

CNIT 123

Ethical Hacking and Network Defense

Spring 2018 Sam Bowne

36684 501 SAT 10:10–1:00 PM SCIE 37

Catalog Description

ADVISE: CNIT 106 or 120 or 201C



Learn how hackers attack computers and networks, and how to protect Windows and Linux systems. Legal restrictions and ethical guidelines will be taught and enforced. Students will perform many hands-on labs, both attacking and defending, using port scans, footprinting, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors. CSU

Learn about attacks and how to defend Windows and Linux systems.

Student Learning Outcomes

After successful completion of this course, students will be able to:

1. Determine what an ethical hacker can and cannot do legally, and evaluate credentials and roles of penetration testers.
2. Perform reconnaissance on a target network using a variety of scanning and probing techniques.
3. Enumerate and classify Microsoft and Linux Operating Systems vulnerabilities.
4. Take control of Web Servers and wireless networks, and protect them.
5. Evaluate and select cryptography and hashing methods, and perform attacks against them.
6. Select and implement security devices, including routers, firewalls, Intrusion Detection Systems, and honeypots.

Textbook

Hands-On Ethical Hacking and Network Defense, Third Edition by Michael T. Simpson, Kent Backman, and James Corley -- ISBN: 9781285454610

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 higher score counts.

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)

<u>Date</u>	<u>Quiz</u>	<u>Topic</u>
Sat 1-20		Ch 1: Ethical Hacking Overview Bitcoin, NCL, & Lockpicking
Sat 1-27		Ch 2: TCP/IP Concepts Review
<i>Fri 2-2</i>	<i>Last Day to Add Classes</i>	
Sat 2-3	Ch 2 & 3 Quiz * Proj 1 & 2 due	Ch 3: Network and Computer Attacks
Sat 2-10	Ch 4 Quiz * Proj 3 & 4 due	Ch 4: Footprinting and Social Engineering
<i>Sat 2-17</i>	<i>Holiday - No Class</i>	
Sat 2-24	Ch 5 Quiz * Proj 5 & 6 due	Ch 5: Port Scanning
Sat 3-3	Ch 6 Quiz * Proj 7 & 8 & 9 due	Ch 6: Enumeration
Sat 3-10	Ch 7 Quiz * Proj 9 & 10 due	Ch 7: Programming for Security Professionals
Sat 3-17		Guest Speaker (may be rescheduled)
Sat 3-24	Ch 8 Quiz * Proj 11 & 12 due	Ch 8: Desktop and Server OS Vulnerabilities
<i>Sat 3-31</i>	<i>Holiday - No Class</i>	
Sat 4-7	Ch 9 Quiz * Proj 13 & 14 due	Ch 9: Embedded Operating Systems: The Hidden Threat
Sat 4-14	Ch 10 Quiz * Proj 15 & 16 due	Ch 10: Hacking Web Servers
Sat 4-21	Ch 11 Quiz * Proj 17 & 18 due	Ch 11: Hacking Wireless Networks
Sat 4-28	Ch 12 Quiz * Proj 19 & 20 due	Ch 12: Cryptography (Part 1)
Sat 5-5	No Quiz due Proj 21 & 22 due	Ch 12: Cryptography (Part 2)
Sat 5-12	Ch 13 Quiz * All extra credit projects due	Last Class: Ch 13: Network Protection Systems
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