Team Exercise #1
Logging

Exercise: March 3, 2010
Report Due Date: March 10, 2010

1 Network Setup

Create a network that contains the following:

1. A Windows domain with a primary domain controller and as many backup domain controllers (if any) that you wish.
2. At least three Windows based workstations that are members of the domain.
3. At least three Linux based machines.
4. A team DNS Server. (This may be the PDC or a different machine, at your discretion).
5. One central logging server (any OS)
6. Additional machines may be provided by the instructor on March 1 or 3.
7. Any additional machines that you wish. [Install disks are available for a wide range of OS's- just ask.]

Secure these machines in whatever fashion you see fit.

1.1 Windows domain and machines

Each Windows machine from group (2) is to have at least three different users. These can be local users or domain users.

Each Windows machine from group (2) 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 (2) 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.

1.2 Linux machines

Each Linux machine from group (3) should have three different users.

Each Linux from group (3) 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.

1.3 DNS server

Each machine on your team must have a host name that your nameserver can resolve.

You must select a single DNS suffix for all of the machines on your team so that each machine has a FQDN of the form hostname.suffix. For example, if your team suffix is "cosc.tu" and your machine name is "dilbert" then your FQDN is "dilbert.cosc.tu" while the machine "wally" would have FQDN "wally.cosc.tu." You must use the same suffix for all of the machines on your team.

Your DNS server should provide name resolution for all of the machines on your team. It should forward all requests that it cannot resolve to the exercise name server, at 10.0.2.2

1.4 Logging server

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.

2 Required Information

Before the end of class on March 1, the Exercise 1 Network Required Elements must be completed and returned electronically.

At the start of the exercise on March 3, a Machine Information Sheet must be completed and turned in for each machine in your network.

3 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 running an SSH server, use your credentials to log in. Check the home directory of your user to find the message file. Record the message.
- If it is sharing a directory, use your credentials to access it. 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.

EVERY COMMAND MUST BE LOGGED using a scheme of your own choosing. Failure to do so will result in a significant grade penalty.

4 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 its function?
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 complete log 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.

The report must also specify the responsibilities and activities of each team member in reasonable detail.

5 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 reconnaissance and 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- up to half of the final grade.

You have been warned.

The report of the responsibilities and activities of each team member will be used together with the report grade to assign the final grade for each student. If, in the judgment of the instructor different team members made substantially different contributions, then members of the team may be assigned different grades.

5.1 Extra Credit

Extra credit may be awarded to teams who go beyond the minimal requirements for the project:

- (+1 pt) Set up a functioning time server for the group, and have each machine use that time server.
- (+0.5 pts) Set up the domain so that each user receives an individual shared drive (H:) from a file server.
- (+1 pt) Add all of the linux machines to the windows domain.
- (+0.5 pts) Add a windows file share to the linux machines.
- (+2 pts) Set up a linux machine as a domain controller for your domain (backup or primary).