Team Exercise #2
The Web

Exercise: April 18, 2011
Report Due Date: April 25, 2011

1 Introduction

You have just been tasked with developing the computer network infrastructure for our new company. We are divided into roughly four groups- there are eight folks in our sales staff, six in our production group, four in our IT group (that includes you!), and of course, me- the CEO.

Below I have sketched out the network I would like you to develop, but remember that I am not a technical expert- so some of my ideas may be wrong. On the other hand, I am also your boss, and if you can't get the work done I will hire someone that can.

2 Network Setup

Create a network that contains the following:

1. A Windows domain. Our sales staff and production staff will be using the Windows domain for all of their day-to-day activities.
2. Being a startup, we do not yet have enough money to buy machines for everyone, but I want to see at least one machine for the sales staff and one for the production staff.
3. Our IT staff keeps telling me that linux systems are necessary for all of their development work- set up at least one for the IT staff. And since they also need to help manage the IT infrastructure, they better have access to the domain.
4. Both the sales staff and the production staff need to share data with one another. I would like the sales staff to have a shared drive where they can keep their common documents, and the same should be true of the production staff. You should also have a common share that everyone can access.
    - These shares should be pre-populated with documents. These can be whatever you want them to be, but your job is allowing the right people access to them and keeping them out of the hands of the wrong people.
5. As the CEO, I want access to all of these systems and file shares; I should also be able to access all of my files from whatever system I am using at the time.
6. We need an internet presence; in particular we need our own domain name.
7. We need to set up public facing web servers. Set up a server for the sales staff, one for the production staff, one for the IT staff, and one for the company as a whole.
    - These web sites should be prepopulated with documents, and should link one to another to form a coherent whole.
    - Each web server should also have a private side, accessible only to the CEO and to members of that team (or the entire company); this should be done securely.
8. We are considering moving some of these servers to remote locations in the future; thus you should be able to administer the entire network remotely.
9. As a start-up, most of our value is in our intellectual property. As such, I want a secure network, and I want to know who is on our system at any moment. You can do that, can't you?

3 Required Information

Before the end of class on April 11, each team must electronically send to the instructor a page that contains the following information:

- For each machine, specify the OS, the hostname, and the IP.
- Specify the name(s) of your domain(s), together with their full host names.

- For each non-root, non-administrator account on any of your hosts, specify the type of account [local, domain] and the password.
- For each file share, either specify the drive letter to which it maps (if it does) and provide explicit instructions on how it is to be accessed.
- For each system with remote access, provide explicit instructions on how to access the system,
- The IP address(es) of the DNS for your team, as well as the hostname for your DNS Server(s).

Some of this data will be provided other teams. You will be graded on its accuracy- if other teams cannot access a system / account / file share then you will receive a deduction in score.

At the start of the exercise on April 18, a Machine Information Sheet must be completed and turned in for each machine in your network.

4 Exercise Instructions

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

Each student must set up at least one web server for this exercise, and be responsible for its management.

Each student must also set up a fully functioning intrusion detection system that covers (at a minimum) the host on which they are running their web server.

At the start of the exercise, you will be provided authentication credentials to machines from other networks, as well as a list of services to verify. You will verify that all of the file shares function as indicated, you will check that the public web pages function correctly, and you will verify that the password protected web pages also function correctly.

Once you have verified that the services from other teams, you are free to engage in offensive activity.

You should also attempt to access any files or web pages, especially files for which you should not have access. Remember that in the real world simply reading a file that you are not allowed to read counts as a security breach- especially if that data is something sensitive. The same holds true for private documents hosted on our web servers.

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. Cunning is even better.

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

5 After the Exercise

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

- For systems requiring authentication- who logged in? When? Did they do so legitimately?
- For your web servers- who accessed your public pages? Who accessed your protected pages? Did any unauthorized user gain access to any of your private data?
- Were there any successful exploits of your system? Note- it is permissible (even encouraged) to use unpatched machines in this exercise that may end up being exploited by common tools like metasploit. The value of the exercise is learning how to detect an intrusion, rather than learning how to patch a machine.

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. Each team member must specify which web server(s) for which they were responsible and how they functioned. Each team member must also describe how they set up their intrusion detection system, including providing a copy of the snort.conf file that was used to tune the system.

6 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.