

ETHICAL HACKING

CIS 102.62Z (CRN: 24252) – Distance Course Fall, 2022

An Online class that Opens in Canvas at 12:01 AM on September 26 (the introductory block will be opened on September 10).

The Final is on December 15, 2022.

Office hours: (1) via “Zoom” on Canvas, and (2) via e-mail.

COURSE STRUCTURE

This is an “asynchronous” online course in which all events other than office hours and tests will be available at asynchronous times. (“Asynchronous” means that you can do all class activities at the times you choose to do them as long as you do not fall outside the boundaries specified for each activity.)

You will be asked to complete 15 laboratory assignments, take 10 Unit Quizzes, and take a Final during the quarter. Additional work will allow you to earn extra credit points.

The course will use the Canvas system, but The full course will not be open in Canvas until the official class start date on September 26, 2022. (I will open the first block of the Canvas course at 12:01 AM Saturday Morning, September 10, 2022). When you do open the course in Canvas after registering, you will find that all but the first block of the course is “grayed out” and inaccessible. I **strongly** recommend that you watch the videos about the class and the labs I have provided in that first block of the Canvas course. I also **strongly** recommend that you obtain a copy of the text before the class begins, and purchase access to the virtual labs also. Before the rest of the course “unlocks” for you, (1) the date must be September 26 or later, and (2) you must have completed the “student contract” in which you verify that you have read and understand the major content of the syllabus. Only then will you have access to the blocks for the 10 Units of the course.

PREREQUISITE SKILLS

Advisory (not required): Computer Information Systems 66 and CIS 108. I would particularly recommend any CIS course about networking or operating systems.

Much of the class involves the use of “command prompt” interfaces on virtual Linux and Windows systems, so some familiarity with the keyboard is necessary. Although no specific skills are required by the labs, a good general knowledge of how computers and the Internet work will definitely help you digest and retain the course content more effectively.

INSTRUCTOR INFORMATION:

Instructor: Leonard (Len) Fisk, Ph.D.

Office Hours:

via scheduled Zoom meetings from 4:00 to 5:00 PM every Tuesday and Thursday from 9/27/2022 through 12/15/2022. These will be treated like traditional office hours, which means that your presence will not be required and that I will be prepared to answer any questions you have. (Occasionally I will talk about things of interest to people who are having troubles with the labs and will announce that I am doing so via e-mail ahead of time.) As with all Zoom meetings, if you drop in, I enjoy it more if you use both audio and video, although audio alone will suffice.

via e-mail: I can be reached almost any time via e-mail (see below for address). Please send e-mail only to the address shown **and use CIS102 in the subject line** to ensure that I will get the mail in a timely manner.

E-mail address: <mailto:fisklen@fhda.edu>

Website: I will post up-to-date information regarding this course at our class Canvas site. I will post updates and changes to this syllabus at that site. You will be accessing this site via MyPortal/Canvas. Various other links and materials will be added at this class site. You will turn in your completed assignments to the Canvas site, all tests will be conducted via this site, and your grades and scored laboratory sheets will be available at this site. It will be the center point for communications about the course.

ATTENDANCE POLICY

The required steps you must take in order for me to consider you as being enrolled in CIS102 is for you to complete the “Student Contract” quiz in Canvas and view both of the introductory lectures before Unit 1. Of course, you must also satisfy the De Anza rules for registration to be added to the class roster.

Drop Policy: By midnight on Friday of the second week (10/7/2022), you will have completed the quiz entitled “Student Contract for CIS 102” posted on the Canvas. Failure to do so may result in a DROP as it means you have not attended class. Your first lab is also due on the Friday of that week (10/7/2022). You have a 5-day reprieve on handing in Labs (i.e., the final deadline for Lab01 is midnight 10/12/2022), although you will forfeit points whenever Labs are late. No Lab will receive credit if handed in after the deadline date. More on this topic appears in “Submitting Weekly Laboratory Assignments/Late Work”, below.

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!

COURSE CONTENT AND OBJECTIVES

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 are emphasized. This course also helps prepare students to pass the Certified Ethical Hacker (CEH) exam.

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

1. Explore ethical hacking basics
2. Explore cryptography
3. Investigate reconnaissance: Information gathering for the ethical hacker
4. Explore scanning and enumeration
5. Explore hacking through the network: Sniffers and evasion
6. Investigate how to attack a computer system
7. Explore low tech hacking techniques
8. Investigate web-based hacking
9. Explore wireless network hacking
10. Investigate trojans and other attacks
11. Perform penetration testing

STUDENT LEARNING OUTCOMES FOR THIS COURSE:

Demonstrate the ability to attack and defend a network.

REQUIRED COURSE MATERIALS

Textbook: All-in-One CEH Certified Ethical Hacker Exam Guide, Fifth Edition, by Matt Walker, McGraw-Hill Education. (ISBN-13: 978-1264269945). This is available at the campus bookstore and also comes in a variety of formats at Amazon for around \$24). The quickest method may be to purchase an e-edition, which you can access immediately. The 4th Edition will also work because it has substantially the same content as the 5th Edition.

Lab: The lab can be purchased directly from infoseclearning.com and will not be available from the Bookstore. You can purchase access from Infoseclearning.com by getting into our course on Canvas and going to any of the fifteen links to labs (you must do the Student Contract during the first week before you can open these labs) which are labeled with the text “Lab *nn* Access: *Title of specific lab*”. Once you click on the link to the virtual lab, InfoSecLearning will automatically begin to create an account for you. You will only authenticate this one time. You will need either a credit or debit card and it will cost about \$80. After this first time, to access the labs you will simply click on the link in Canvas and will be taken directly to the lab that is indicated with no further authentication. You must always be logged into Canvas and access our class site within Canvas to access the labs.

Once you have access to the virtual laboratory via any of the 15 “*Lab n Access: ...*” links found on the Canvas web page for CIS 102 you will have access for the length of your subscription (about 6 months). I have arranged for the canvas site for this class to remain active for that period of time because you will then be able to use the virtual systems in many more ways than to simply complete the required exercises.

One thing that you must do in order to receive credit for extra-credit “capture-the-flag” exercises is to link your personal account to the course and to me. Instructions for this are found in a PDF posted in the initial block you access for this course on Canvas. It is entitled ‘**How to link your virtual lab account to me so that I can give you credit for doing the "Challenge capture-the-flag exercises".**’

RELATED ACCESS ISSUES

If your code doesn't work or you are unable to register please email InfoSecLearning at info@infoseclearning.com. If you do have access to the labs and encounter a technical problem with the labs, you can simply click on the blue “hamburger” (3 horizontal bars on top of one another in a circle) symbol at the upper right corner of the “lab instructions” window which will pull down a menu. The bottom item on the menu is “Help Desk”.

Canvas and the Virtual Lab Site: As noted above, Canvas will be used for completing all class assignments. This site also allows you to create discussion forums or chat rooms with other class members. I encourage you to use regular email to reach me rather than the Canvas messaging capability – it is much faster and allows you to include attachments, which may not get through Canvas. I almost always have my iPhone nearby and will respond to regular email quickly at most times.

Hardware and Software Requirements: Although a tablet will work for much of what you must do in this course, it is awkward to use in the labs where a keyboard and relatively large display is necessary. (I do have a wireless keyboard that I use with my iPads, but although I suspect it will work (I do run Chrome on iOS, but I have never attempted to do any labs with it.)

Software: The software required for this class is:

- (1) **Chrome web browser** (download from <https://www.google.com/intl/en/chrome/browser/#eula>).
- (2) You will need **MS Word** or a tool that produces output compatible with MS Word (.DOC, .DOCX or .RTF files), like Apache **Open Office** or **OfficeLibre**. (Please note that I will expect that the formatting I place on the lab template documents will remain on your submitted labs: I will exact penalty points for labs that have changed formatting.)
- (3) **Microsoft PowerPoint** (even older versions work fine) on a computer with a microphone to record audio will be required if you wish to earn extra credit by recording audio PowerPoint presentations.

Please note that all students who obtain a De Anza e-mail address can install Microsoft Office 365 (“software as a service” via the Internet) **free of charge.**

WAYS TO EARN POINTS TOWARD A GRADE

This course will require the completion of 15 “hands-on” lab assignments in which you will be using hacking software tools. You will also take Unit quizzes and will take a final exam. Finally, in addition to these graded

activities, you be given the opportunity to earn additional “extra credit” points by doing some extra work in the labs (“capture the flag” points), and by researching and presenting additional information about tools and various hacking issues currently being discussed in the press and on the web to the class. The points earned from “for-credit” items and extra-credit items are summarized in the table shown below.

Source	number	credit each item	extra credit each item	total
Laboratory assignments (answers and captures)	15	15		225
<i>Extra Credit “capture the flag” challenge flag points</i>	<i>15</i>		<i>2.5</i>	<i>37.5</i>
Unit MC Quizzes	10	15		150
Final from reading/labs	1	150		150
<i>Extra Credit Presentations</i>	<i>5</i>		<i>10</i>	<i>50</i>
Total points possible (Credit = 525 , Extra Credit = 87.5)				<u>612.5</u>

SUBMITTING LABORATORY ASSIGNMENTS

This course uses a virtual hacking environment (“sandbox”) provided by InfoSecLearning to accompany the All-in-One CEH Certified Ethical Hacker Exam Guide textbook, and all 15 labs will require access to this environment via Canvas. All course information, including assignments, course deadlines, etc. will be made available to you online via the Canvas course web site you enter via “myPortal”. There, you will find the assignments that you will be asked to complete, listed within each Unit module 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 Canvas. Each week’s lab assignment(s) will require you to use the virtual environment and do multiple screen captures, which you will use to document your actions there, as well as answer specific questions about the lab session. You will then crop and paste portions of the captured screen images into the Lab Report you assemble using the MS Word template provided for that lab in the Unit for that week, answer the questions printed there, and post the resulting MS Word formatted document to satisfy the assignment at the link that reads “Lab0*n* (Required or Extra Credit) Report Turn-in”. You will find a video that details how to prepare the lab reports in introductory block for this course in Canvas.

Each Lab will have both a “due date” and a “deadline” date associated with it. The “deadline” date represents the date beyond which no labs will be accepted for scoring. Your job is simply to stay ahead of the “due dates” (and most importantly, the “deadline” dates). Failure to post any required (i.e., not extra credit) Lab may result in your being unable to access later course materials.

The Grading of Labs:

I will usually get the labs that are submitted before the due date graded, record the scores and upload the marked copies for you to read within 48 hours of the time they were due. (You will find your marked copy in exactly the same place you submitted it in the Canvas page.) The marked-up copy of your original submission will use colors to highlight comments and show where the points are earned. (Green for credit, orange for comments, red when pointing out things that you got wrong.) I also ask you to fill in your name in the blank that is labelled “Name” with your name (it is useful to know who submitted it). This will contribute to your score on the lab.

Late Work

Lab reports and extra credit labs 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 5 days have elapsed beyond the due date, 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

There are two ways you can earn extra credit points: (1) by doing the “Challenge” (“capture the flag”) exercises for any or all of the 15 Labs in this course (2.5 points per lab), and (2) by doing extra credit presentations in the form of PowerPoints with your audio narrative added. The extra credit lab reports will be submitted via Canvas in the same way that your regular lab reports will be submitted. Extra credit points earned by doing the “Challenge, capture-the-flag” exercises will be retained by the InfosecLearning virtual lab servers, which I will access for grading. **If you wish to earn these extra credit points, you must take time to connect your account on the virtual systems to this class by using my e-mail, as discussed in the PDF posted in Canvas entitled “Students Linking to Instructors”.**

“Challenge” Exercises for Extra Credit: If you choose to do so, the “Challenge” exercises for each of the fifteen Labs (including the Extra Credit Labs) will be “capture the flag” exercises done as part of the InfoSecLearning Lab. The challenge results are recorded at the InfoSecLearning site, after which you can access your score. Although I will have access to those scores for grading if you have connected it as discussed above, you will also be able to view your “flag points” earned at the virtual laboratory site.

Audio-augmented PowerPoint presentations for Extra Credit: Unlike the lab extra credits, this form of Extra Credit will be prepared as a PowerPoint presentation of an approved topic (see below), with an audio recording of your voice making the presentation, which I will post for the full class to access. (Even older versions of PowerPoint permit the recording of your voice for presentations: all you need is a laptop with a built-in microphone, or an external microphone with either USB or audio jack. I strongly recommend the latter, as the sound quality of built-in microphones is often not good.) You will upload a PowerPoint presentation that has been augmented with your own voice recording, explaining each slide, with no more than 10-minutes time being taken for the full presentation.

Extra Credit work will be posted on topics that are truly substantive and that target specific security issues pertinent to this course. These Extra Credit topics will include:

- (1) The analysis and demonstration of the accomplishment of significant hacks on **hackthissite.org** or a similar site (e.g., accomplishment of a “realistic” hack on HackThisSite), 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, Kali Linux, the setting up of a lab to test tools [“virtual” is optimal], exploits, etc.), or
- (3) The reporting and technical analysis of major events and issues in the digital security realm (e.g., analysis of a major new exploit),

All Extra Credit presentations **will require my prior approval of the topic via email** and will be posted to the Canvas site to earn extra credit points. If it is accepted for credit, I will also make your report available to the full class.

I will accept a maximum of only 5 Extra Credit presentation submissions per week for the full class (priority is in the order I receive them), and you cannot submit any more than one per week. I will accept a maximum of 5 Presentation Extra Credits from any one person for the quarter.

The Sequence of Events to Finish the Curriculum:

date	week	chapter	text chap title	Lab due	Lab deadl ine	Lab # and Title
26-Sep	1	1	Getting started (Lab demos during Office Hours)	7-Oct	12-Oct	1 Performing Reconnaissance from the WAN
3-Oct	2	2	Reconnaissance	14-Oct	19-Oct	2 Scanning the Network on the LAN
				16-Oct	21-Oct	3 Enumerating Hosts using Wireshark, Windows, and Linux Commands
10-Oct	3	3	Scanning & Enumeration	21-Oct	26-Oct	4 Remote and Local Exploitation
17-Oct	4	10	Trojans & Other Attacks	28-Oct	2-Nov	5 Crafting and Deploying Malware Using a Remote Access Trojan (RAT)
		4	Sniffing & Evasion	30-Oct	4-Nov	6 Capturing and Analyzing Network Traffic Using a Sniffer
24-Oct	5	5	Attacking a System	4-Nov	9-Nov	7 Social Engineering Using SET (Social Engineering Toolkit)
		12	Low Tech: Social Engineering			
31-Oct	6	6	Web-Based Hacking	11-Nov	16-Nov	10 Attacking Webservers from the WAN
				13-Nov	18-Nov	11 Exploiting a Vulnerable Web Application
7-Nov	7	8	Mobile Computing & IoT	18-Nov	23-Nov	15 Performing SQL Injection to Manipulate Tables in a Database
		9	Security in Cloud Computing			
14-Nov	8	11	Cryptography 101	25-Nov	30-Nov	9 Using Browser Exploitation to take over a Host's Computer
				27-Nov	2-Dec	14 Using Public Key Encryption to Secure Messages
21-Nov	9	7	Wi-Fi Hacking	2-Dec	7-Dec	12 Breaking WEP and WPA and Decrypting the Traffic
28-Nov	10	13	Pen Testing	9-Dec	14-Dec	13 Attacking the Firewall and Stealing Data over an Encrypted Channel
				11-Dec	15-Dec	8 Performing a Denial of Service Attack from the WAN
5-Dec	Catch up with labs and study for Final					
15 Dec	FINAL: 120 MC (4:00-12:00)			15-Dec	120 min.	

For each unit, the materials should be accessed and completed before the listed “deadline” dates. The following sequence is recommended:

1. Read the Chapter(s) for this Unit
2. Watch my lecture(s) for this Unit
3. Do the Lab(s) for this Unit, filling out the Lab Report with text answers and captures and posting the filled-in lab sheet at correct spot on the Canvas site: In Canvas it will read “*Lab On Report Turn-in (due ...)*”. The grading of each of the labs may take several workdays before a score is posted but are usually completed within 48 hours.
4. You may miss “deadline” dates. If you do, and have not made prior arrangements, Canvas will not accept them at later times/dates, and you must simply accept that these will be recorded as zeroes in your course gradebook. If you have a compelling reason to miss a deadline date (“my chihuahua ate the keyboard!”, “I had hiccups!”, “demented, flesh-eating aliens abducted my mother-in-law!”) – I will consider whether it is an appropriate reason to grant an extension and cut you some slack if it is.
5. Take the Unit Quiz after completing the Lab(s) for the Unit.

Testing and Grading Policies

To pass this course, you must complete the assignments, quizzes, and final exam. I will calculate the percentage of the total “required” 525 points that you have earned after adding all your earned points. (You can earn as many as 612.5 points when we include extra credit, so your percentage may rise above 100%). Deadlines for all assignments will be posted via Canvas and this syllabus.

Quarter 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:

Required Labs	42.9%
Quizzes	28.6%
Final Exam	28.6%
<i>Extra Credit Flag Captures</i>	<i>7.1%</i>
<i>Extra Credit Presentation</i>	<i>9.5%</i>
	=====
Total	= 116.7%

I will simply sum all the points you have earned, both “credit” and “extra credit”, and divide the total by 525, convert the result to a percentage, and look it up on the table labelled “Quarter Grading Scale”.

ACADEMIC INTEGRITY:

Students who submit work of others as their own or cheat on exams or other assignments will be reported to college authorities and will receive a zero on the assignment or test.

Note to students with disabilities

The Final will be 120 multiple-choice questions, and you will be given 120 minutes in which to complete the test. Disabled students who require additional time for completion of the quizzes and Final can contact either the Disability Support Services (DSS) or the Educational Diagnostic Center (EDC) and arrange for a TAV form from either the DSS counselor (864-8753 DSS main number) or EDC advisor (864-8839 EDC main number). If I receive such notice from either office, I will arrange special testing conditions for you.