Team Exercise #2
ICMP Reconnaissance Techniques
Exercise: March 2, 2005
Report Due Date: March 9, 2005

Before the Exercise

You have 30 minutes to set up and configure one or more machines for your team. You must start at least one machine, but you may start as many additional machines as you wish. You may choose any operating system or combination of operating systems.

You must complete a Machine Information Sheet for every machine that you start.

You should configure your machines so that they collect enough information to allow you to complete the exercise.

During the Exercise

You are to determine the IP address of every active machine in the room on the 10.0.1.* network. [This network holds only virtual machines; the host machines have been configured on a different subnet.]

You are to use ICMP techniques for your reconnaissance. You are not allowed to send TCP or UDP packets for this purpose. With this restriction, you may use any and all techniques to evade detection.

During the exercise, you need to complete your command summary sheets.

After the Exercise

Based on your work, answer the following questions:

- List all of the active machines in the room.
- If possible, determine the operating system for each machine.
- Which machines scanned your network.

After the exercise, you will write a final report that contains your findings.