CompSci 657/790 Topics: Introduction to Cybersecurity
HW #4 (50 points)
2024 Spring

Due: April 5, 2024 8:30pm

1 Overview

In this homework, we will gain first-hand experience on network attacks. In the lecture on Week 8, we demoed how to use the network tools of *tcpdump* and *hping3* to conduct a Denial of Service attack on a victim host. This homework is for learning how to use these tools in the created network with three host machines.

1.1 Hands-on Lab Environment Setup in your local computer

- Download the **docker-compose-hw4.yml** on your local computer, and change the file name to be **docker-compose.yml**.
- Download the docker image:

  docker pull introsecuwm/homework4
- In the same folder of **docker-compose.yml** on your local computer, run the command

  docker-compose up
- Open the other three terminals and run the command to access the hostA and hostB, and the attacker.

  docker exec -it hostA-192.168.0.5 /bin/bash

  docker exec -it hostB-192.168.0.6 /bin/bash

  docker exec -it attacker-192.168.0.7 /bin/bash
- sudo password: uwm24s

##################################
If your local computer cannot support the docker env for homework 3, please follow these steps to use the assigned virtual machine.

- save the given .pem file on your local computer.
- login to the assigned virtual machine by following the instructions sent by TA.
- In the virtual machine, go to folder **homework4**, and run the command

  docker-compose up
- Open the other three terminals, follow the same previous steps to login the virtual machine, and run the command to access the hostA and hostB, and the attacker.

  docker exec -it hostA-192.168.0.5 /bin/bash

  docker exec -it hostB-192.168.0.6 /bin/bash

  docker exec -it attacker-192.168.0.7 /bin/bash
- sudo password: uwm24s

##################################

2 Task 1: Conducting ACK flooding attack and capture the network traffic data

By using the knowledge we discussed in the live demo of SYN flooding attack on week 8 to conduct ACK flooding attacks on hostA.

What you need to do:

Step 1. use the network tool of *hping3* on the attacker to conduct ACK flooding attack to hostA with a random source IP, and a fixed source IP (10.0.9.4), respectively.

Step 2. use the network tool of *tcpdump* to monitor and record this ACK flooding attack as an ack_attack.pcap on hostA.

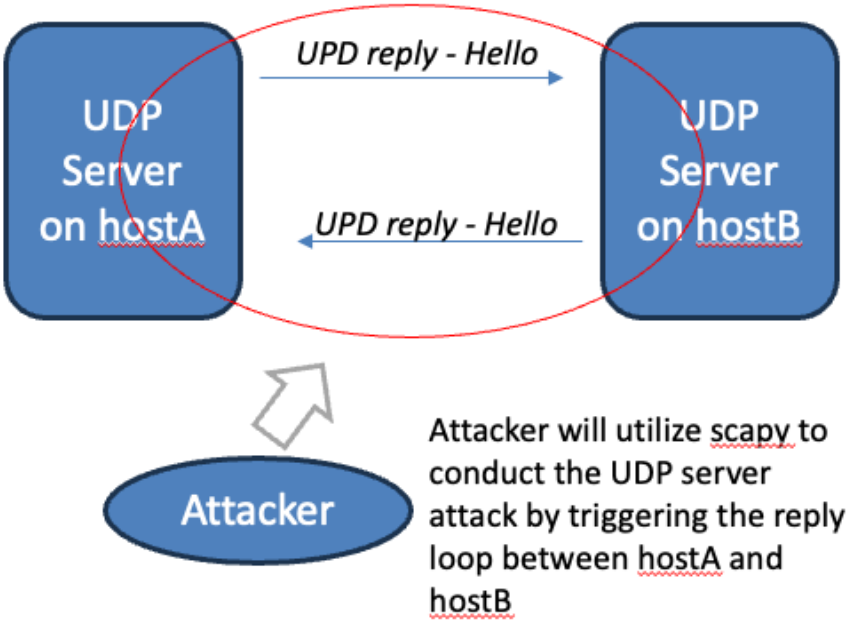
Step 3. log in with your GitHub account on hostA, and push the ack_attack.pcap file to your GitHub repository.
* Please limit the traffic recording to around 1 minute to ensure a good size for the git push.

Step 4. download the ack_attack.pcap from your GitHub repository to your local computer and use Wireshark to analyze this pcap file and identify the attack traffic flows.

Make screen prints for each step, and explain your ACK flooding attack pattern with the associated wireshark traffic analysis result in the report to show your work.

3 Task 2: UDP Server Attack

In homework#3, we developed a UDP server, and in the lecture of week 8, we analyzed the behavior of the UDP Server. The attacker on the virtual machine of *attacker-192.168.0.7* knows that the given UDP server will respond to each received message with a response message on both hostA and hostB. Now, attacker utilizes this feature of UPD server to conduct a UDP server attack on hostA and hostB, which results in UDP servers on both hostA and hostB sending a "UPD reply-Hello" message to each other and never ending this loop.



What you need to do:

Step 1. Exam how UDP server works on hostA and hostB, respectively.

```
nc -u 192.168.0.5 9090
nc -u 192.168.0.6 9090
```

Step 2. Review the sample code of sniffing & spoofing with Scapy on Week7 lecture notes. Create a Python file "udp_attacker.py" on the virtual machine of attacker. In this python file by using the scapy to:

1. create packet with *ip, udp, data*, and
2. send the created packet

Step 3. Execute "udp_attacker.py" to conduct UDP server attack.

```
sudo python3 udp_attacker.py
```

Step 4. Make screen prints for "udp_attacker.py" and the UDP message reply loop. Explain how this attack works in your design.

4 Submission

Submit the following item on Canvas:

- report.pdf