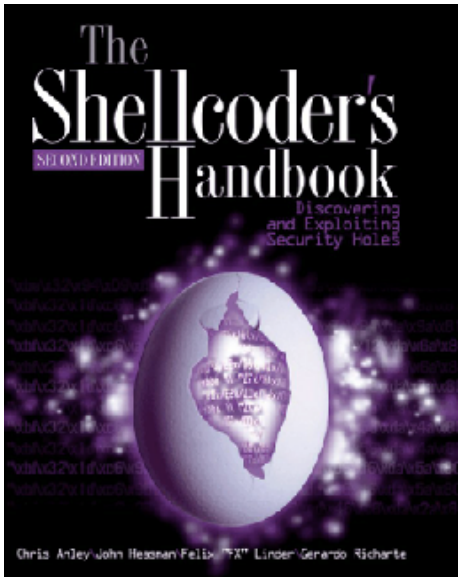
CNIT 127: Exploit Development

Sat 1-4 PM SCIE 37

Spring 2018



Catalog Description

Learn how to find vulnerabilities and exploit them to gain control of target systems, including Linux, Windows, Mac, and Cisco. This class covers how to write tools, not just how to use them; essential skills for advanced penetration testers and software security professionals.

Advisory: CS 110A or equivalent familiarity with programming

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

A. **Read and write basic assembly code routines**
B. **Read and write basic C programs**
C. **Recognize C constructs in assembly**
D. **Find stack overflow vulnerabilities and exploit them**
E. **Create local privilege escalation exploits**
F. **Understand Linux shellcode and be able to write your own**
G. **Understand format string vulnerabilities and exploit them**
H. **Understand heap overflows and exploit them**
I. **Explain essential Windows features and their weaknesses, including DCOM and DCE-RPC**
J. **Understand Windows shells and how to write them**
K. **Explain various Windows overflows and exploit them**
L. **Evade filters and other Windows defenses**
M. **Find vulnerabilities in Mac OS X and exploit them**
N. **Find vulnerabilities in Cisco IOS and exploit them**

Student Learning Outcomes

1. **Read and write basic assembly code routines**
2. **Find stack overflow vulnerabilities and exploit them**
3. **Evade filters and other Windows defenses**

Textbook

"The Shellcoder's Handbook: Discovering and Exploiting Security Holes ", by Chris Anley, John Heasman, Felix Lindner, Gerardo Richarte; ASIN: B004P5O38Q

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 12:30 pm 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, first claim your RAM ID and then log in to Canvas here:

https://ccsf.instructure.com

Live Streaming

You can attend class remotely using Zoom.

Join from PC, Mac, Linux, iOS or Android: https://zoom.us/j/4108472927
Meeting ID: 410-847-2927

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

Schedule (may be revised)

Date	Due	Topic
Sat 1-20		**Ch 1: Before you Begin**
Sat 1-27	**Ch 1 Quiz**** **Ch 2 Quiz****	**Ch 2: Stack overflows on Linux**
Sat 2-3	**Ch 3 Quiz****	**Ch 3: Shellcode**
Sat 2-10	**Ch 4 Quiz*** **Proj 0, 1, & 2 due**	**Ch 4: Introduction to format string bugs**
Sat 2-17	***Holiday - No Class***	
Sat 2-24	**Ch 5 Quiz*** **Proj 3 & 4 due**	**Ch 5: Introduction to heap overflows**
Sat 3-3	**Ch 6 Quiz*** **Proj 5 & 6 due**	**Ch 6: The Wild World of Windows**
Sat 3-10	**No Quiz due** **Proj 7 & 8 due**	**Lecture 7: Intro to 64-Bit Assembler (Not in book)**
Sat 3-17	**Ch 8a Quiz*** **Proj 8a & 8b due**	**Ch 8: Windows overflows (Part 1)**
Sat 3-24	**Ch 8b Quiz*** **Proj 9 due**	**Ch 8: Windows overflows (Part 2)**
Sat 3-31	***Holiday - No Class***	
Sat 4-7	**Nothing due**	**Guest TBA**
Sat 4-14	**Ch 14 Quiz*** **Proj 10 & 11 due**	**Ch 14: Protection Mechanisms**
Sat 4-21	**Ch 16+17 Quiz*** **Proj 12 & 13 due**	**Ch 16: Fault Injection** **Ch 17: The Art of Fuzzing**
Sat 4-28	**Ch 18 Quiz*** **Proj 14 & 15 due**	**Ch 18: Source Code Auditing**
Sat 5-5	**No Quiz** **Proj 16 due**	**Hopper Debugger**
Sat 5-12	**No Quiz** **All Extra Credit Proj due**	**Last Class: TBA**
Wed 5-16 - **Wed 5-23**	**Final Exam available online throughout the week.** **You can only take it once.**	

**** Quizzes due 30 min. before class***
***** Not counted as late until 2-10***