Team Exercise #1

Logging

Exercise: February 11, 2009

Report Due Date: February 18, 2009

Network Setup

(1) Create a network that contains the following

(a) At least three Windows based machines

(b) At least three Linux based machines

(c) One central logging server (any OS)

(d) Additional machines may be provided by the instructor on February 9.

(e) Any additional machines that you wish. [Install disks are available for a wide range of OS's- just ask.]

The machines must each have a unique name associated with your team, and they must be present on the class network.

Secure these machines in whatever fashion you see fit.

(2) Each Windows machine from group (a) is to have three different users. These can be local users, or, if you want to set up and maintain a domain controller, then they can be domain users. Record the machine name, OS, account name, and passwords on the provided sheet(s).

Each Windows machine from group (a) must contain a network share that can be read by any authenticated user. In each shared directory, create a plain text file with a message of your choice.

Each Windows machine from group (a) must contain a network share that can be read by only one particular user. In each shared directory create a second plain text file with a different message.

(3) Each Linux machine from group (b) should have three different users. Record the machine name, OS, account name, and passwords on the provided sheet(s).

Each Linux from group (b) machine should have a functioning SSH server. In the home directory of each user, create a plain text file with a message of your choice.

(4) The logging server should record the logs from all of the machines in your network. You can set up more than one logging server if you wish, but one machine must server as your central logger.

Required Information

Before the end of class on February 9, the Password Sheet must be complete and turned in. Failure to do so will result in a grade penalty.

At the start of the exercise on February 11, a Machine Information Sheet must be completed and turned in for each machine in your network.

Exercise Instructions

You may not access machines from other teams until after the start of the exercise.

At the start of the exercise, you will be provided authentication credentials to machines from other networks.

For each machine for which you have authentication credentials, do the following:

- Determine the OS
- If it is a Linux machine, use your credentials to log in to the SSH server. Check the home directory of your user to find the message file. Record the message.
- If it is a Windows XP machine, use your credentials to access the shared directory. Locate the message file, and record the message.

For each machine for which you do not have authentication credentials, attempt to do the same thing.

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

For each machine in your network, answer the following questions:

- Who logged on to your SSH servers?
- Who accessed your shared files?
- Which teams have read your message files?

Describe how well your logging server functioned. Were there any significant issues with is function?

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.
- A copy of the messages for each of your machines.
- The results of your reconnaissance as described above.
- The analysis of your logs, described above.

Grading

Your report will be graded out of 25 points. Points will be awarded for the following:

5 points for the overall written quality of your report.
5 points for the actions you took to prepare your network.
5 points for the attack activities you took during the exercise
10 points for your analysis of what took place on your own network.

Accurate record keeping is essential for each team.

This includes accurate Machine Information Sheets, and complete Command Summary Forms.

Failure to submit accurate records will result in ***SUBSTANTIAL GRADE PENALTIES***.

You have been warned.