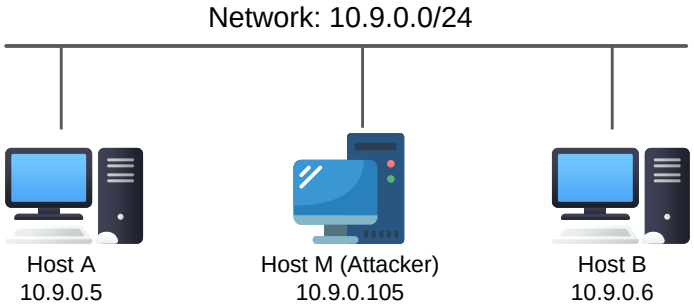

Figure 1: Environment created using Docker containers.

After starting the containers, you can leave the current terminal running in the background and start new terminals for the remaining tasks.

You can later use the following to shut down all contains after finishing this problem:

```
docker compose down
```

(d). Start a new terminal and run the following command to list all running containers:

```
docker ps
```

Running the above command will list the ID of each container. Identify the ID of the attacker's host and run the following command to start a root shell on it where `CONTAINER_ID` is the ID of the attacker's host:

```
docker exec -it CONTAINER_ID /bin/bash
```

(e). Inside the root shell of the attacker's container, run the following commands to install `arpspoof`:

```
apt-get update
apt-get install dsniff
```

You can check the manual of `arpspoof` at `https://man.archlinux.org/man/arpspoof.8.en`.

Task

Your task in this assignment is to launch an ARP spoofing attacker from the attacker's host using `arpspoof`. Specifically, you want to fool Host A (`10.9.0.5`) into believing the MAC address of Host B (`10.9.0.6`) is the MAC address of Attcker's Host (`10.9.0.105`). You also want to fool Host B (`10.9.0.6`) into believing the MAC address of Host A (`10.9.0.5`) is the MAC address of Attcker's Host (`10.9.0.105`). Since IP forward has been turned on in the attacker's host (if not, use the following command to manually turn it on),

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

the attacker's host will now act as a man-in-the-middle to intercept and forward any packets exchanged between Host A and Host B.

During the attack, you can start root shells on each host and use the following command to check their MAC address:

```
ifconfig
```

You can start root shells on Host A and B and then use the following command to check the ARP table on host A and host B:

```
arp -n
```

To remove a IP address, e.g., xxxx.xxxx.xxxx.xxxx, and its mapped MAC address from the ARP table, you can use:

```
arp -d xxxx.xxxx.xxxx.xxxx
```

To make sure you launch the attack successfully, run `tcpdump` on the attacker's machine to show all packets passing through attacker's machine:

```
tcpdump -i eth0 -n
```

If the attack is successful, when executing

```
ping 10.9.0.6
```

on Host A, `tcpdump` running on the attacker's host will display that all ICMP packets exchanged between Host A and Host B will be intercepted and forwarded by the attacker.

Submission Instructions

Write a report including the following materials:

- Screenshots of launching ARP spoofing attacks using `arpspoof`, including the constructed attacking command using `arpspoof`.
- Screenshot of ARP table on Host A, showing that the MAC address mapped to `10.9.0.6` is the MAC address of the attacker's host.
- Screenshot of ARP table on Host B, showing that the MAC address mapped to `10.9.0.5` is the MAC address of the attacker's host.
- Screenshots of running `tcpdump` on attacker's machine while executing `ping 10.9.0.6` on Host A, showing that the `ping request` and `ping reply` exchanged between Host A and Host B are intercepted and forwarded by the attacker's host.

The report should be in PDF format and named as Q1.pdf. It should be placed under the Q1 folder of the submission.

Optional Extra Credit Question

This part is **optional**. If you complete this part correctly, you will receive **5 bonus points** towards your **final score of the whole class**. There will be **no partial points** for this extra credit question, i.e., you either get 5 points if you submit the correct answer or 0 point if you submit the wrong answer.

Your task is to write a `C` or `Python` program yourself to launch the ARP spoofing attack on the attacker's host **instead of** using `arpspoof`. This program would construct the spoofed ARP replies and send them to Host A and Host B. The attacking goal is the same as Question 1.

Hint: if using `Python`, you can use the `Scapy` package to help you construct ARP packets.

Submission: Write a report including the following materials:

- Screenshots of launching ARP spoofing attacks using the program written by yourself on the attacker's host. Explain the major steps in your program.
- Screenshot of ARP table on Host A, showing that the MAC address mapped to `10.9.0.6` is the MAC address of the attacker's host.
- Screenshot of ARP table on Host B, showing that the MAC address mapped to `10.9.0.5` is the MAC address of the attacker's host.
- Screenshots of running `tcpdump` on attacker's machine while executing `ping 10.9.0.6` on Host A, showing that the `ping request` and `ping reply` exchanged between Host A and Host B are intercepted and forwarded by the attacker's host.

The report should be in PDF format and named as Q1Bonus.pdf. In addition, you need to **submit the source code of your program** and named it as Q1Bonus.c or Q1Bonus.py. Place the report and the source code under the Q1Bonus folder of the submission.

Question 2 DoS Attack (20 points)

Denial of Service (DOS) attack is a very simple technique to deny access to services (that's why it is called "denial of service" attack). This attack consists of overloading the target with oversized packets, or a big quantity of them. While this attack is very easy to execute, it does not compromise the information or privacy of the target, i.e., it is not a penetrative attack and only aims to prevent access to the target. By sending a large number of packets that the target can not handle, attackers can prevent the server from serving legitimate users.

`hping` (current version is `hping3`) is a command-line oriented TCP/IP packet assembler/analyzer. You can find the manual of `hping3` at `https://www.kali.org/tools/hping3/`. The interface is inspired by the `ping` Unix command, but `hping3` is a more powerful tool compared with `ping`. It supports TCP, UDP, ICMP, and RAW-IP protocols, has a traceroute mode, the ability to send files between a covered channel, and many other features. `hping3` allows you to send manipulated packets and control the size, quantity, and fragmentation of packets in order to overload the target and bypass or attack firewalls. The `--flood` option in `hping3` will let `hping3` shoot at discretion, replies will be ignored (that's why replies won't be shown), and packets will be sent as fast as possible. In this question, you will enumerate several DoS attacks using `hping3` with the `--flood` option.

Environment Setup

(a). You will continue to use the environment that has been set up in Question 1.

(b). Inside the root shell of the attacker's container, run the following commands to install `hping3`:

```
apt-get update
apt-get install hping3
```

You can check the manual of `hping3` at `https://www.kali.org/tools/hping3/`.

Task

1. Land Flood Attack: deploy land flood attack using `hping3` from Host M (attacker's host `10.9.0.105`) to Host A (`10.9.0.5`). Attack requirements:

- TCP header: source port = 80, destination port = 80, TCP SYN Flag = 1.
- IP Header: source IP = Host A's IP address, destination IP = Host A's IP address.

Run `tcpdump` on Host A to show the captured attacking traffic.

2. SYN Flood Attack: deploy SYN flood attack using `hping3` from Host M (attacker's host `10.9.0.105`) to Host A (`10.9.0.5`). Attack requirements:

- TCP header: source port = any, destination port = 80, TCP SYN Flag = 1.
- IP Header: source IP = random, destination IP = Host A's IP address.

Run `tcpdump` on Host A to show the captured attacking traffic.

3. Smurf Flood Attack: deploy Smurf flood attack using `hping3` from Host M (attacker's host `10.9.0.105`). The target of this Smurf flood attack is Host A (`10.9.0.5`). Attack requirements:

- ICMP header: type = 8 (echo request), code = 0.
- IP Header: source IP = Host A's IP address., destination IP = broadcast IP address.

Run `tcpdump` on Host A to show the captured attacking traffic.

Note: You should run the following command on Host B so that it would reply to ICMP echo requests sent to a broadcasting address:

```
echo 0 > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
```

Submission Instructions

Write a report including the following materials:

- Screenshots of launching the above 3 DoS attacks from the attacker's machine, including the constructed attacking commands using `hping3`.
- Screenshots of running `tcpdump` on Host A while launching the above 3 DoS attacks, showing the DoS attacking packets received by Host A.

The report should be in PDF format and named as Q2.pdf. It should be placed under the Q2 folder of the submission.