Date of last update: 3/9/2015

ETHICAL HACKING

CIS 102 (CRN: 43529)
Spring, 2015
*Fisk, "Online Course," materials at **moodle.jblcourses.com**,*
Office hours: 5:00-6:30 PM every Tuesday and Wednesday.

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, foot-printing, 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 (computer networking) and CIS 108 (PC security basics).

About Professor Fisk:

Name: Leonard (Len) Fisk, Ph.D., CISSP

In-Person Office Hours: from 5:00-6:30 PM, in ATC 203b on 4/15 and 6/24.
Remote Video Office Hours: from 5:00-6:30 PM, every Tuesday and Wednesday that I am not holding in-person office hours in ATC, via http://www.cccconfer.org (instructions appear below).
Remote E-Mail Office Hours: you may e-mail me any time day or night at fisklen@fhda.edu. I respond quickly, as I use my cell phone for the purpose.

In-person Office Location: ATC 203b.

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

Remote Video Office Hours: The **cccconfer.org** website is a videoconferencing site and you need a computer with microphone and speakers, plus, if you wish, a webcam. Or, you can use an iPhone, iPad, or Android device if you download the mobile app "Blackboard Collaborate": you will find instructions at http://www.cccconfer.org/trainingCenter/goMobile.aspx.

Other Points of Communication: 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. You will pay a fee to buy access to this site, which links to the required virtual laboratory.

Any other critical or significant events will be announced via e-mail sent to you.

Attendance Policy

There is no everyday attendance policy because this is an "on-line" course. However, **you MUST attend the on-campus final to receive credit for the course**, which means that you must keep up with the classwork sufficiently well to be certain that you have completed all of the materials in time to take the final. The required in-person final will be held on June 25 from 6:00-7:50 PM, in ATC 203 on the De Anza campus. **You will be required to present legal picture identification to take the final exam**, which will, in turn, be required to receive a grade in the course. If you cannot complete the course or take the final, you must present clear and compelling reasons in order to earn an Incomplete rather than a failing grade and then be able to take a rescheduled final.

I **strongly recommend** that you make an effort to meet me during my scheduled office hours on April 15. I also strongly recommend that you meet with me via CCCConfer.org. I find that face-to-face meetings help minimize misunderstandings, and video connections can be better than e-mails..

Drop Policy:

By midnight, Saturday of the second week of the class (**4/18/2015**), **you must have (1) purchased a textbook, (2) acquired lab access, and (3) have logged into the Jones and Bartlett site** that provides the Moodle "main office" for the class and the critically important virtual laboratory **and signed in to this particular Moodle class**. **FAILURE TO DO SO WILL CLASSIFY YOU AS A "NO SHOW" STUDENT AND YOU WILL BE DROPPED**.

By midnight, Saturday of the second week of class (**4/18/2015**), **you must also complete** and turned in (to J&B Moodle) your **Week 1 Lab assignment report**, using the form posted on the website (we will ignore the "challenge" assignments). 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 have met the following objectives. You will have:

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

Student Learning Outcomes:

Students who complete the course will:

Demonstrate the ability to attack and defend a network.

Required Course Materials:

Textbook: Hacker Techniques, Tools, and Incident Handling, Second Edition, with special virtual lab access, by Sean-Philip Oriyano. (Please note that the textbook is the 2nd Edition, which has different chapters than the 1st edition.)

Purchasing text materials and lab access: You must purchase access to the virtual labs required for the course, and the access codes that will gain you access will be available only at the De Anza bookstore (http://books.deanza.edu/home.aspx). The bookstore will have both "e-books" and "hard copies" of the book for sale as well as access codes that will buy you access to the virtual laboratory for the course. Please note that access to the virtual lab must be purchased separately for each person enrolled in the course, and cannot be shared: i.e., the code you purchase will belong to you and to you alone. **To redeem the access code** to the JBL Virtual Security Cloud Lab that you purchased at the De Anza Bookstore, 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 **eight 8 digit lab access code** you purchased, and the **four digit code for this specific course**, which will be mailed to all who enroll for the course. 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
    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.

Get it done well before April 18th, or you will find yourself disenrolled.

J&B Moodle and Virtual Lab Site: As noted above, the J&B Moodle site will be used for completing all class assignments and the everyday business of the class. 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 the lab, and, perhaps, an additional access code to download your text if you purchased an e-book, the fastest way to the J&B Moodle site for this course and access to the laboratory will be the URL **https://moodle.jblcourses.com**.

Required Computer Components and Internet Connection:

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 "pen-testing" tools that are installed in the Jones & Bartlett virtual environment on their own machines, although this is certainly 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 (at ToolWire) 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. This installation is automatic, requiring only your consent.

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

How to Earn Points Toward Your Grade:

This course will require completion of 10 hands-on lab assignments in which you will be working to either hack or defend a virtual system. You will take 10 unit 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 by submitting them via an upload to the "extra credit" item listed in each week's materials. These extra credit items will be posted in Moodle for the class to view. The maximum possible points are summarized in the table shown below.

Source	number	points	total
Laboratory assignments	10	10	100
Unit/Week Quizzes	10	10	100
Final	1	100	100
Extra Credit/Security News	5	5	25
Total points possible: (without/with – extra credit)			300/325

The On-campus Final:

You will be required to take your final on a computer at the ATC (Advanced Technology Center), where you must have obtained an account that allows you access to the ATC workstations before the final. Therefore, it is important that you obtain usernames and passwords for both the campus workstation network at ATC, and for moodle.jblcourses.com before the final.

Submitting Laboratory Assignments and the sequencing of activities for the course:

This course uses a virtual hacking environment 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. You can access this site from anyplace you have Internet access. 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 "unit," which corresponds to a particular week of the quarter. The date and time of office hours, and the final are fixed. The due dates for the unit quizzes and Laboratory assignments are not fixed, and can be completed any time, although they must be completed in a set sequence, and you are strongly advised to adhere to a one-unit-per-week schedule. Each unit's lab assignment will require you to use the virtual environment to follow the laboratory instructions. You will fill out a laboratory report in MS Word format by answering a set of questions for the specific unit (the form is posted with the unit in Moodle) and do a number of screen captures and reports in various formats. You will capture a screen shot of the first page of each required report (jpg is probably the best because it compresses well), and then paste the various required screen shots under the appropriate heading within the Word document Lab Report. You will then upload the resulting document to Moodle to satisfy the assignment. You will find additional information about how to prepare and upload the lab reports in the weekly lecture notes, which contain an audio narrative, plus some clear hints about how to manage to make each upload fit the 1 MB upload size limit and still have the requisite screen captures in it.

Late Lab Work

Because you are taking this as an online course, **you may work ahead of the schedule that is posted** in the "Unit Sequence" table shown above, and repeated in the "Schedule/Calendar" at the end of this syllabus. You must not fall behind this schedule, as the **labs will not be accepted any later than the official unit end date/time, and unit quizzes cannot be taken any later than the unit end date (the Final included).** If you become ill, or have another reason to miss a due date, you must contact Professor Fisk and submit evidence of the reasons for missing the deadline. If your reasons are truly "serious and compelling," Professor Fisk will arrange a makeup for you. If you fail to take quizzes, or if you fail to submit Lab reports and do not have clear evidence of a serious and compelling reason to do so, these scores will be recorded as zeros.

You must not expect that labs will be graded instantaneously. Realistically, you must expect several workdays to intervene between your submission and getting a score posted for the lab. Quizzes, however, will be scored immediately.

The Sequence of Events for Finishing Each Unit of the Curriculum:

Initially, you will find that the Moodle page looks rather empty. The reason is that the successive portions of the course only become visible and available to you as you finish each unit/week in the sequence. There will be 10 units associated with specific chapters in the text and specific Laboratory exercises, as shown in the table below:

Unit Sequence:

Unit/Week	Date	Topic	Reading
1	Lab done by 4/18	Intro, syllabus, hacking & OSI-TCP/IP	Chpt 1&2
2	Lab done by 4/25	Cryptography, symmetric, asymmetric	Chpt 3
3	Lab done by 5/2	Footprinting and social engineering	Chpt 5&13
4	Lab done by 5/9	Port scanning, enumeration & syst. hacking	Chpt 6&7
5	Lab done by 5/16	Web & database attacks	Chpt 9
6	Lab done by 5/23	Malware, worms & viruses	Chpt 10
7	Lab done by 5/30	Network analysis, Linux & pen testing	Chpt 11&12
8	Lab done by 6/6	Wireless vulnerabilities	Chpt 8
9	Lab done by 6/13	Physical Security, Incident Response	Chpt 4 & 14
10	Lab done by 6/20	Defensive Technologies, and Incident Response –	Chpt. 15
11	Week of 6/22	**FINAL - (120 min) 6:30-8:20 PM, Wed., 6/24, ATC 203**	

For each unit, the materials must be accessed and completed in a required order: The Lab must be completed before the unit mastery quiz can be taken. Because the grading of each of the labs may take a workday or two before it is complete, be sure to get the labs posted as early as possible. Practice quizzes have been provided (these are T/F questions) to help you determine if you are ready to take the unit quiz. You will be permitted only one shot at each unit quiz. Once you complete the quiz, you will be allowed to continue on to the next unit immediately. Again, please note that you will get only one try at the quiz. **All the graded activities of the first unit must be completed before midnight, 4/18.**

In general, the sequence you will follow for each unit is as follows:

1. Read the chapter(s) for the unit ; watch the lecture, with audio narrative for each slide of the unit;
2. **Do the virtual lab for the unit and post the lab report to Moodle as a single DOC document**;
3. Take the "self-test" practice quiz for the unit (it is scored, but will not count toward your grade);
4. **Take the unit quiz for the unit after the lab report is graded and posted**. Until the Lab report is graded, the unit quiz will remain hidden..

The bold faced items on the numbered list above are the only items that must be done in sequence, and the only activities you are required to do. As you complete each unit quiz, the next two units will become visible on the Moodle page for the class.

Quizzes:

The unit quizzes will be 20 question, multiple-choice, and you will be given 15 minutes to complete each one of them. Each week's/unit's quiz will appear only when you have posted your Laboratory report for that week/unit. You will get only one try for the quiz, so be certain you understand the material well before taking it. The score you get will be your recorded entry on the grade sheet.

Late Assignments:

Extra Credit Assignments:

Various extra credit assignments will be made available via the J&B site. 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 the reporting and analysis of either major events in the digital security realm, or the demonstration and analysis of major tools used in hacking (like Wireshark, Metasploit, Kalli Linux, etc.), or the analysis of the accomplishment of major tasks on sites such as hackthissite.org or http://www.enigmagroup.org/ (e.g., accomplishment of two "realistic" hacks on HackThisSite). 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.)

Attendance:

You must attend the Final and present photo identification in order to receive a passing grade in this class.

Testing/Grading Policy/Final Grades:

To pass this course, your total score will contribute to your final grade as shown below. If you have post extra credit assignments, they will contribute true extra credit points toward raising your grade. With a maximum of 300 points possible, adding as many as 25 extra credit points can potentially lift your grade two categories in the table shown below.

Course Grading Scale:

A+	96%-100%
A	93% -95.9%
A-	90%-92.9%
B+	87%-89.%
B	83%-86.9%
B-	80%-82.9%
C+	77%-79.9%
C	70%-76.9%
D+	65%-69.9%
D	60%-64.9%
F	0%-59.9%

ACADEMIC INTEGRITY:

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

Note to students with disabilities

If you have a disability-related need for reasonable academic accommodations or services in this course, particularly for the taking of tests, 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).

Because the content lectures are based on Powerpoint slides, some with graphics, all with audio tracks, and because the labs are presented via complex GUI interfaces with many texted elements (they are the "real thing": Linux and Windows interfaces with many windows open that require to use the systems), and if you are aurally or visually impaired, you may need assistance in the form of an interpreter or reader.

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

Unit/ Week	Date	Topic	Reading	Required Meeting in ATC	Week of	Office Hr. location, T/W, 4:30-6:00
1	**Lab by 4/18**	Intro, syllabus, hacking & OSI-TCP/IP	Chpt 1&2		**April 6**	CCCConfer(7th)/ CCCConfer(8th)/
2	**Lab by 4/25**	Cryptography, symmetric, asymmetric	Chpt 3		**April 13**	CCCCConfer(14h)/ **ATC (15th)**
3	**Lab by 5/2**	Footprinting and social engineering	Chpt 5&13		**April 20**	CCCConfer(21st)/absent-surgery
4	**Lab by 5/9**	Port scanning, enumeration & syst. hacking	Chpt 6&7		**April 27**	CCCCConfer(28th)/CCCCConfer(29th)
5	**Lab by 5/16**	Web & database attacks	Chpt 9		**May 4**	CCCConfer(5th)/CCCCConfer(6th)
6	**Lab by 5/23**	Malware, worms & viruses	Chpt 10		**May 11**	CCCConfer(12th)/CCCCConfer(13th)
7	**Lab by 5/30**	Network analysis, Linux & pen testing	Chpt 11&12		**May 18**	CCCConfer(19th)/CCCCConfer(20th)
8	**Lab by 6/6**	Wireless vulnerabilities	Chpt 8		**May 25**	CCCConfer(26th)/CCCConfer(27th)
9	**Lab by 6/13**	Physical Security, Incident Response	Chpt 4 & 14		**June 1**	CCCConfer(2nd)/CCCConfer(3rd)
10	**Lab by 6/20**	Defens. Technologies & Incident Response	Chpt. 15		**June 8**	CCCConfer(9th)/CCCConfer(10th)
11		**Study for final!!**			**June 15**	CCCConfer(16th)/CCCConfer(17th)
12	6/24/2015	**FINAL - (120 min) 6:30-8:20 PM in ATC 203**		**6:30PM, Thu., 6/24**	**June 22**	CCCConfer(23rd)/**ATC (24th)**