Team Exercise #1

Logging

Exercise: February 16, 2005

Report Due Date: February 23, 2005

Team #4- Basketball

Before the Exercise

Each machine must be configured as per Assignment #2:

- Machine 1 (Bulls) Windows 2000, IIS Web server.
- Machine 2 (Pistons) Windows 2000 SP2.
- Machine 3 (Lakers) RH 7.3 Workstation, SSH server.
- Machine 4 (Heat) Windows 2000. IIS FTP server.
- Machine 5 (Spurs) RH 7.3 Server, SSH Server, Apache Web Server
- Machine 6 (Kings) RH 7.3 Workstation, SSH Server
  - *Note that this has been changed to 7.3 from 7.0. You may still use 7.0 if you are able to make it work.*
- Each machine must have its correct service set loaded, users and accounts configured as per Assignment #2, and have its logging configured as per Assignment #3. *The importance of good logging can not be underestimated in this exercise!*

New Features

- Each web server must have a default web page that displays correctly.
- On the FTP server, create a text file with a message of your choice. It should be downloadable by anonymous FTP.
- On Machine 2, create two shared directories. One should be accessible to any authenticated user, and one should be accessible only to user "Wallace". Create two more text files, with messages of your choice. Place one in the share open to all authenticated users, and the second open only to "Wallace".
- In addition, you may start as many additional machines as you wish, or any type, and for whatever purpose.
- For each additional machine assign an appropriate name; the names and IP addresses of each machine will be given to the class.

- For each machine that is started, a Machine Information Sheet must be completed.

All of these tasks must be completed by 5:45 on the day of the exercise.

During the Exercise

Known information:

Machine: Braves
User: Smoltz
Password: nvIdhA2Y

Machine: Colts
User: Manning
Password: OKee3sWz

Machine: Twins
User: Jones
Password: 23aRShZV

Machine: Jets
User: Martin
Password: xQxlGRtl

Machine: Astros
User 1: Bagwell
Password: 4rWk39n2

Machine: Eagles
User: Westbrook
Password: WdGanaYb

For each machine on team #1 (Football) and Team #2 (Baseball)

- If the machine is running a web server, describe the home page.
- If the machine is running an ftp server
  - If it is serving files anonymously, describe the contents of the file.
  - If requires authentication, and you can authenticate, then download the file and describe the contents.
- If the machine is running an ssh server, and you can authenticate, then do so.
- If the machine is running as a SMB file server,
  - Determine if possible all of the shares.
  - Attempt to download each shared file.

In your final report, you will give neat and concise answers to all of these questions.

While the exercise is running, you may use any and all means to prevent your activities from appearing in the logs of the target machine. Creativity in this regard is not only permitted, but encouraged.

IMPORTANT!
For each command you execute, you must complete the corresponding Command Summary Form. Failure to do so will result in a substantial grade penalty.

After the Exercise

- Who visited the web page on Arsenal?
- Who accessed the files shared by Liverpool?
- Who logged on to the SSH server on Blackburn?
- Who downloaded files from Manchester?
- Who used SSH to log on to Everton?
- Who visited the web page on Everton?
- Who used SSH to log on to Newcastle United?

In your final report, you will give complete and concise answers to each of these questions.

The final report will be neat, organized, and well-written. It will contain:

- A copy of the Machine Information Sheet for each of your machines.
- A copy of each of your Command Summary Forms for each command executed.
- The results of your reconnaissance as described above.
- The analysis of your logs, described above.