CSSE 490 -- Network Security

Rose-Hulman Institute of Technology

Lab 1: Introduction to Networking

Learning Objectives

At the end of this lab, you should be able to:

- Identify the data link and network layer protocols.
- Capture traffic on a network using `tcpdump` and/or `scapy`.
- Examine network packets captured on the wire.
- Craft and send network packets to achieve a certain goal.

Name: _____

Question	Points	Score
Question 1	10	
Question 2	5	
Question 3	10	
Question 4	15	
Question 5	5	
Question 6	15	
Question 7	5	
Question 8	5	
Question 9	10	
Question 10	5	
Question 11	10	
Question 12	15	
Question 13	10	
Question 14	15	
Question 15	15	
Question 16	30	
Question 17	0	
Question 18	0	
Question 19	0	
Total:	180	

1 Prelude

Question 1. (10 points) My `CSSE332` morning section struggles to stay awake. Please write down something interesting or a joke that I can share with them to wake them up.

2 The ARP protocol

The questions below refer to section 1 of the lab documentation, specifically to the *Address Resolution Protocol* (ARP) section.

2.1 Examining packet captures

Question 2. (5 points) How many protocols have you captured? List them all (there should be at least three).

Question 3. (10 points) Before we see any `ping` packets, there are two packets that show up in the capture. In your own words, describe what you think these packets are for.

2.2 Digging into ARP

Question 4. (15 points) Based on your observations in this section, what is the purpose of the ARP protocol?

Question 5. (5 points) Where are ARP mappings stored on a machine?

2.3 Workings of ARP

Question 6. (15 points) In your own words, describe how the ARP protocol operates. List the steps involved in obtaining a mapping from a given `IPv4` address to a corresponding `MAC` address.

Question 7. (5 points) On average, how often is an ARP request refreshed?

Question 8. (5 points) Consider the following scenario: `hostA` is pinging `hostB`, but all of a sudden, `hostB` dies. In terms of ARP, what do you think `hostA` will do after it asks `hostB` directly for its `MAC` address and it doesn't receive a response?

3 The ICMP protocol

The questions below refer to the `ICMP` section of the lab documentation.

3.1 `ping`

Question 9. (10 points) Based on your observations, draw a simple structure of an ICMP packet, stacking together the different headers that must be present in the packet so that communication can happen successfully.

3.2 Digging into an `ICMP` packet

Question 10. (5 points) Describe the setup of your experiment and the commands you used to launch it.

Question 11. (10 points) Examine the `ICMP` packet headers, based on your observations, how can `hostA` match `Echo (ping) reply` packets received from `hostB` to corresponding `Echo (ping) request` packets?

4 Implementation

4.1 `traceroute`

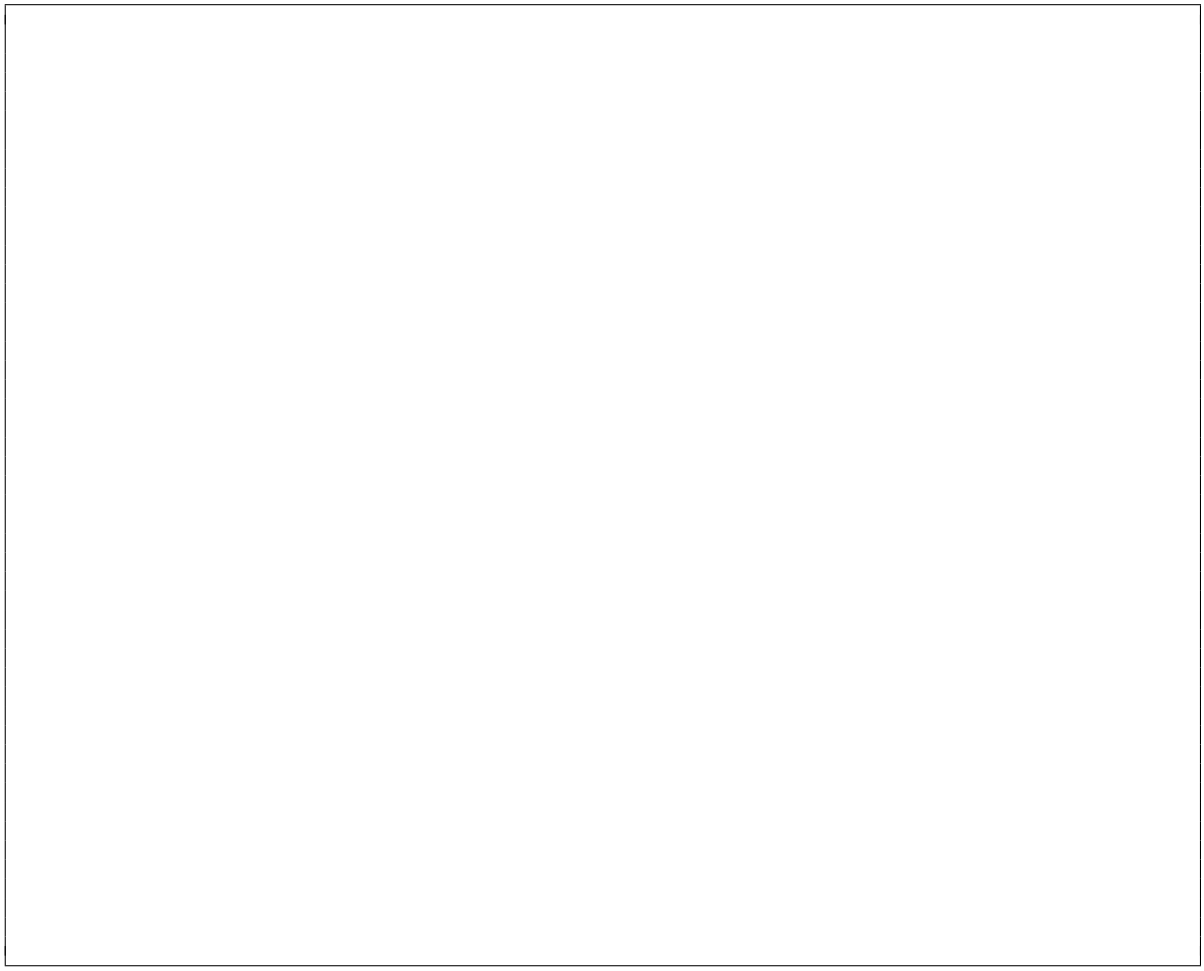
Question 12. (15 points) Describe an experiment in which you can capture packets to examine `traceroute` traffic and reverse engineer its operation.

Question 13. (10 points) Based on the outcomes of your experiment, describe how `traceoute` determines the hops on the path between `hostA` and `1.1.1.1`

Question 14. (15 points) Implement `traceroute` using your chose programming language.

4.2 The `ghost` machine

Question 15. (15 points) Describe your exploit using text and/or diagrams. Make sure to list all the steps that an attacker should do in order to trick `hostA`.



Question 16. (30 points) Implement your exploit using your chosen programming language.

5 Wrap-up

Question 17. (0 points) In your own words, please write a quick summary of what you have learned in this lab.

Question 18. (0 points) How much time did it take you to complete this lab?

This page is intentionally left blank ...

Question 19. (0 points) Do you have any feedback about this lab? (If you'd like to leave an anonymous feedback, feel free to detach this page and slide it under my door).