Directed Study in Forensics: Overview

Chris Williams

2010-10-22

1 Introduction

The purpose of this directed study is to cover the theory and techniques of digital forensics. This includes malware and rootkit analysis, investigation of intrusions and the legal implications of forensic analysis. The focus is on the theory. The purpose is *not* to replace a real Network Security course, but to act as more of a deeper look into one topic of security.

2 Reading

Due to the theory-based focus, there is a significant amount of reading involved. The following have been read to date, with analyses and summaries or "book reports" forthcoming.

1. *Forensic Discovery* (Farmer, Venema, 2005)
2. *Rootkits: Subverting the Windows Kernel* (Hoglund, Butler, 2005)
3. *Cyber Crime Investigations* (Reyes, 2007)
4. *Hacking Exposed: Malware Rootkits Secrets and Solutions* (Davis, Bodmer, LeMasters, 2009)

Possible future reading:

1. *Computer Forensics for Dummies* (Volonino, Anzaldua, 2008)
2. *Snort for Dummies* (Scott, Wolfe, Hayes, 2004)

3 Practical Work

While the focus of the study is on theory, certainly there must be some element of hands-on work. This should involve a forensic investigation of some sort, likely an analysis of an infected or otherwise compromised machine. A smaller project could be the disassembly and analysis of a specific piece of malware.

Additionally, documentation on malware detection, analysis and removal with specific tools (such as Trend Micro's *HijackThis!* could be written, targeted at "power users."

4 Miscellaneous

I attended a meeting of the *Messaging Anti-Abuse Working Group* (MAAWG) in early October. Malware was a frequent topic of discussion, so it is somewhat related to this course. Due to the confidentiality policy, it might not be possible to release notes from the conference. If notes can be released, they must be edited first.