Carnegie Mellon
Heinz College

<table>
<tr><td>Course Information*</td><td>Course Title: 95-483 & 95-883 Ethical Penetration Testing
Instructor: Derrick Spooner

Office Hours: Discord Chat, and by appointment only

Textbook:
All readings are online resources as indicated by each week’s section.

The Hacker Playbook (Optional)
https://www.amazon.com/Hacker-Playbook-Practical-Penetration-Testing/dp/1494932636
*DO NOT get The Hacker Playbook 2. It is not a second edition but rather a continuation.

Red Team Field Manual (Optional)
http://www.amazon.com/Rtfm-Red-Team-Field-Manual/dp/1494295504</td></tr>
<tr><td>Prerequisites (if applicable)</td><td>Students will be required have a basic understanding of networking concepts (TCP/IP) and will be expected to put in the additional time to research solutions on their own. This course will utilize the Kali Linux platform so basic Linux command line knowledge will be required.

Networking and Linux skills will NOT be taught during the course. Students are expected to already possess this knowledge.</td></tr>
<tr><td>Description*</td><td>This course will introduce students to professional penetration testing by teaching offensive tactics along with the appropriate methodologies and responsibilities it takes to ethically attack systems. The majority of time will be spent in hands-on labs performing reconnaissance, discovering vulnerabilities, developing exploits, and carefully penetrating targets.</td></tr>
<tr><td>Course Materials (if applicable)</td><td>Documents posted on the course’s Canvas site and distributed in class.</td></tr>
<tr><td>Evaluation Method</td><td>The final grade will be out of 400pts (100%). The grading breakdown is listed below.

<table><tr><td>Assignments (8)</td><td>30pts each for a total of 240 (60%)</td></tr><tr><td>Quizzes (6)</td><td>10pts each for a total of 60 (15%)</td></tr><tr><td>Final Exam (1)</td><td>100pts (25%)</td></tr></table></td></tr>
<tr><td>Grading Scale</td><td>A+ 100% B+ 87 - 89% C+ 77 - 79%
A 93 - 99% B 83 - 86% C 73 - 76%
A- 90 - 92% B- 80 - 82% C- 70 - 72%

*A+ cannot be achieved through any bonus points or curving</td></tr>
<tr><td>Grading Rubric/explanation of grades</td><td>Quizzes:
A short quiz will be administered at the beginning of weeks 2 through 7 consisting of multiple choice and fill-in-the-blank questions. The content will be derived from the previous week’s lecture and assigned readings. Quizzes are designed to be completed in 10 minutes.</td></tr>
</table>

	Labs: Weekly assigned labs are not graded exercises and will not be monitored for completion. They are, however, essential to the lessons taught during the week and will serve the student well in preparing for the assignments and final exam. **Assignments**: The format of the assignment will vary depending on the subject, with some being completed on personal computers and others being completed within the hands-on lab environment. Each assignment will have explicit directions and guidance on how it will be scored. All assignments will be due at 6:30 PM, the start of the next week's class. **Late Policy:** Any assignment turned in late will face an hourly deduction of up to 50% for the first 24 hours that it is turned in late. After the 24 hours, the assignment will receive a 0% grade. Points will be deducted per this policy unless the student has made arrangements with me prior to the assignment's due date. PRIOR ARRANGEMENTS MUST BE MADE NO LATER THAN 12 PM ON THE DUE DATE. The timestamp given by Canvas will be the determining factor if the assignment is late or not. One second past the due date is still late! I suggest giving yourself enough time to log into Canvas and submit. If there are any issues, feel free to email the assignment to the instructor, in which case the email timestamp will be used. You have unlimited attempts to re-submit updated copies of your assignments in Canvas until the due date/time, and I will only consider the most recent, on-time submission for grading. **Final Exam:** The final exam will consist of a network of machines that the must be be properly assessed to determine potential vulnerabilities and opportunities for exploitation. You will work as a group throughout the semester to compile a professional report. During the scheduled final exam time slot you will deliver an outbriefing on your findings just like on a real penetration test. Grading will be broken down as follows: • Written Report – 50pts • Outbriefing – 30pts • Systems Compromised – 10pts • Peer Review – 10pts **Grade Challenges:** Students will only have 2 weeks after an assignment or exam is returned to question or challenge a grade. After the two-week challenge period, the grade will not be changed. Please contact the instructor if you wish to question a grade. You must provide justification for why the specific question(s) on an assignment should be reviewed and updated.
Course/Topical Outline:	A weekly breakdown of topics and assignments (readings, homework, project due-dates) **Week 1**

	Topic	• Becoming a penetration tester
		  ○ Methodologies
		  ▪ Penetration testing lifecycle
		  ▪ Scoping
		  ▪ Rules of Engagement
		  ▪ Pen testing vs. red teaming
		  ▪ External vs. internal
		  ○ Ethics
		  ▪ Confidentiality
		  • Handling PII
		  ▪ Business continuity
		  ▪ Staying within scope
		  ○ Hacking within the law
		  ▪ Statutes and Acts
		  ▪ Disclosure policies
		  ○ Reporting
		  ▪ Technical vs. business level language
		  ○ Client interaction
		• Gaining access to STEPfwd
		• Using TryHackMe
		• Reconnaissance
		  ○ Knowing your target
		  ○ Public information
		  ▪ DNS, site cache, public hosted docs, etc.
		  ○ Google Dorks
		  ○ Maltego and other tools

	Labs	• Using StepFWD
		• Basic Shell Scripting
		• TryHackMe Labs:
		  ○ Tutorial
		  ○ OpenVPN
		  ○ Linux Fundamentals
		  ○ Windows Fundamentals
		  ○ Introductory Networking
		  ○ Introductory Research
		  ○ Google Dorking
		  ○ Hacker Methodology
		  ○ Sublist3r

	Assignments	• Scripting exercise (1) • Reconnaissance report (2)

	Readings	• http://linuxcommand.org/lc3_writing_shell_scripts.php
		• http://www.pentest-standard.org/index.php/Pre-engagement
		• http://www.pentest-standard.org/index.php/Reporting
		• Hacker Playbook (optional)
		  ○ Pregame – The Setup
		  ○ Post Game Analysis – Reporting
		• https://www.linux.com/learn/beginners-guide-nmap
		• https://nmap.org/book/man.html
		• http://null-byte.wonderhowto.com/how-to/use-google-hack-googledorks-0163566/

Week 2	

Topic	• Network scanning
	  ○ Host/port discovery
	  ○ Using Nmap
	  ▪ Notable flags
	  ▪ NSE Scripts
	  ○ Data analysis
	  ▪ Interpreting results
	  ▪ Parsing results
	  ▪ EyeWitness
	  ▪ Dirbuster
	• Brute-force attacks
	  ○ Hydra
	  ○ SNMP
	• Vulnerability Scanning
	  ○ Identifying and testing false positives
	  ○ Vulnerability signatures
	  ○ CVSS scores
	  ○ OpenVAS

Labs	• Network Mapping with Nmap
	• Scanning with OpenVAS
	• TryHackMe Labs:
	  ○ Nmap
	  ○ Hyrdra
	  ○ Nessus
	  ○ OpenVas
	  ○ RustScan

Assignments	• EPT network scan report (3) • EPT vulnerability scan report (4)

Readings	• Hacker Playbook (optional)
	  ○ Before the Snap – Scanning the Network
	• http://www.first.org/cvss/specification-document
	• https://www.first.org/cvss/calculator/3.0
	• Hacker Playbook (optional)
	  ○ Special Teams – Cracking, Exploits, Tricks (Vulnerability Searching section only)

Week 3	

Topic	• Ethical exploitation
	  ○ When to exploit
	  ○ Types of exploits
	• Attacking network services
	  ○ Anonymous FTP
	  ○ Default Credentials
	• Metasploit Framework
	  ○ Background
	  ▪ Community development
	  ▪ Structure
	  ○ Using exploits

	▪ Configuring options o Payloads/Shellcode ▪ Meterpreter/reverse shells/bind shells ▪ Singles vs. stagers ▪ Msfvenom o Session management • C2 Frameworks
Labs	• Using Metasploit • vCenter Metasploit Use Case • TryHackMe Labs: o Blue o Metasploit o Ice o Empire o AttackerKB
Assignments	• Pwn Challenge #1 (5)
Readings	• http://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-1-primer-overview-0155986/ • http://www.fastandeasyhacking.com/manual • Hacker Playbook (optional) o The Drive – Exploiting Scanner Findings

Week 4	
Topic	• Anti-virus evasion o Understanding AV signatures o Using Veil • Windows AD Overview • Intro to post-exploitation o Searching for sensitive files o Privilege Escalation ▪ Local exploits ▪ Group Policy Preferences o Extracting passwords ▪ Hashdump ▪ Mimikatz o Persistence
Labs	• Evading Anti-Virus with Veil • TryHackMe Labs: o Linux PrivEsc o Post-Exploitation Basics o Windows PrivEsc o Linux PrivEsc Arena o Windows PrivEsc Arena
Assignments	• Pwn Challenge #2 (6) • Pwn Challenge #3 (7)
Readings	• http://www.slideshare.net/VeilFramework/the-veilframework

	• https://adsecurity.org/?page_id=1821 (optional reading on inner workings of Mimikatz) • Hacker Playbook (optional) ○ The Quarterback Sneak – Evading AV

Week 5	

Topic	• Intro to Web Exploitation
	  ○ Identifying vulnerabilities
	  ▪ Dirbuster
	  ▪ Nikto
	  ○ SQL injection
	  ▪ Background
	  ▪ SQLMap
	  ○ Cross-site Scripting
	  ▪ Reflected vs. persistent
	  ○ Session hijacking
	  ○ Web shells
	  ○ File inclusion
	  ▪ Remote vs. Local

Labs	• Exploiting DVWA (Metasploitable2)
	• TryHackMe Labs:
	  ○ Web Fundamentals
	  ○ OWASP Top 10
	  ○ OWASP Juice Shop
	  ○ Web Scanning
	  ○ Introduction to OWASP ZAP
	  ○ SQL Injection Lab
	  ○ Injection
	  ○ LFI Basics
	  ○ DVWA
	  ○ Ffuf
	  ○ SSTI
	  ○ OWASp Multillidae II
	  ○ WebGOAT

Assignments	• Pwn Challenge #4 (8) • Pwn Challenge #5 (extra credit)
Readings	• http://www.binarytides.com/sqlmap-hacking-tutorial/ • https://portswigger.net/web-security • http://www.acunetix.com/websitesecurity/cross-site-scripting/ • Hacker Playbook (optional) ○ The Throw – Manual Web Application Findings

Week 6	

Topic	• Additional Topics
	  ○ WiFi
	  ○ IoT
	  ○ Cloud
	• Lecture recaps
	• Walkthrough of all PWN challenges and assignments

	• Q&A with professor
Assignments	• Pwn Challenge #6 (extra credit)

Week 7	
Topic	• Final Presentations

Course Policies & Expectations	**Students with Disabilities:** Our community values diversity and seeks to promote meaningful access to educational opportunities for all students. CMU and your instructors are committed to your success and to supporting Section 504 of the Rehabilitation Act of 1973 as amended and the Americans with Disabilities Act (1990). This means that in general no individual who is otherwise qualified shall be excluded from participation in, be denied benefits of, or be subjected to discrimination under any program or activity, solely by reason of having a disability. If you believe that you need accommodations for a disability, please contact us ASAP, and we will work together to ensure that you have the correct access to resources on campus to assist you through your coursework and time at CMU. **Academic Integrity:** Carnegie Mellon University sets high standards for academic integrity. Those standards are supported and enforced by students, including those who serve as academic integrity hearing panel members and hearing officers. The presumptive sanction for a first offense is course failure, accompanied by the transcript notation "Violation of the Academic Integrity Policy." The standard sanction for a first offense by graduate students is suspension or expulsion. Please see https://www.cmu.edu/policies/student-and-student-life/academic-integrity.html for any questions. The instructors of this course have a strong aversion to cheating of any kind and will hold no reservations enforcing CMU's strict academic policy. As the course name suggests, ethics are important to penetration testing and must also be displayed in the classroom as well. **Cell Phones, Smartphones and other handheld wireless devices:** Other than during class breaks, please silence ring tones and refrain from engaging in calls, messaging or other use during class time. All devices must not be visible in any way during quizzes. **Policy Regarding Students Using English as a Foreign Language:** Assignments in this course are graded with reference to evidence of the acquisition of concepts, presentation format, and accuracy of information. Having done business in countries that use languages other than English, we understand that the use of an unfamiliar language can result in unusual word choices or grammatical errors that are not critical to the overall understanding of the information. Therefore, we will take into account your need to function in a language that may be unfamiliar to you. We will provide feedback as appropriate if we feel that language or grammar you have used in assignments would be best if it were configured in a different way. **Use of CMU Canvas System for this course:** The Heinz Colelge uses Carnegie Mellon University's Canvas system to facilitate distance learning as well as to enhance main campus courses. In this course, we will use the Canvas system generally to post lecture notes and related documents and to receive assignments electronically from students. We welcome feedback during and after the course. Students are encouraged to share life-experiences in class. We are open to suggestions about class sequences, changes to the content and additional topics to cover.