Hunter College
Computer Science Department
CIS 493.75: Network Security
Fall 2017

Instructor: Stan Wine Email address: stanley.wine@baruch.cuny.edu
Section: 001 code: 8160
Meeting times: Tuesday and Friday, 3:45 to 5:00 P.M. Classroom: HN1516
Office hours: By appointment, preferably immediately before class.
Office location: Baruch College, Vertical Campus, 55 Lexington Avenue, cube 12-210C (look for door marked ZSB Faculty Offices 12-210).

Office phone: (646) 312-3413
Class website: http://www.cuny.edu

The daily activities of businesses, enterprises and individuals are dependent on the correct and secure operation of computers. These systems must operate reliably and we must have confidence in the results produced by these systems, yet they are the targets of individuals and groups who seek to subvert them. The threats that our systems face undergo continuous evolution and improvement. Today, the security of corporate, government and individual computers is a major concern. This course will teach you the vocabulary necessary to understand and discuss computer security issues and will provide an appreciation of the range of threats in the current environment and the measures that can be taken to counter these threats.

Questions you will be able to answer:

What are the key aspects of cybersecurity?
How does the Internet work? What are its major design principles and protocols?
What technical aspects of communications protocols do cybercriminals exploit?
What are the major Internet security problems and threats?
What can we do promote a more security-conscious organization?

This course is concerned with the general issues and principles that appear in computer and network systems; it is not an exhaustive study of any particular topic. This is not a vocational course that teaches you how to install a particular security package or to configure an operating system for maximum security. This course develops a sound understanding of the basic concepts underlying computer and network security, providing an appreciation of the scope and scale of the security issue, its criticality in today's environment, and the wide-ranging nature of the issues, which involve not just technology but also management issues and human factors. It is hoped that this course will provide you with the necessary background to be able to understand any specific security concern or product on your own.

To stay abreast of the ever-changing developments, we will discuss articles from many sources. Students are expected to come to class prepared to discuss these articles; your grade will be dependent on this, as described in the section on grading below. Articles can be found in the Articles or Newspaper Articles subfolders of the Course Documents folder on the course website.

Due to the interrelated nature of the material in the course, we may deviate at times from the order of topics as listed in the syllabus below or because of time reserved for student presentations.

Learning goals: This course satisfies the following departmental learning goals:
1D: in-depth knowledge of an area of specialization: Network security.
3B: understand the ethical concerns typically arising in the context of computing.

4: computer science students should graduate prepared to continue to learn throughout their careers, keeping up-to-date in a quickly developing field.

Required text: Stallings, William, and Brown, Lawrie, *Computer Security: Principles and Practice*, 4th Ed., Pearson Prentice Hall, 2018, ISBN 0-13-479410-9. Most of the material in the fourth edition is similar to third edition content. Topics with new or expanded coverage include data center security, virtualization security, cloud security and IoT security. If you use the third edition, you will be responsible for finding sources to acquaint yourself with these topics.

Information on the text can be found here:
http://hunter.textbookx.com/institutional/index.php?action=browse#books/1740289/

Corrections to the text can be found in the errata folder on our Blackboard site. Additional books that may be referred to in the course have been placed on reserve or ordered for reserve use.

If you find any typos or errors in the textbook or my documents, please bring these to my attention.

Website: http://www.cuny.edu The class website uses Blackboard. The syllabus, lecture slides, handouts, glossary, newspaper articles and suggested study topics for exams will be posted on the class website, which can be found at www.cuny.edu. I tend to update the slides as the semester progresses, so to get the freshest version, please do not print them out until shortly before each class meeting.

Announcements of Class Cancelations: Some students posing as instructors have made announcements to classmates via email or through signs affixed to classroom doors. These announcements have indicated that a class in which an exam has been scheduled has been canceled. If I cancel a class, you will be notified via CUNY email (I will never use Gmail or any other account that a student could create in my name) and by posting an announcement on the Blackboard site.

Student email: I will only respond to emails from CUNY email addresses; mail from personal email accounts will be ignored. Please check your email and the BlackBoard site on a daily basis. These tools will be used to notify you of assignments and of newly posted materials, and for all advisories.

A Word to the Wise: This course introduces a large number of terms and concepts. In order to succeed in this course, you must become familiar with these terms and their usage. It is imperative that you do the assigned reading before class. I recommend that you take extensive notes.

Homework: See the assignment column of the schedule below for a list of Review Questions. The questions are intended to verify and strengthen your understanding of terminology and concepts. The homework will not be collected; you will find that doing it in a timely fashion will help you to prepare for exams.

Electronic Devices and Note Taking:
Electronic devices may not be used in class and should be put away. I suggest you bring a paper notebook for taking notes.

Grading: Exam material will be derived from both the reading assignments and from material covered in the lectures. Some of the lecture material will not be found in the text. Therefore, it is very important to attend class regularly, take good notes and keep up with the pace of the reading assignments. The course grade will be derived from the following factors:

Exams (exam I – 28%, midterm – 28% and final – 28%)	84%
Wireshark lab assignment	16%

Lab assignments make use of industry-standard products; there is a 25% penalty for each day that an assignment is late.

Class participation will be considered in grading.
There will be no "extra-credit" assignments and make-up tests will not be given. Students will have an opportunity to check their graded exams but the instructor will retain all exams.

Exams will consist of a mix of multiple choice, fill-in-the-blank, matching, true/false, short and long answer questions and problems to be worked. In some sections, you may be able to choose from among a set of questions. There may also be questions on the articles discussed in class or available on the website. The Course Docs/Exams/folder contains study guides for each exam.

Electronic devices may not be used during an exam; you may not leave the room for any reason during an exam.

Academic integrity: Hunter College regards acts of academic dishonesty (e.g., plagiarism, cheating on examinations, obtaining unfair advantage, and falsification of records and official documents) as serious offenses against the values of intellectual honesty. The college is committed to enforcing the CUNY Policy on Academic Integrity and will pursue cases of academic dishonesty according to the Hunter College Academic Integrity Procedures.

I have **zero tolerance** for any of the offenses described above. The Dean of Students will be advised of any incident of suspected academic dishonesty.

Students with disabilities: In compliance with the American Disability Act of 1990 (ADA) and with Section 504 of the Rehabilitation Act of 1973, Hunter College is committed to ensuring educational parity and Accommodations for all students with documented disabilities and/or medical conditions. It is recommended that all students with documented disabilities (Emotional, Medical, Physical and/ or Learning) consult the Office of AccessABILITY located in Room El124 to secure necessary academic accommodations. For further information and assistance please call (212) 772-4857/TTY (212) 650-3230).

Attendance: You are expected to be present and punctual for each class meeting.

Academic calendar:
See http://www.baruch.cuny.edu/registrar/due_dates.htm#Fa17Ac

Schedule: If required, the course content and schedule may be changed at the instructor's discretion. The dates for holidays, withdrawal, and final exams were taken from the academic calendar and should be checked by the student against the official academic calendar. All other dates are approximate.

In the Assignments column, RQ = Review Questions and P= Problems

Week	Date	Topic	Assignments
1	8/25–29	Overview Networking and TCP/IP Protocol Architecture	Read Chapter 1 RQ: all. Read Appendix F (supplied as a pdf) and relevant sections of Comer, Kurose, Stallings or Tanenbaum (see supplementary references below). View *Bundled, Buried and Behind Closed Doors* (10 minutes) See Blackboard for homework questions.
2	**9/4** 9/1- 9/5	**Labor Day – College is closed** Networking and TCP/IP Protocol Architecture, continued	

Week	Date	Topic	Assignments
3	9/8- **9/12**	Networking and TCP/IP, continued **Wireshark demo**	 **Install Wireshark on a laptop** per Assignment #1 and bring to class for brief demo.
4	9/15- **9/19** 9/26	Cryptographic Tools **Classes follow Thursday schedule**	Read Chapter 2 RQ: 2.1 – 2.6 and 2.8 – 2.13. For Review Question 2.6, use Fig 2.5, not Fig. 2.3.
5	10/3 - 10/6	User Authentication	Read Chapter 3 RQ: all.
6	**10/9** **10/10** -10/13	**College is closed** **Assignment: Wireshark Lab due** **Exam I** Malicious Software	 Covers Chapters 1 - 3 and Networking Read Chapter 6 RQ: 6.1 - 6.3; 6.5 - 6.16.
7	10/17- 10/20	Review Exam I Malicious Software, continued	.
8	10/24- 10/27	Denial-of-Service Attacks Intrusion Detection	Read Chapter 7 RQ: all. Read Chapter 8 RQ: all except 8.12.
9	10/31- **11/3**	Firewalls and Intrusion Prevention **Midterm**	Read Chapter 9 RQ: all except 9.8. Covers Chapters 6 - 9.
10	11/7 **11/10** **-**11/10	Review Midterm **Last day to withdraw with "W" grade.** Buffer Overflow	 Read Chapter 10 RQ: 10.1 – 10.7, 10.10 - 10.14 (we will examine this chapter at a high level only – do not concern yourself with the detailed coding examples).
11	11/14- 11/17	Software Security Operating System Security	Read section 5.4 and Chapter 11 RQ: 11.1 – 11.10; 11.13, 11.16 Read Chapter 12 RQ: 12.1-12.9; 12.23 - 12.26
12	11/21 **-**11/28	Cloud and IoT Security IT Security Management and Risk Assessment	Read section 5.8 and Chapter 13 RQ: all. Read Chapter 14 RQ: all.
13	12/1- 12/5	IT Security Controls, Plans and Procedures Human Resources Security	Read Chapter 15 RQ: all. Read Chapter 17 RQ: all.
14	12/8 **-12/12**	Human Resources Security, continued Security Auditing **Last day of class**	 Read Chapter 18 RQ: all.
	12/19	**Final Exam** 1:45 – 3:45 P.M.	Covers parts of Chapters 5.4, 5.8, 10 - 15, 17 and 18. http://www.hunter.cuny.edu/onestop/repository/files/registrar/Fall%202017%20Final%20Exam%20Schedule.pdf

Supplementary references:
These books are available in the library (some are on reserve) and can be used to explore topics in more detail:

Anderson, Ross, *Security Engineering*, 2nd Ed., Wiley, QA76.9 .A25 A54 2008
Bellovin, Thinking Security, Pearson Prentice-Hall, 2016, TK5105.59 .B45154 2016
Bosworth, Kabay and Whyne, *Computer Security Handbook*, 5th Ed., Wiley, 2009, electronic resource, Baruch library
Comer, Douglas E., *Computer Networks and Internets*, 6th Ed., Prentice-Hall, TK5105.5 .C5897 2015

Comer, Douglas E., *Computer Networks and Internets*, 5th Ed., Prentice-Hall, TK5105.5 .C5897 2009
Comer, Douglas, *Internetworking with TCP/IP,* 6th Edition, Pearson Prentice-Hall, 2014 TK5105.585 .C66 2014
Comer, Douglas E., *Internetworking with TCP/IP (volume-I)*. Prentice-Hall, TK5105.585 .C66 2006
Eagle, Harper, Harris, Lenkey, Ness, Williams, *Gray Hat Hacking*, 3rd Ed., McGraw Hill Professional, QA76.9 .A25 G743 2011
Erickson, Jon, Hacking: *The Art of Exploitation*, 2nd Ed., No Starch Press, 2008, electronic resource, Baruch library
Goodrich and Tamassia, *Introduction to Computer Security*, Addison-Wesley, QA76.9 .A25 G655 2011
Hernandez, Steven, *Official (ISC)^2 Guide to the CISSP CBK,* 3rd Ed., Auerbach Publications, 2013, TK 5105.59 .O438 2013
Kurose, J. and Ross , K. W., *Computer Networking: A Top-Down Approach Featuring the Internet*, 5h Ed., Addison-Wesley, TK5105.875 .I57 K88 2010
Mowbray, T.J., Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions, 2014, John Wiley & Sons, electronic resource, Hunter library
Pfleeger, Charles and Pfleeger, Shari, *Security in Computing*, 5th Ed., Prentice-Hall, QA76.9 .A25 P45 2015
Pfleeger, Charles and Pfleeger, Shari, *Security in Computing*, 4th Ed., Prentice-Hall, QA76.9 .A25 P45 2007
Schneier, Bruce, *Secrets and Lies: Digital Security in a Networked World*, Wiley, QA76.9 .A25 S352 2000
Schneier, Bruce, *Schneier on Security*, Wiley, 2008, electronic resource, Baruch library
Smith, Richard, *Elementary Information Security*, Jones and Bartlett, QA76.9 .A25 S652 2012
Schneier, Bruce, *Liars & Outl*iers, Wiley, 2012, ISBN: 978-1-1181-4330-8, electronic resource
Stallings, William, *Computer Security*: *Principles and Practice*, 3rd Ed., Pearson Prentice-Hall, QA76.9 .A25 S685 2014
Stallings, William, *Data and Computer Communications*, 10th Edition, Pearson Prentice-Hall, TK5105 .S73 2014
Stallings, William, *Data and Computer Communications*, 9th Edition, Pearson Prentice-Hall, TK5105 .S73 2011
Tanenbaum, Andrew, *Computer Networks*, 5th Ed., Prentice-Hall, TK 5105.5 .T36 2011
Tanenbaum, Andrew, *Computer Networks*, 4th Ed., Prentice-Hall, TK 5105.5 .T36 2003
Tipton, Harold, *Information Security Management Handbook,* 6th Ed., Auerbach Publications, 2007, electronic resource, Baruch library
Tipton, Harold, *Official (ISC)^2 Guide to the CISSP CBK,* 3rd Ed., Auerbach Publications, 2013, TK 5105.59 .O438 2013

Various study guides for the Certified Information Systems Security Professional (CISSP) certification exam are available as electronic resources at the Cooperman library.