Goal: The goal of this lab is to have you apply the skills and tools learned over the course of the semester to evaluate the security of a simulated network.

Lab Scenario: After graduation you have been hired by a BuzzCo Security, a network security consulting firm. One of BuzzCo’s clients is Burdell University, and you have been assigned to evaluate the security of their network. Using knowledge gained in the previous 10 labs, as well as the reading assignments, take the guise of a white hat hacker and try to infiltrate the University network.

Your assignment is as follows:
There are several machines up on the 138.210.0.0/16 network (University). Using past labs and anything you can find on the internet, you are to map out the network to find these machines, determine what vulnerabilities, if any, are present, and then try to break into them. You will then write up a report summarizing your procedures and findings.

Some notes:

1) All of the machines are on the 138.210.0.0/16 network. DO NOT try and break into anything that is not on this network, especially anything on the 57.35.0.0/16 network.
2) Refer back to Lab 1 for helpful network mapping and vulnerability scanning tools
3) This is a live network. There is some traffic between the machines. However, remember that we are on a switched network, and you will not be able to just see this traffic floating by (hint: Lab 2…)
4) You are not required to break into any of the machines in order to get a good grade on this lab. You will be graded entirely on the effort you put into it, as described by your report.
5) If you break into a machine, do not alter the state of the machine as a courtesy to other teams.
6) No length is specified. The report is done when you have followed the guidelines given below and can justify the numeric grade (see below) you have assigned to the network.
The Report:

The report should be in the form of a network security assessment document including but not limited to the following sections: a summary of the security state of the network, the network topology, justifications for your assessment, and recommendations on how to fix vulnerabilities and enhance security.

The summary of the state of security should briefly explain the vulnerabilities as well as the strengths of network. An overall numeric grade should be assigned and justified in the justification section. Please explain your grading scale. The justification section should be the core of the report including specific details such as the vulnerabilities present, tools used to detect them, and how they were exploited. Please backup your assumptions with scan results. You may place these in the Appendix. The recommendations section should contain fixes for the vulnerabilities and techniques on how to prevent compromises and bolster the network.

Please understand that this document should be “as real world” as possible. You are a security consultant presenting a report to your clients. The document should clearly convey to them the current state of their network and your recommendations.

General Questions

How long did it take you to complete this lab? Was it an appropriate length lab?