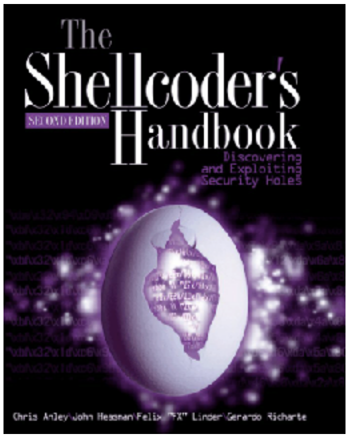
The Shellcoder's Handbook
Second Edition
Discovering and Exploiting Security Holes
Chris Anley John Heasman Felix "FX" Linder Gerardo Richarte

CNIT 127: Exploit Development

78189 501 Wed 6:10 - 9:00 PM SCIE 37

Fall 2019 Sam Bowne

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 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 due 30 min. before class. 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.

Quizzes are here:

https://canvas.instructure.com/enroll/7G44CD

Live Streaming

You can attend class remotely 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.127sam@gmail.com