Comp 8506 Computer Systems Technology September 2010

Selected Topics in Network Security and Design

Assignment #2

Due: October 7, 1330 hrs. This is a team assignment.

Objective: To become familiar with Active and Passive network reconnaissance techniques.

Assignment:

- Download any passive and active reconnaissance tool(s) of your choice and set them up on your system at home.
- Use both passive and active reconnaissance techniques to obtain as much information as possible on another team's network or system at home.
- The type of information you are after is what a hacker would want to know in order to launch an attack against the subnet.
- Present your findings in a brief but concise report showing the processes, tools and techniques you used.
- Your report must also explain how such activities may be detected and show possible ways of blocking such activity.
- This is a good opportunity to use all of the scanning, mapping, and enumeration tools that we have discussed in class. In addition, you can also use the knowledge and skills acquired from the Comp 7006 and 8006 courses (hping3, nmapfe, etc).

Constraints:

- Make CERTAIN that you restrict your reconnaissance activities to the team that you have agreed to conduct this experiment with.
- Your report must have technical depth in presenting and explaining your findings. In other words it should not be a high-level marketing type report. The same applies to the defensive and detection recommendations you make.
- You report must include all the information that you have obtained in a clear and easy to understand format. Diagrams and tables are a good idea.
- Use the standard technical format for you report, i.e., Introduction/Summary, Body, Conclusions, etc.

To Be Submitted:

- Submit a complete package on disk that includes your report, tools that you used, and any supporting data (dumps, etc), and references.

Assignment #2 Evaluation

(1). Explanation of Methodology/Recon Plan:
15
(2). Technical Depth (use of terminology, protocol characteristics, supporting data, etc):
35
(3). Defensive/Detection Recommendations:
15
(4). Variety of tools & processes: 20
(5). Report format and clarity: 15

Total: 100