Date of last update: 6/21/2015

ETHICAL HACKING

CISD102.61Z (CRN: 11528)
Summer, 2015
*Fisk, "Hybrid Course," materials at **moodle.jblcourses.com**,*
Class times: 6:00-8:50 Thursdays, 7/2, 7/9, 7/23, 7/30, 8/6
Office hours: 5:00-5:55 PM Thursdays, 7/2, 7/9, 7/23, 7/30, 8/6
other hours, at a distance, by arrangement

Course Description:

This is an accelerated "hybrid" course with both online and face-to-face components in which you will be given twice weekly Laboratory assignments and weekly quizzes to complete. The course is compressed into a six week period and will require a heavy commitment in time. 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 5:00-5:55 PM, in ATC 203b on 7/2, 7/9, 7/23, 7/30 and 8/6. Other times on request.
Remote E-Mail Office Hours: you may e-mail me any time day or night at fisklen@fhda.edu. I generally respond quickly, as I use my cell phone for the purpose.
E-mail address: **fisklen@fhda.edu**
Remote Chat Room Hours: The Moodle website includes a bulleted "chat-room" link (at the top of the Moodle CIS 102 class site). If you wish to arrange a particular time to meet in this venue, I will be more than happy to spend time there. I will be signed on to that chat room during my normal office hour times on campus (5:00-5:55 PM on 7/2, 7/9, 7/23, 7/30 and 8/6).

Other Points of Communication: I will post up-to-date information regarding this course at Jones & Bartlett's Moodle 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. Both Lab Access and textbook are available in the De Anza bookstore, and can be purchased from them at a distance (see http://books.deanza.edu/home.aspx).

Any other critical or significant events will be announced via e-mail sent to directly your registered e-mail address.

Attendance Policy

Attendance will be required at each of the scheduled, on-campus meeting times (there are only five of them, including the Final), and you must attend them to receive credit for 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.

Drop Policy:

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! If you do wish to drop, the process is described at http://www.deanza.edu/registration/add-drop.html.

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**, **7115**. 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 YOUR USERNAME, 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 YOUR PASSWORD, 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.

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 (faster is better!) if you wish to work at home, especially if you wish to download lectures, which are roughly 150 MB..

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, although they are not equipped with headphones or speakers and audio-augmented lectures are available to download.

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) and a word-processing program that is capable of opening and saving document s in an MS Word format. You may also find that you require a snipping tool, or a photo editing tool like GIMP in order to reduce images to a small enough storage imprint to stay under the 1 MB upload size limit.

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 textbook (both e-book and hardcopy versions), and all of the software used will be located on their servers. The one exception is the necessary installation of the (free) **Citrix ICA Client**, which you will be prompted to permit when you first access the virtual lab from the J&B Moodle site. This installation is automatic, requiring only your consent, and is essential for you to do the laboratories.

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 penetrate or defend a virtual system. You will take 10 unit quizzes (these will be clustered into three quizzes, each of which combines a number of units) 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. (More on "Extra Credit" later in this document.) The maximum possible points are summarized in the table shown below.

Source	number	points	total
Laboratory assignments	10	20	200
40 point quiz	1	40	40
60 point quizzes	2	60	120
80 point quiz	1	80	80
Final	1	200	200
Extra Credit/Security News	5	20	100
Total points possible: (without/with extra credit)			640/740

Quizzes and Final:

You will be required to take all of the quizzes and the 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 first class. **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 first class meeting**.

Submitting Weekly 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 posted within each of ten "units." Each unit's lab assignment will require you to use the virtual environment, which will provide detailed laboratory instructions to follow. You will fill out a pre-formatted 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 paste a number of screen captures and reports into the Word document. You will capture a screen shot of the first page of each required report (jpg is probably the best image format 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 complete and upload your labs for this class" on the Jones and Bartlett Moodle site (moodle.jbl courses.com).** This is in the form of a PowerPoint file that contains an audio narrative, plus a number of clear hints about how to manage to make each upload fit the 1 MB upload size limit and still have the requisite number of readable screen captures in it.

The First Lab

By **midnight, Saturday of the first week of class (7/4/2015)**, 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 get "signed in" to this particular Moodle class. **The first Lab assignment is due at this time also,** but the assignment will be accepted up to one week after the initial due date. Normally, this comes with a penalty (see "Late Work", below), but the penalty will be waived for this first Lab assignment..

As noted above, to receive credit for the first Lab, you must submit it to Moodle by midnight, Saturday of the second week of class (7/11/2015). You will use the Lab report form provided on the website (we will ignore the "challenge" assignments).

Late Lab Assignments

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 Lab 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 if possible.

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.

Unit Sequence Table:

Unit	Lecture / LabTopic	Reading
1	Intro, syllabus, hacking & OSI/TCP-IP / Assessing & Securing Systems on a WAN	Chpt 1&2
2	Cryptography, symmetric, asymmetric / Applying Encryption & Hashing Algorithms for Secure Communications	Chpt 3
3	Footprinting and social engineering / Data Gathering and Footprinting on a Targeted Website	Chpt 5&13
4	Port scanning, enumeration & syst. Hacking / Using Ethical Hacking Techniques to Exploit a Vulnerable Workstation	Chpt 6&7
5	Web & database attacks / Attacking a Vulnerable Web Application and Database	Chpt 9
6	Malware, worms & viruses / Identifying and Removing Malware on a Windows System	Chpt 10
7	Network analysis, Linux & pen testing / Analyzing Network Traffic to Create a Baseline Definition	Chpt 11&12
8	Wireless vulnerabilities / Auditing a Wireless Network and Planning for a Secure WLAN Implementation	Chpt 8
9	Physical Security, Incident Response / Investigating and Responding to Security Incidents	Chpt 4 & 14
10	Defensive Technologies / Securing the Network with an Intrusion Detection System (IDS)	Chpt. 15
	FINAL - (120 min) 6:00-7:50 PM, Thursday., 8/6, ATC 203	

Practice quizzes have been provided (these are constructed with T/F questions) with each unit to help you determine if you are prepared to take the next quiz. You can take practice quizzes as often as you wish.

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

1. Read the chapter(s) for the unit and watch the lecture, with audio narrative for the unit;
2. Do the virtual lab for the unit and post the lab report to Moodle as a single DOC document (<1 MB);
3. Take the "self-test" practice quiz for the unit (it is scored, but will not count toward your grade);
4. Be prepared to take the unit quiz for the unit at the scheduled time in class.

Quizzes:

The Quizzes will be roughly 20 questions per unit and multiple-choice, but the quizzes for most units will be combined with others because this course is compressed down from 10 weeks. You will be given roughly 45 seconds per item to complete the quiz. You will get only one try at the quiz, so be certain you understand the material well before coming to class after posting the Lab for that unit. The score you get will become your recorded entry on the grade sheet.

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 reporting and technical analysis of major events in the digital security realm (a major new exploit), or

(2) 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
(3) the analysis and demonstration of the accomplishment of significant 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.)

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 June 28.

Attendance:

You must attend all five class meetings in order to receive credit for this course. If you are unable to attend one or more classes, please provide evidence of a serious and compelling reason in order to arrange an alternative solution.

Testing/Grading Policy/Final Grades:

To pass this course, your total score will contribute to your final grade as shown below. If you have posted 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 online content lectures are based on Powerpoint slides, some with graphics, most with audio tracks, and because the labs are presented via complex GUI interfaces with many texted elements (they are the "real thing" in the form of Linux and Windows interfaces with many windows open that require you to carry out systems management tasks), if you are aurally or visually impaired, you will probably 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

Week	Unit	Meeting	Topic	Reading	Lab due date	Quiz/Units covered/# questions / *minutes*
1	1	7/2 - 6:00-8:50 in ATC	Intro, syllabus, hacking & OSI-TCP/IP	Chpt 1 & 2	Lab 01 – midnight 7/4	
2	2 & 3	7/9 - 6:00-8:50 in ATC	Cryptography, symmetric, asymmetric - Footprinting and social engineering	Chpt 3, 5,13	Lab 02 – midnight 7/8 Lab 03 – midnight 7/11	1 / 1&2 / **40** / *30 min*
3	4 & 5	Online, on demand	Port scanning, enumeration & syst. Hacking - Web & database attacks	Chpt 6, 7, 9	Lab 04 – midnight 7/15 Lab 05 – midnight 7/18	2 / 3 ,4 &13 / **60** / *45 min*
4	6, 7 & 8	7/23 - 6:00-8:50 in ATC	Malware, worms & viruses - Network analysis, Linux & pen testing - Wireless vulnerabilities	Chpt 10, 11, 12, 8	Lab 06 – midnight 7/22 Lab 07 – midnight 7/25	3 / 6, 7 &9 / **60** / *45 min*
5	9 & 10	7/30 - 6:00-8:50 in ATC	Physical Security, Incident Response - Defens. Technologies & Incident Response	Chpt 4 & 14, 15	Lab 08 – midnight 7/29 Lab 09 – midnight 8/1	4 / 10, 11, 12 &8 / **80** / *60 min*
6	final	8/6 - 6:00-7:50 in ATC	Study for final!!	Chpt 1 - 14	Lab 10 – midnight 8/5	Final / all / **200** / *110 min*