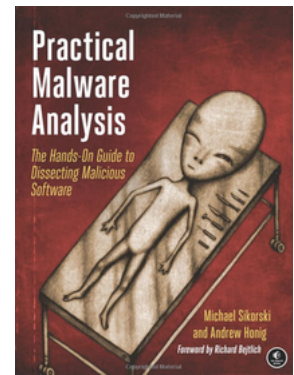


# CNIT 126: Practical Malware Analysis

Fall 2019 Sam Bowne

78188 Tue 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 comTue packers and how to unpack them

## Textbook

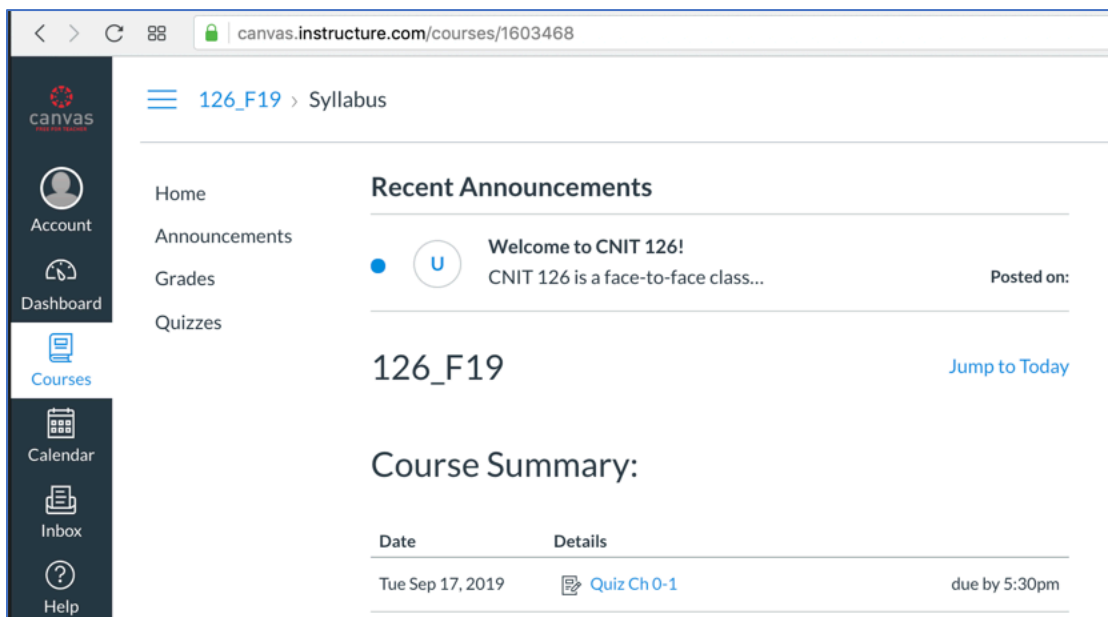
"Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software", by Michael Sikorski and Andrew Honig; ISBN-10: 1593272901 [Buy from Amazon](#)

## Quizzes

The quizzes are multiple-choice, online, and open-book. Study the textbook chapter and take the quiz before that class. Each quiz is due 30 min. before class. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts.

To access the quizzes:

- Go to <https://canvas.instructure.com/enroll/TYTAPN>
- If you've taken one of my class previously, you should already have an account on this Canvas server (it's NOT the usual CCSF Canvas system). Otherwise, create a new account.
- You should see the course, including the quizzes, as shown below.
- After you have joined the course, you can access it at [canvas.instructure.com](https://canvas.instructure.com)
- **Questions? Email [CNIT.126sam@gmail.com](mailto:CNIT.126sam@gmail.com)**



The screenshot shows the Canvas LMS interface for course 126\_F19. The browser address bar displays [canvas.instructure.com/courses/1603468](https://canvas.instructure.com/courses/1603468). The page title is "126\_F19 > Syllabus". The left sidebar contains navigation links: Home, Account, Announcements, Grades, Quizzes, Dashboard, Courses, Calendar, Inbox, and Help. The main content area features a "Recent Announcements" section with a message: "Welcome to CNIT 126! CNIT 126 is a face-to-face class..." posted on an unspecified date. Below this is a section for "126\_F19" with a "Jump to Today" link. The "Course Summary" section includes a table with columns for "Date" and "Details".

Date	Details
Tue Sep 17, 2019	Quiz Ch 0-1 due by 5:30pm

## Live Streaming

Live stream at: <https://zoom.us/j/4108472927>

Classes will also be recorded and published on YouTube for later viewing.

## Email

For class-related questions, please email  
[cnit.126sam@gmail.com](mailto:cnit.126sam@gmail.com)