# PENETRATION TESTING—ETHICAL HACKING

Course Number: CIS 6930

Section:

Credit Hours: 3

Academic Term: Fall 2020

Class meeting time and location: This class is facilitated 100% online.

## INSTRUCTOR INFORMATION

**INSTRUCTOR NAME:** Joseph N. Wilson

**EMAIL:** jnw@ufl.edu

**PHONE NUMBER:** 352-514-2191 (cell phone)

**OFFICE HOURS:** To be announced on Canvas site.

**COURSE TA OR COORDINATOR:** To be announced on Canvas site.

## COURSE INFORMATION

**COURSE WEBSITE:** http://elearning.ufl.edu

**COURSE COMMUNICATIONS:** I will respond to email communications (to jnw@ufl.edu) within 36 hours. I respond to communications via the *UFCISE cis4204-ethical-hack* slack channel with 36 hours. Use email for issues that are confidential, use slack for issues of general interest.

**RECOMMENDED TEXTBOOKS:**
Title: The Hacker Playbook
 Author: Peter Kim
 Publication date and edition: 2014
 ISBN: 978-1494932633
Title: The Hacker Playbook 2
 Author: Peter Kim
 Publication date and edition: 2015

ISBN: 978-1512214567

Title: The Hacker Playbook 3

Author: Peter Kim

Publication date and edition: 2018

ISBN: 978-1980901754

Title: How to be Less Stupid About Race:

on Racism, White Supremacy, and the Racial Divide

Author: Crystal M. Fleming

Publication Date and Edition: 9/18/2018

ISBN: 978-080705077-4

**MATERIALS AND SUPPLIES FEES:** N/A

**COURSE DESCRIPTION:** Introduction to the principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The student discovers how system vulnerabilities can be exploited and learns to avoid such problems.

**PREREQUISITE KNOWLEDGE AND SKILLS:** Data Structures (COP 3530)

**COURSE GOALS AND/OR OBJECTIVES:** By the end of this course, students will be able to identify and explain the role of penetration testing in improving the security posture of an enterprise; properly scope the elements of a penetration test to satisfy the needs of an enterprise, and enumerate rules of engagement appropriate to such a test; identify and explain the role of penetration testing techniques and tools; employ penetration testing techniques and tools to exploit vulnerabilities in an enterprise's computer systems, services, and networks; and communicate the business risk of computer system, network, and service vulnerabilities and identify and explain methods of avoiding and/or mitigating security risk.

## HOW THIS COURSE RELATES TO THE STUDENT LEARNING OUTCOMES IN THE COMPUTER SCIENCE AND ENGINEERING:

ABET student outcomes addressed by this course:

1. An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.

3. An ability to communicate effectively with a range of audiences.

4. An ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts.
6. An ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions.
7. An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

**INSTRUCTIONAL METHODS:**

*Lecture Videos* are used to provide the information necessary to understand the principles, tools, and techniques of penetration testing as well as its role in securing a business's computational resources and maintaining the security of individuals. Per-module quizzes (I really should have more) are employed to ensure that you are actually viewing the lecture videos.

*Exercises* are practical assignments that show you understand how to employ penetration testing tools to identify insecure software and that you can report the outcomes and importance of your activities in a coherent manner. Except for the first and last exercises (which are individual assignments), you will work in randomly assigned groups of three to carry out as much of the work as you feel comfortable doing. You should work until completion of the assignment or a minimum of one hour (whichever is shorter). This allows you to meet people in the class, and share your knowledge or need for it with other class members. Being able to work well with other people is indispensable in the computer security field. Don't waste this opportunity.

*Project* completion helps you demonstrate that you can creatively apply the concrete knowledge you embody during the semester. Projects (approved by the instructor) take one of the following forms: contribution to an open-source security software project *or* development of a penetration testing exercise based on current vulnerabilities suitable for use as a practical exercise in this class

*Final Examination* questions should be relatively easy to answer if you actually watched the videos, took the quizzes, and carried out all the work required in the exercises. You can use any *printed* materials that you can carry in your own hands to help you in taking this examination, so it is open book in the same way as Global Information Assurance Certification (GIAC) exams such as the GIAC Penetration Tester (GPEN). The final exam must be completed in two hours. It has 55 equally weighted questions. The scores of the 50 highest questions are summed to yield at most 100 points.

*Leeway Points* will be added to your final examination score (not to exceed 100). Up to 6 leeway points will be provided for qualifying CTF problem solutions. Four leeway points will be provided for a correct key phrase from solving the course key puzzle. Two points will be deducted from your score if you provide an incorrect key phrase. This is done to discourage guessing or trusting someone else to tell you the key phrase.

## COURSE POLICIES

**ATTENDANCE POLICY:** Requirements for class attendance and make-up exams, assignments, and other work in this course are consistent with university policies that can be found on the Attendance Policies page.

**QUIZ/EXAM DATES/POLICIES:** Quizzes and the final examination must be taken before the due date published on Canvas.

**MAKE-UP POLICY:** If, as a result of extreme circumstances, you will not be able to complete a quiz or the final examination, **you must contact the instructor before the due date** in order to have this requirement waived. Failures of technology and general circumstances that make it impossible to complete a quiz or turn in an assignment by the due date will be accommodated on a case-by-case basis, but such situations must be brought to the instructor's attention as soon as possible.

**ASSIGNMENT POLICY:** Assignments must be submitted by the required date. After completing an assignment by the due date and reviewing their grade, a student may submit the assignment for regrading until the Canvas *Available Until* date and notify the instructor of the desire for a regrade. Assignments to be regraded must have received less than 70% credit and the resubmission must have change bars showing edits made since the initial submission. Resubmissions with excessive edits (or resubmissions from those using this policy too frequently) will be rejected at the discretion of the instructor. Regrades will receive no more than a 20% higher grade.

**COURSE TECHNOLOGY:** This course is facilitated 100% online through Canvas. You may access Canvas from UF's e-Learning webpage: http://elearning.ufl.edu/. Please contact the UF Help Desk, http://helpdesk.ufl.edu, if you have any technical difficulties with Canvas.

A Netlab NDG system will be used for completion of all exercises in this class. Information on how to access and use the Netlab system will be provided in class.

**ONLINE COURSE EVALUATION:** Students are expected to provide professional and respectful feedback on the quality of instruction in this course by completing course evaluations online via GatorEvals. Guidance on how to give feedback in a professional and respectful manner is available at https://gatorevals.aa.ufl.edu/students/. Students will be notified when the evaluation period opens, and can complete evaluations through the email they receive from GatorEvals, in their Canvas course menu under GatorEvals, or via https://ufl.bluera.com/ufl/. Summaries of course evaluation results are available to students at https://gatorevals.aa.ufl.edu/public-results/.

## UF POLICIES

**UNIVERSITY POLICY ON ACCOMMODATING STUDENTS WITH DISABILITIES:** Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, www.dso.ufl.edu/drc ) by providing appropriate documentation.  Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation.  Students with disabilities should follow this procedure as early as possible in the semester.

**UNIVERSITY POLICY ON ACADEMIC CONDUCT:**  UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honesty and integrity by abiding by the Honor Code.  On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment."  The Student Honor Code specifies a number of behaviors that are in violation of this code and the possible sanctions.  Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel.  If you have any questions or concerns, please consult with the instructor or TAs in this class.

**CLASS DEMEANOR OR NETIQUETTE:** All members of the class are expected to follow rules of common courtesy in all email messages, threaded discussions, and chats. Review the Netiquette Guide for Online Courses for expected student behavior.

**SOFTWARE USE**: All faculty, staff, and students of the university are required and expected to obey the laws and legal agreements governing software use.  Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator.

Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate.  We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

## GETTING HELP AND RESOURCES

For issues with technical difficulties for Canvas, please contact the UF Help Desk at http://helpdesk.ufl.edu or (352) 392-HELP (4357).

Any requests for make-ups due to technical issues MUST be accompanied by the ticket number received from the Help Desk when the problem was reported to them. The ticket number will document the time and date of the problem. You MUST e-mail your instructor within 24 hours of the technical difficulty if you wish to request a make-up.

Other resources are available at Distance Learning's Getting Help for:

- Counseling and Wellness resources
- Disability resources
- Resources for handling student concerns and complaints
- Library Help Desk support

Should you have any complaints with your experience in this course, please visit Distance Learning's Student Complaint Process to submit a complaint.

## GRADING POLICIES

**COURSE GRADING POLICY:** Grades will be determined based on your performance on the following activities:

| Assignment Type | Points or percentage |
|---|---|
| Quizzes | 20% |
| Practical Assignments | 30% |
| Project | 30% |
| Final Examination | 20% |

| Assignment Type | Points or percentage |
|---|---|
| | |

**GRADING SCALE:** For more information, review Frequently Asked Questions for Minus Grades.

| Percent | Grade | Grade Points |
|---|---|---|
| 90.0 – 100.0 | A | 4.00 |
| 87.0 – 89.9 | A- | 3.67 |
| 84.0 – 86.9 | B+ | 3.33 |
| 81.0 – 83.9 | B | 3.00 |
| 78.0 – 80.9 | B- | 2.67 |
| 75.0 – 79.9 | C+ | 2.33 |
| 72.0 – 74.9 | C | 2.00 |
| 69.0 – 71.9 | C- | 1.67 |
| 66.0 – 68.9 | D+ | 1.33 |
| 63.0 – 65.9 | D | 1.00 |
| 60.0 – 62.9 | D- | 0.67 |
| 0 – 59.9 | E | 0.00 |

## COURSE SCHEDULE

### A WEEKLY SCHEDULE OF TOPICS AND ASSIGNMENTS:

Modules denoted M0x##, quizzes denoted Q0x##, practical assignments denoted Ex##

Rather than listing actual weeks, here, I am listing what I will call *module weeks*. Each module week will consist of at most 5 work days and at least 4 work days. Be careful, Module Weeks 10 and 11 have due dates on Monday 2 November and Friday 6 November. Also, module weeks can contain one or two modules. Module weeks 4, 11, and 16 each contain two modules, so don't get caught unawares! And, yes, that means the first week of November is pretty much crunch time for this class.

| Week | Topic | Assignment | Due Date |
|---|---|---|---|
| 1 | M0x00 Pentesting—What is it, Really? | Q0x00<br>Ex000 Pen Test Agreement | 4 Sep 2020<br>11 Sep 2020 |
| 2 | M0x01 Doing the Right Things… | Q0x01<br>Ex010 Netlab Kali | 11 Sep 2020<br>18 Sep 2020 |
| 3 | M0x02 Reconnaissance | Q0x02<br>Ex020 OSInt<br>Ex030 DNS Reconnaissance | 17 Sep 2020<br>24 Sep 2020<br>24 Sep 2020 |
| 4 | M0x03 Networking Introduction<br>M0x04 Service Discovery and Interrogation | Q0x03<br>Q0x04<br>Ex040 Wireshark<br>Ex050 Nmap | 24 Sep 2020<br>24 Sep 2020<br>1 Oct 2020<br>1 Oct 2020 |
| 5 | M0x05 Program Exploitation and Metasploit | Q0x05<br>Ex060 OpenVAS | 30 Sep 2020<br>7 Oct 2020 |
| 6 | M0x06 Linux and Passwords | Q0x06<br>Ex070 Brian's Service | 7 Oct 2020<br>14 Oct 2020 |
| 7 | M0x07 Exploiting Windows Credentials | Q0x07<br>Ex080 Through the Gate<br>Ex090 PowerUp<br>Ex0a0 HashTag | 13 Oct 2020<br>20 Oct 2020<br>20 Oct 2020<br>20 Oct 2020 |

| Week | Topic | Assignment | Due Date |
|---|---|---|---|
| 8 | M0x08 Effective Exploitation Antivirus and Pivoting | Q0x08<br>Ex0b0 Netcat Pivot<br>Ex0c0 Lifting the Veil | 20 Oct 2020<br>27 Oct 2020<br>27 Oct 2020 |
| 9 | M0x09 Windows Administration and Configuration | Q0x09<br>Ex0d0 Patronum is Breached | 26 Oct 2020<br>2 Nov 2020 |
| 10 | M0x0a Attacking Layer 2 Here in the Middle of All Things | Q0x0a<br>Ex0e0 SSLStrip | 2 Nov 2020<br>9 Nov 2020 |
| 11 | M0x0b More Windows Exploitation and Post Exploitation<br>M0x0c Kernel and Processor Bugs | Q0x0b<br>Q0x0c<br>Ex0f0 Recent Linux Vuln.s<br>Ex100 Responder | 6 Nov 2020<br>6 Nov 2020<br>13 Nov 2020<br>13 Nov 2020 |
| 12 | M0x0d HTTP, Web Browsers, Web Proxies, XSS | Q0x0d<br>Ex110 Beef Hooking | 12 Nov 2020<br>19 Nov 2020 |
| 13 | M0x0e XSS, CSRF, SSRF, Path Normalization | Q0x0e<br>Ex120 Brian's Project | 18 Nov 2020<br>25 Nov 2020 |
| 14 | M0x0f Where We're Going, We Don't Need Wires | Q0x0f<br>Ex130 EAP Wireless | 24 Nov 2020<br>1 Dec 2020 |
| 15 | M0x10 Going Mobile | Q0x10<br>Ex140 Mobile App Test | 1 Dec 2020<br>8 Dec 2020 |
| 16 | M0x11 Cloud and IoT Pen Testing<br>M0x12 Exploiting Physical and Mental Access | Q0x11<br>Q0x12<br>Ex150 DC Has Fallen<br>Ex160 F4rmC0rp Pentest Report | 9 Dec 2020<br>9 Dec 2020<br>9 Dec 2020<br>9 Dec 2020 |

Disclaimer: This syllabus represents my current plans and objectives.  As we go through the semester, those plans may need to change to enhance the class learning opportunity.  Such changes, communicated clearly, are not unusual and should be expected.

Last update: 8/31/2020