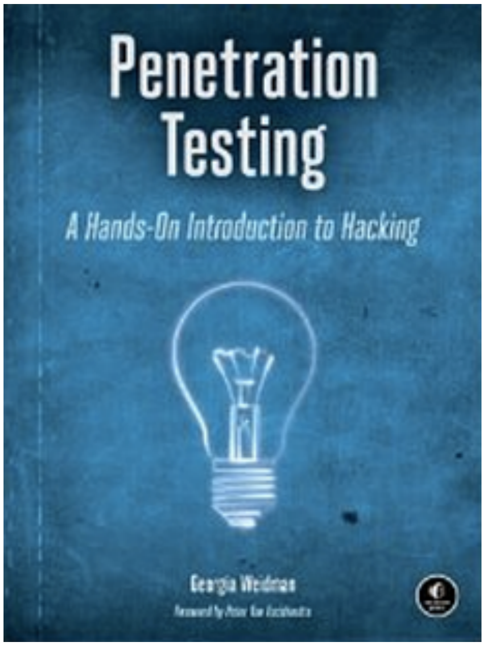
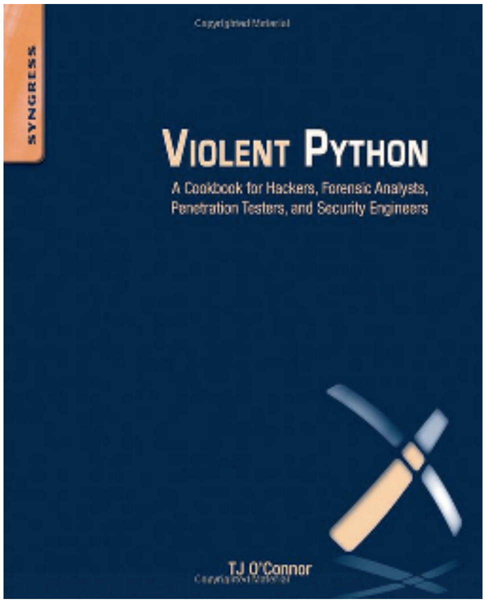


Required book ($25 - $33)

CNIT 124 Advanced Ethical Hacking

Fall 2017 Sam Bowne

```
CRN 77818
Thu 6:10-9:00
MUB 388
```


Copyrighted Material
SYNGRESS
VIOLENT PYTHON
A Cookbook for Hackers, Forensic Analysts, Penetration Testers, and Security Engineers
TJ O'Connor

Optional book ($35)

Catalog Description

Advanced techniques of defeating computer security, and countermeasures to protect Windows and Unix/Linux systems. Hands-on labs include Google hacking, automated footprinting, sophisticated ping and port scans, privilege escalation, attacks against telephone and Voice over Internet Protocol (VoIP) systems, routers, firewalls, wireless devices, Web servers, and Denial of Service attacks.

Prerequisites: CNIT 123.

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

A. **Use Google and automated footprinting tools to locate vulnerable Web servers, passwords, open VNC servers, database passwords, and Nessus reports**
B. **Perform sophisticated ping and port scans with several tools, and protect servers from the scans**
C. **Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services**
D. **Use authenticated and unauthenticated attacks to compromise Windows and Unix/Linux systems and install backdoors and remote-control agents on them, and protect the systems from such attacks**
E. **Enter networks through analog phone systems, defeating many authentication techniques, and defend networks from such attacks**
F. **Penetrate PBX, voicemail, Virtual Private Network (VPN), and Voice over Internet Protocol (VoIP) systems, and defend them**
G. **Perform new wireless attacks, including denial-of-service and cracking networks using Wi-Fi Protected Access (WPA) and WPA-2**
H. **Identify firewalls and scan through them**

I. **Perform classical and modern Denial of Service (DoS) attacks, and defend networks from them**
J. **Locate Web server vulnerabilities, exploit them, and cure them**
K. **Describe many ways Internet users are attacked through their browsers and other Internet clients, and the protective measures that can help them**

Student Learning Outcomes (measured to guide course improvements)

Enumerate resources on systems using banner-grabbing and specific attacks against common Windows and Unix/Linux services including FTP, Telnet, HTTP, DNS, and many others, and protect those services
Perform classical and modem Denial of Service (DoS) attacks, and defend networks from them
Locate Web server vulnerabilities, exploit them, and cure them

Textbook

***Penetration Testing: A Hands-On Introduction to Hacking* by Georgia Weidman -- ISBN-10: 1593275641, No Starch Press; 1 edition (June 8, 2014) 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 30 minutes 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 higher score counts.

To take quizzes, first claim your RAM ID and then log in to Canvas here: https://ccsf.instructure.com

Live Streaming

Live stream at: ccsf.edu/webcasts

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

Schedule (may be revised)

Date	Quiz	Topic
Thu 8-24		**Ch 1: Setting Up Your Virtual Lab**
Thu 8-31		**Ch 2: Using Kali Linux**
Thu 9-7		**Ch 3: Programming**
Fri 9-8	*Last Day to Add Classes*	
Thu 9-14	**Quizzes Ch 2 & 4 due before class** **Proj 1-3 due**	**Ch 4: Using the Metasploit Framework**
Thu 9-21	**Quizzes Ch 3 & 5 due before class** **Proj 4 & 5 due**	**Ch 5: Information Gathering**
Thu 9-28	**No Quiz**	*Guest Speaker (may be rescheduled)*
Thu 10-5	**Quiz Ch 6 due before class** **Proj 7 due**	**Ch 6: Finding Vulnerabilities**
Thu 10-12	**Quiz Ch 7 due before class** **Proj 8 due**	**Ch 7: Capturing Traffic**
Thu 10-19	**Quiz Ch 8 due before class** **Proj 9 due**	**Ch 8: Exploitation**
Thu 10-26	**Quiz Ch 9 due before class** **Proj 10 & 11 due**	**Ch 9: Password Attacks**
Thu 11-2	**Quiz Ch 10-12 due before class** **Proj 12 due**	**Ch 10: Client-Side Exploitation** **Ch 11: Social Engineering** **Ch 12: Bypassing Antivirus Applications**
Thu 11-9	**No Quiz**	*Guest Speaker (may be rescheduled)*
Thu 11-9	*Last Day to Withdraw*	
Thu 11-16	**Quiz Ch 13 (Part 1) due before class** **Proj 13 due**	**Ch 13: Post Exploitation (Part 1)**
Thu 11-23	*Holiday - No Class*	
Thu 11-30	**Quiz Ch 13 (Part 2) due before class** **Proj 14 & 15 due**	**Ch 13: Post Exploitation (Part 2)**
Thu 12-7	**No Quiz** **Proj 16 due**	**TBA**
Thu 12-14	**No Quiz** **All extra credit projects due**	**Last Class: TBA**
Thu 12-21		*Final Exam*