Comp 8506   Computer Systems Technology   October 2010

Selected Topics in Network Security and Design

Assignment #3

Due: October 8, 2010, 1330 hrs. This is a team assignment.

Objective: To understand, perform and analyze Active Sniffing of a Switched LAN.

Assignment:

- Set up a testbed within your team. As a minimum you will need 3 machines and a switch.
- Download and install switch-sniffing tool (**dsniff** or **Ettercap** for example) on the attacking machine.
- Download and read the paper titled "**Penetration Testing with dsniff**" by Christopher Russel.
- You are required to replicate at least one of the four attacks described in the paper above and present a detailed report on your team experiment.
- 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.

Constraints:

- One of your tests must be to replicate the Man-in-the-Middle attack.
- As part of your experiment you must also deploy an IDS of your choice and provide data to indicate whether or not the IDS was successful in detecting the dsniff activity.
- 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.
- You must support that data in your report with actual captures from your experiments.
- Use the standard technical format for you report, i.e., Introduction/Summary, Body, Conclusions, etc.

To Be Submitted (on disk):

- Submit a technical report, including all relevant data and references.
- Provide all of the captured evidence of your exploits on disk.

Assignment #3 Evaluation

(1). Explanation of Methodology/active sniffing:	/ 15
(2). Basic Assignment Requirements:	/ 30
(3). Variety of attacks:	/ 10
4). Report format and clarity:	/ 15

Total:	/ 70

Comments: