Lab and Homework 2
Scanning

As with most assignments, pending on time, we will start working on these in class as a lab, discuss any possible questions. You will need to submit these on Oaks by the due dates.

Background

What are TCP and UDP?

In order to understand this exercise, you should be familiar with the 3-way handshake for TCP. You should also know something about ICMP and UDP. This exercise is not designed to teach you all the details of those protocols, but it will teach you why some of those details are important. You can read about them in any standard networking textbook.

Laboratory Assignment

1. The first goal is to locate hosts on the target network using a TCP scan. What flags do you set to do this? Use tcpdump or tshark to list the SYN and SYN-ACK packets. What ports are scanned? Is there a pattern? How many packets are sent? What is the scan time?

2. How many IP addresses are there in the target network? How would you divide up the address space into two equal parts? Divide the recon task into 2 parts and have a different person scan each part.

3. Try a ping scan. What flags did you use? Do the same hosts show up? How many ports are scanned? What is the scan time? 5

4. Try a UDP scan. What flags did you use? Do the same hosts show up? How many ports are scanned? What is the scan time?

5. Make your scan faster. What flags did you use?

6. Make your scan more stealthy. What flags did you use?

7. How can you increase the speed of your scan?

Diagram of Recon I network

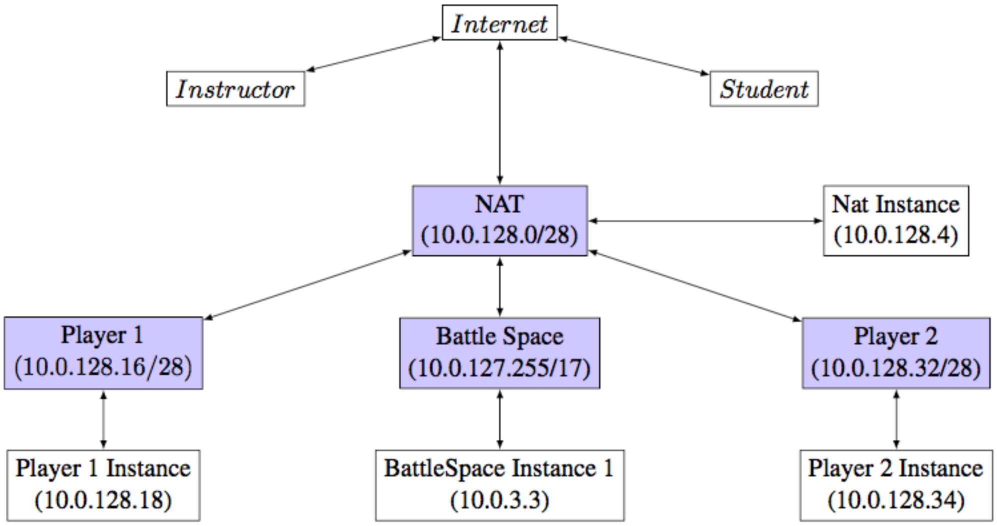

Figure 1: Conceptual diagram of the Recon I game. Note subnets are blue, and IP addresses are just as an example.

Source: http://blogs.evergreen.edu/edurange/