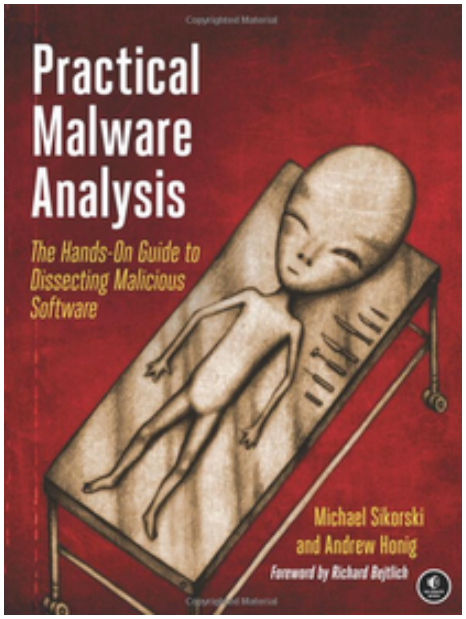
CNIT 126: Practical Malware Analysis



Spring 2017 Sam Bowne

37184 Mon 6:10 - 9 PM SCIE 200

Catalog Description

Learn how to analyze malware, including computer viruses, trojans, and rootkits, using disassemblers, debuggers, static and dynamic analysis, using IDA Pro, OllyDbg and other tools.

Advisory: CS 110A or equivalent familiarity with programming

Upon successful completion of this course, the student will be able to:

A. **Describe types of malware, including rootkits, Trojans, and viruses.**
B. **Perform basic static analysis with antivirus scanning and strings**
C. **Perform basic dynamic analysis with a sandbox**
D. **Perform advanced static analysis with IDA Pro**
E. **Perform advanced dynamic analysis with a debugger**
F. **Operate a kernel debugger**
G. **Explain malware behavior, including launching, encoding, and network signatures**
H. **Understand anti-reverse-engineering techniques that impede the use of disassemblers, debuggers, and virtual machines**
I. **Recognize common packers and how to unpack them**

Textbook

"Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", by Michael Sikorski and Andrew Honig; ISBN-10: 1593272901 Buy from Amazon

Quizzes

The quizzes are multiple-choice, online, and open-book. However, you may not ask other people to help you during the quizzes. You will need to study the textbook chapter before the lecture covering it, and take the quiz before that class. Each quiz is available for one week, up till 8:30 am Saturday. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts. If you take the quiz twice, the second score is the one that counts, not necessarily the higher score.

To take quizzes, log in to CCSF's online class site here:

https://ccsf.instructure.com

Schedule (may be revised)

Note: Chapter Numbers are one too high in the E-Book: Chapter 0 is mislabeled as Chapter 1, etc.

Date	Quiz	Topic
Mon 1-23		**0: Malware Analysis Primer & 1: Basic Static Techniques**
Mon 1-30		**2: Malware Analysis in Virtual Machines & 3: Basic Dynamic Analysis**
Fri 2-3	***Last Day to Add Classes***	
Mon 2-6	**Ch 0-1 Quiz due before class Ch 3-4 Quiz due before class Proj 1-2 due**	**4: A Crash Course in x86 Disassembly**
Mon 2-13	**Ch 2-3 Quiz due before class Ch 5 Quiz due before class Proj 3 due**	**5: IDA Pro**
Mon 2-20	***Holiday - No Class***	
Mon 2-27	**Ch 6 Quiz due before class Proj 4-5 due**	**6: Recognizing C Code Constructs in Assembly**
Mon 3-6	**Ch 7 Quiz due before class Proj 6 due**	**7: Analyzing Malicious Windows Programs**
Mon 3-13	**Ch 8 Quiz due before class Proj 7-8 due**	**8: Debugging**
Mon 3-20	**Ch 9 Quiz due before class Proj 9 due**	**9: OllyDbg**
Mon 3-27	***Holiday - No Class***	
Mon 4-3	**Ch 10 Quiz due before class Proj 10-11 due**	**10: Kernel Debugging with WinDbg**
Wed 4-6	***Mid-Term Grades Due***	
Mon 4-10	**Ch 11 Quiz due before class Proj 12 due**	**11: Malware Behavior**
Mon 4-17	**Ch 12 Quiz due before class Proj 13 & 14 due**	**12: Covert Malware Launching**
Mon 4-24	**Ch 13 Quiz due before class Proj 15 due**	**13: Data Encoding**
Mon 5-1	**Ch 14 Quiz due before class Proj 16 due**	**14: Malware-Focused Network Signatures**
Mon 5-8	**Ch 15 Quiz due before class No Proj. due**	**15: Anti-Disassembly**
Mon 5-15	**Last Class · No Quiz · All extra credit Proj. due · TBA**	
Mon 5-23		***Final Exam***