Team Exercise #2

Reconnaissance

Exercise: March 15, 2006

Report Due Date: March 29, 2006

Before the Exercise

You are to set up a collection of machines, including

- at least 2 SSH servers,
- at least 2 FTP servers,
- at least one Windows Shared folder,
- at least one telnet server, and
- at least two web servers.
    - at least one with a password protected directory
    - at least one with an SSL protected portion

- Each machine, with the exception of the web server, needs two or more enabled, non-root accounts. All account and password information must be given to the instructor by the end of class on Monday, March 13.
- The FTP server and the Windows Shared folder need to have files accessible for download.
- For these machines, you may use any operating system, and any available version of the service.
- Each machine must have an accurate NETBIOS name or hostname. Each team must choose a team "theme", and all of their machine names must be related to that theme.
- All machines started by the team must have accurate names- not just the ones providing services described above!
- 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 to you complete the exercise.

During the Exercise

Try to complete a machine information sheet for all of the other machines in the room. In particular, for each active machine, try to determine

- The IP address,
- The hosting team,
- The OS, and
- The types and versions of all available services.

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

Try to cover your tracks as best as you can. The use of cunning and guile are encouraged.

After the Exercise

Based on your work, you will write a final report. This report should contain the results of your scans- including machine information sheets for all of the active guests in the room.

More importantly, the report try to ascertain who scanned and/or probed your network, and what they accomplished. To answer these questions, you will need to set up a good system of logging and even sniffing.