CSS 579 Malware Analysis and Reverse Engineering

Explores techniques and technologies for detecting and responding to attacks. Types of malware are discussed, and techniques for detection, identification and eradication are explored. Reverse engineering of code and network exploits are presented as a method for understanding and development of countermeasures.

Learning Objectives

- Identify different types of malware by operation and effective mitigation strategies
- Perform reverse engineering to determine the function of malicious code in a binary
- Determine malicious communication protocols from network communication
- Understand and utilize intrusion and anomaly detection techniques
- Detect and eradicate malicious software from a system

Grading

Labs	40%
Project	15%
Research	10%
Quizzes and Exams	35%

Labs

You will complete 8 labs. Most of these require reverse engineering malware or writing C++ code that will demonstrate techniques that malware uses.

Required Textbooks

Practical Malware Analysis by Michael Sikorski and Andrew Honig, 2012

Optional Textbooks and Readings

Malware Analysis: An Introduction [whitepaper]
http://www.sans.org/reading_room/whitepapers/malicious/malware-analysis-introduction_2103 (Links to an external site.)Links to an external site.

GIAC Reverse Engineering Malware (GREM) [Certification]
http://www.giac.org/certification/reverse-engineering-malware-grem (Links to an external site.)Links to an external site.

Forensic Discovery [book]
http://www.amazon.com/exec/obidos/tg/detail/-/020163497X/104-5123010-9411940 (Links to an external site.)Links to an external site.

http://www.porcupine.org/forensics/forensic-discovery/ (Links to an external site.)Links to an external site.

Practical Malware Analysis [presentation]
http://www.blackhat.com/presentations/bh-dc-07/Kendall_McMillan/Paper/bh-dc-07-Kendall_McMillan-WP.pdf (Links to an external site.)Links to an external site.

Malware Analysis for Administrators [article]
http://www.symantec.com/connect/articles/malware-analysis-administrators (Links to an external site.)Links to an external site.

Stuxnet Malware Analysis [paper]
http://www.codeproject.com/KB/web-security/StuxnetMalware.aspx (Links to an external site.)Links to an external site.

Tentative Schedule

Week 0 Introduction to malware, analysis, and trends. Infection vectors and discovery
Week 1 Sandboxing and dynamic analysis and Assembly Language review
Week 2 Introduction to IDA Pro
Week 3 C code constructs in assembly and Analyzing Windows Programs
Week 4 Malware Behavior and Covert Malware Launching
Week 5 Data Encoding and Network Signatures
Week 6 Malicious documents and Browser-based exploits
Week 7 Protocol reverse engineering
Week 8 Advanced Anti-Reverse Engineering
Week 9 Automated Reverse Engineering
Week 10 Final Presentations