Date of last update: 8/17/2015

ETHICAL HACKING

CIS 102 (CRN: 22478)
Fall 2015
Fisk, Thursdays 6:00-9:50 in ATC 205,
Office hours: Thursday 5:00-6:00 PM in ATC 203b,
and all other times via e-mail

COURSE DESCRIPTION

Students will scan, test, hack and secure systems. Implement perimeter defenses, scan and attack virtual networks. Other topics include intrusion detection, social engineering, footprinting, DDoS attacks, buffer overflows, SQL injection, privilege escalation, trojans, backdoors and wireless hacking. Legal restrictions and ethical guidelines emphasized. This course also helps prepare students to pass the Certified Ethical Hacker (C|EH) exam.

PREREQUISITE SKILLS

Advisory: Computer Information Systems 66 and CIS 108.

INSTRUCTOR INFORMATION:

Instructor: Leonard (Len) Fisk

Office Hours: from 5:00-6:00 PM, every Thursday, in ATC 203b, and almost all other times during the week - via e-mail (see below for address). I will hold office hours beginning on 9/24/2015 (I have surgery scheduled for the week of 10/8, and will not be present for my office hour that day, although I will have scheduled classroom activities in ATC 205 during the regularly scheduled class time).

Office Location: ATC 203b.

E-mail address: **mailto:fisklen@fhda.edu**

Website: I will post up-to-date information regarding this course at Jones & Bartlett's site for this course. In particular, I will post updates and changes to this syllabus at that site which, like the campus "Catalyst" system, is Moodle-based. You will be accessing this site via https://moodle.jblcourses.com/ . Various other links may be added at this class site, and assignments will be uploaded to it as well. It will be the center point for communications about the course. Effectively, the fee for your "textbook" will also be included in the fee to buy access to this site.

ATTENDANCE POLICY

Students are required to attend all class meetings every Thursday, 6:00-9:50 PM in AT 205.

Drop Policy: By **midnight**, Wednesday of THE SECOND WEEK OF THE COURSE (9/30) you must have purchased the text and the lab access, and have logged into the Jones and Bartlett site that provides the Moodle "main office" for the class and the critically important virtual laboratory and registered there. **By**

midnight on Thursday of the second week (10/1), you will also have completed and turned in (to J&B Moodle) all of the Week 1 Lab assignment posted on the website (we will ignore the "challenge" assignments). (This due day is one day later than I will expect for all remaining Lab assignments, which will be due at midnight Wednesday of each week.)

Failure to do so may result in a DROP.

Students who wish to drop this class must follow the De Anza College drop procedures. The Drop calendar deadlines can be found at https://www.deanza.edu/calendar. Do not assume you will be automatically dropped from this course. If you intend to drop the course, you must drop yourself!

OBJECTIVES

Upon completion of this course, you will be able to use a personal computer and understand the following personal computer objectives.

A. Explore ethical hacking basics
B. Explore cryptography
C. Investigate reconnaissance: Information gathering for the ethical hacker
D. Explore scanning and enumeration
E. Explore hacking through the network: Sniffers and evasion
F. Investigate how to attack a computer system
G. Explore low tech hacking techniques
H. Investigate web-based hacking
I. Explore wireless network hacking
J. Investigate trojans and other attacks
K. Perform penetration testing

STUDENT LEARNING OUTCOMES FOR THIS COURSE:

Demonstrate the ability to attack and defend systems and networks.

REQUIRED COURSE MATERIALS

Textbook: Hacker Techniques, Tools, and Incident Handling, Second Edition, with special virtual lab access, by Sean-Philip Oriyano.

Purchasing text and lab materials: You can purchase access to the virtual labs required for the course in person, at the De Anza bookstore, where it will be bundled with either a "hard" or "e-copy" of the textbook. If you would prefer a hard-copy version of the textbook, the bookstore will have a number of copies for purchase. Please note that access to the virtual lab is unique for each person and cannot be shared: i.e., the code you purchase will belong to you and to you alone.

The bookstore will sell you a packet with either **e-book**:
Hacker Techniques, Tools, and Incident Handling EVB/ VLA/ VLE 2.0 (ISBN #978-1-2840651-3-8), plus lab access, or
hard copy text:
Hacker Techniques, Tools, and Incident Handling EVB/ VLA/ VLE 2.0 (ISBN #978-1-2840651-4-5), plus lab access.

Either will provide you with the access code you need for individual access to the Jones & Bartlett virtual lab site (plus the e-book if you have chosen that option). **Please note that the specific code needed to access the virtual laboratory MUST be purchased, otherwise you cannot participate in the class.**

If you already have a copy of the second edition of the textbook and wish to buy lab access separately, you can contact the Jones & Bartlett sales representative via e-mail and request to do so. The sales representative is Jennifer Kaufman (mailto:JKaufman@jblearning.com).

To redeem your access code to the JBL Virtual Security Cloud Lab, do the following:

1. Go to www.jblcourses.com (NOT moodle.jblcourses.com)
2. Click on "**Redeem an Access Code**" on upper right side of screen
3. Enter the 8 digit lab access code you purchased and the four digit code for this specific section of the class - **XXXX**. Then click **Submit**.
4. Once your access code has been validated, click on the blue **New User Sign Up** link underneath the yellow submit button. You must do the new user "sign-up" before you can enter a username and password.
5. In the **New User** Box type in
    a. **Username** - must contain alphabetical letters, numbers, a hyphen, underscore, period, or @ sign (DON'T FORGET THIS, AS IT ALLOWS YOU INTO THE LAB!).
    b. **Password** – must contain at least 8 characters, and include one digit, one lower case letter, one upper case letter, and one non-alphanumeric symbol such as"#". For instance, ABCabc1# sign (AGAIN, DON'T FORGET THIS, AS IT ALLOWS YOU INTO THE LAB!).
    c. **First Name/Last Name** in appropriate box (please use the name you used to enroll in the class at De Anza, otherwise I cannot give you credit)
    d. **Email**
    e. Click **submit**
    f. You have successfully entered a link to your course on the next screen.
    g. Click on the course name to enter the course.

If your code doesn't work or you are unable register please contact our tech support specific for the virtual labs and lecture presentations at 1-866-601-4525 or www.jblcourses.com/techsupport.

J&B Moodle and Virtual Lab Site: As noted above, the J&B site will be used for completing all class assignments. The J&B site also provides an interesting feature that allows you to create discussion forums and to reach other students to form study groups, etc., as well as a chat-room to use in addition to regular e-mail. I am available at most times during the week via regular e-mail (I have my iPhone nearby at almost all times).

After you redeem your access code to gain full access to the lab, and to Moodle, the fastest way to the J&B Moodle site for this course will be the URL https://moodle.jblcourses.com.

REQUIRED COMPUTER COMPONENTS AND AVAILABILITY

You will need a **broadband Internet connection** (not dial up!) if you wish to work at home.

Hardware Requirements: A PC computer is required to run the Jones and Bartlett software to access the labs for this course. If you do not own a PC, you may use the De Anza lab computers in ATC 203. In addition, some students may wish to install some of the tools that are installed in the Jones & Bartlett virtual environment on their own machines, although this is not required. (Some extra-credit will be available for installing and demonstrating such software, although you will be encouraged to exercise great caution in using it. Setting up a virtual environment like the lab, in which both the hacking machine and the targets are virtual, is a very safe way to do it; it spares you the risk of being blacklisted by ISPs.)

Software: The only software required for this class is a Firefox web browser (preferably). The Jones and Bartlett access codes will allow access to the Jones & Bartlett virtual environment that accompanies the Hacker Techniques, Tools, and Incident Handling e-book, and all of the software used will be located on their servers. One exception is the necessary installation of the (free) Citrix ICA Client, which you will be prompted to do when you first access the virtual lab from the J&B Moodle site.

Computers in the De Anza Labs: If you do not have a broadband-connected computer, you can use our CIS lab computers. For CIS computer lab hours, see http://www.deanza.edu/buscs/lab/hours.html.

WAYS TO EARN POINTS TOWARD A GRADE

This course will require weekly, hands-on lab assignments in which you will be working to either hack or defend a virtual system. You will take 5 "surprise" quizzes and a final exam. Finally, in addition to these graded activities, you have the opportunity to earn additional "extra credit" points by researching and presenting additional information about tools, hacks, and security issues in the press and on the web to the class. The maximum possible points are summarized in the table shown below.

Source	number	points	total
Laboratory assignments	10	10	100
Unit Quizzes	10	9	90
Final	1	100	100
Extra Credit (10/8 & 10/15)	1	20	20
Extra Credit (other dates)	4	10	40
Total points possible (290 w/o Extra Credit):			350

SUBMITTING WEEKLY LABORATORY ASSIGNMENTS

This course uses a virtual hacking environment ("sandbox") provided by Jones and Bartlett to accompany the Hacker Techniques, Tools, and Incident Handling textbook, and all of the labs will require access to this environment. All course information, including assignments, course deadlines, etc. will be made available to you online via the Jones and Bartlett course web site. When you enter the Jones and Bartlett online course site, you will find the assignments that you will be asked to complete, listed within each class week of the quarter. The actual course schedule and due dates for exams and assignments are subject to change and will be posted in the schedule in this course syllabus on the J&B Moodle site. Each week's lab assignment will entail using the virtual environment and doing a number of screen captures, which you will use to document your actions there. You will then paste the captured screen images into your narrative, answering the questions and describing what you did, and post the resulting document to satisfy the assignment at the class Moodle site.

Late Work

Work will be accepted after the due date according to the following rules: Ten percent (10%) of the maximum possible points will be subtracted for each working day (24 hours) the assignment is late. This will continue until one week (5 working days) has elapsed, when the points total will drop to zero, and no credit will be earned. If you have clear and compelling reasons for not getting an assignment in on time, please let me know on or before the day it is due, and I will arrange an extension for you.

Extra Credit Assignments:

Various extra credit assignments will be posted via the J&B site, and will be on topics that you choose and seek approval for before doing. Like all of the other assigned work, it will be turned in via the Jones & Bartlett site. Unlike lab work, **extra credit work will be posted on topics that are truly substantive and that target specific security issues pertinent to this course.** All extra credits will involve:

(1) The demonstration of, and/or installation of, and/or use of, and/or analysis of, major tools used in hacking (like Wireshark, Metasploit, Kalli Linux, etc.), or
(2) The analysis and demonstration of the accomplishment of significant tasks on sites such as hackthissite.org or enigmagroup.org/ (e.g., accomplishment of two "realistic" hacks on HackThisSite), or
(3) The reporting and technical analysis of major events in the digital security realm (analysis of a major new exploit),

Any extra credit work involving the installation and analysis of tools, and accomplishments at the aforementioned websites **will require the prior approval of Professor Fisk** and will be posted to the Moodle site in order to earn extra credit points. (If it is accepted for credit, Dr. Fisk will make your report available to the full class.)

Your Extra Credit must be submitted in the form of a single, stand-along document that will be both interesting and instructive and can be posted in a format that is readable by all students in the class (i.e., PDF, .DOC, or .PPT). It is subject to the same <1 MB constraint that you have for your Labs. I will accept only the first eight approved Extra Credit submission per week (first come-first served), and you cannot submit any more than one per week. Weeks begin at midnight on Sunday night. Week 1 begins on Midnight September 20.

ATTENDANCE/PARTICIPATION

You must attend lectures and participate in class discussions in order to receive full credit for all Laboratory assignments. Roll will be taken.

TESTING/GRADING POLICIES/FINAL GRADES

To pass this course, you must complete ALL assignments plus ALL Exams with the minimum scores shown below**.** Weekly deadlines for all assignment will be posted via Catalyst.

Exam Grading Scale:

A+	96%-100%
A	93% -95%
A-	90%-92%
B+	87%-89%

B	83%-86%
B-	80%-82%
C+	77%-79%
C	70%-76%
D+	67%-69%
D	63%-66%
F	0%-62%

Final Grade Mix:

The following percentages reflect how the final grade will be determined:

Lab Assignments	29.4%
Quizzes	26.5%
Final Exam	29.4%
Extra Credit	14.7%
	=====
Total =	100%

ACADEMIC INTEGRITY:

Students who submit work of others as their own or cheat on exams or other assignments will receive a failing grade in the course and will be reported to college authorities.

Disruptive Classroom behavior

Disruptive classroom behavior may include (but is not limited to) the following: talking when it does not relate to the discussion topic, sleeping, reading other material (e.g. newspapers, magazines, textbooks, from other classes), snoring loudly, eating or drinking, monopolizing discussion time, refusing to participate in classroom activities, leaving cell phones and pagers on, riding motorcycles on desks, texting, making rude biological noises, and engaging in any other activity not related to the classroom activity. Students who engage in disruptive behavior will be approached by the instructor. If the disruptive behavior continues, students may be asked to leave the classroom and/or eventually be dropped from the course.

Note to students with disabilities

If you have a disability-related need for reasonable academic accommodations or services in this course, provide your instructor with a Test Accommodation Verification Form (also known as a TAV form) from Disability Support Services (DSS) or the Educational Diagnostic Center (EDC). Students are expected to give a five day notice of the need for accommodations. Students with disabilities can obtain a TAV form from their DSS counselor (864-8753 DSS main number) or EDC advisor (864-8839 EDC main number).

TECHNICAL DIFFICULTIES

If you have technical problems with the Jones and Bartlett virtual laboratory, please contact Jones and Bartlett Technical Support directly at msupport@jblearning.com or, if the problem stems from a client software glitch in your personal computer, complete your course work using the computers in the CIS lab.

SCHEDULE/CALENDAR

Wk	Date	Topic	News/Extra Credit	Reading	Test (1)/ Quiz (10)	Due
1	9/24/2015	Intro, syllabus, hacking & OSI-TCP/IP	No	Chpt 1&2		
2	10/1/2015	Cryptography, symmetric, asymmetric	Yes	Chpt 3	Quiz 1	Lab 1
3	10/8/2015	Footprinting and social engineering (Video lecture due to surgery)	Yes	Chpt 5&13	Quiz 2	Lab 2
4	10/15/2015	Port scanning, enumeration & syst. Hacking (More video lecture)	Yes	Chpt 6&7	Quiz 3	Lab 3
5	10/22/2015	Web & database attacks	Yes	Chpt 9	Quiz 4	Lab 4
6	10/29/2015	Malware, worms & viruses	Yes	Chpt 10	Quiz 5	Lab 5
7	11/5/2015	Network analysis, Linux & pen testing	Yes	Chpt 11&12	Quiz 6	Lab 6
8	11/12/2015	Wireless vulnerabilities	Yes	Chpt 8	Quiz 7	Lab 7
9	11/19/2015	Physical Security, Incident Response	Yes	Chpt 4 & 14	Quiz 8	Lab 8
	11/26/2015	Thanksgiving				
10	12/3/2015	Defensive Technologies, and Incident Response –	Yes	Chpt. 15	Quiz 9	Lab 9
11	12/10/2015	FINAL - (120 min) 6:15-8:15 PM	No		FINAL	Lab 10