

Comp 8506 Computer Systems Technology September 2018

Selected Topics in Network Security and Design

Assignment #1

Due: September 20, 1430 hrs. This is an individual assignment.

Objective: To observe and understand the nature of exploits and attacker processes.

Assignment:

- You are required to research at least three major vulnerabilities and exploits that have occurred in the last two years.
- Obviously there have been a huge number of exploits, so select three that had the most impact and research as much technical information on those as possible.
- The type of information you are looking for is how the vulnerability was uncovered, how the exploit was carried out, the impact it had on industry or society in general, and how the vulnerability was patched.
- Specifically, you will be identifying the following:
 - The main vulnerability and the exploit(s) that was used on it.
 - Type of attacks that were launched.
 - Attack routes that were used.
- Comment on what sort of reconnaissance (Active and Passive reconnaissance) would be required to uncover and identify the vulnerabilities you have selected.
- Write a brief technical report describing all of the above characteristics you have found.

Constraints:

- The discussion in class on “**Exploits and Attacker’s Processes**” must be used as the framework for your analysis and critique.
- Provide references and/or correlations for the exploits you have observed.
- Use the standard technical format for your report, i.e., Introduction/Summary, Body, Conclusions, etc.

To Be Submitted:

- Submit a brief report, including all relevant data and references.
- Submit a **PDF** report in the sharein folder for this course under “Assignment #1”.

Assignment #1 Evaluation

Explanation of Methodology/Recon Plan:	10
Technical Depth (use of terminology, protocol characteristics, supporting data, etc):	25
Defensive/Detection Recommendations:	5
Report format and clarity:	10
Total:	50