

IT 263-501 Syllabus – Applied Networks and Security – Winter 2020

| | | | |
|-----------------------|---|-------------------|--|
| Instructor | Dr. Sharief Oteafy | Phone | 312 362-8127 |
| Office | CDM 846 | E-mail | soteafy@depaul.edu |
| Office Hours | Thursdays 10 – 11:30 am (or by appointment) | Website | d2l.depaul.edu |
| Class Location | CDM 226 | Class time | Tu/Th 1:30 pm – 3 pm |

--- Any changes made to this syllabus will be announced in class as well as D2L --- This is Version 1: Jan 1st ---

Course Overview

This course introduces the networking and security technologies required to build and maintain a home or small-office network. Networking topics will include client/server application software configuration, network connectivity (cabling, switch and router configuration), basic IP addressing, network address translation and options for public Internet access services. Security topics will include typical threats and responses, firewalls, host hardening, password management and virtual private network (VPNs). The course has a lab component where students apply wired and wireless technologies to design and administer a small network with various applications. PREREQUISITE(S): None.

Resources:

E-Text: Introduction to Networks: Cisco Networking Academy, which you can access at <https://www.netacad.com>.

Grade distribution over required coursework

| Task | % of final grade |
|------------------------|------------------|
| 3 Homework assignments | 20 % |
| 3 lab exercises | 10 % |
| 1 Quiz | 5% |
| Midterm exam | 20 % |
| Final exam | 30 % |
| Technology report | 10 % |
| Class participation | 5 % |

Coursework

Course topics expected to be covered in each class and the corresponding readings in the Network Academy Introduction to Networks (ItN) course are listed in the course schedule on page 3. Note: you are not required to do any Activities or Labs within the ItN course unless specifically stated, but you are encouraged to complete them for extra practice if you wish.

The Technology Report will consist of an individual report on a relevant information security topic. More details on this assignment will be provided in Week 1. The Class Participation grade will be earned as follows: students gain 0.5% credit towards their final grade for each lecture actively attended (until the maximum of 5.0% of the final grade). Active attendance means that you will respond/contribute when I call upon you, and actively engage in class discussions.

Course policies

General academic policies

All students are required to manage their class schedules each term in accordance with the deadlines for enrolling and withdrawing as indicated in the [University Academic Calendar](#). Information on enrollment, withdrawal, grading and incompletes can be found at: cdm.depaul.edu/enrollment. Note that **January 17th, 2020** is the last date to drop the class with no penalty.

Plagiarism

There is a "zero-tolerance policy" regarding plagiarism. This stands for both the plagiarizer and the person(s) facilitating plagiarism (e.g., allowing someone to plagiarize their work). There's a great resource put together by DePaul University, which you can find here: <https://resources.depaul.edu/teaching-commons/teaching-guides/learning-activities/Pages/avoiding-plagiarism.aspx>

Academic Integrity

One of the core principles of education is establishing Academic Integrity. It is a viable component in the classroom, one by which learning objectives could be honestly and efficiently met. The principles of academic integrity should span all of your learning endeavours, within and beyond this course. For more information on Academic Integrity, especially definitions and norms, please visit: <https://resources.depaul.edu/teaching-commons/teaching/academic-integrity/Pages/default.aspx>. This will be the basis of all of our interactions in this course. If you have any questions or concerns, feel free to drop by and see me.

Deadlines and submission policies

Assignments are due on D2L by 11:59 pm on the deadline day posted on each assignment, unless otherwise announced. All of your work (exams, assignments, report, etc) must be your original work. Any evidence of departure from Academic Integrity will be reported, and ensuing sanctions will be pursued. You are expected to read, understand and comply with DePaul's policy on Academic Integrity, which you can reach from the aforementioned website.

Late submissions receive a 10% penalty for every 24 hour delay, starting from the minute past the deadline.

Missing exams and/or deadlines

Emergencies happen and that is quite understandable. If you miss an exam due to a certain emergency (e.g., accident, emergency hospitalization, etc) please communicate with me as soon as you can to resolve any outstanding issues. If a major illness hinders you from attending an exam or submitting a deliverable (assignment), you need to contact me beforehand via e-mail. Notices received after the deadline will not be accounted for (unless for an emergency as highlighted above). If the illness occurred after the deadline, even if accompanied with a doctor's note, you would receive a zero for that exam/deliverable.

Otherwise, missing an exam without prior approval will warrant an automatic zero. Generally, all extensions are considered on a case-by-case basis. Falling sick prior to a deadline does not automatically warrant an extension. If you have any questions or concerns, please don't hesitate in contacting me.

Disability Accommodation

Feel free to speak to me as soon as possible regarding any difficulties you feel you might be encountering in this course, ideally within our first week of classes. Kindly refer to DePaul's Center for Students with Disabilities website at <https://offices.depaul.edu/student-affairs/about/departments/Pages/csd.aspx>. If you feel that any given disability is hindering you, or you are not sure and wish for a consult, please reach out to CSD at csd@depaul.edu; they are trained to help out and point you to the appropriate resources.

Grade calculation

Final grades will be calculated as follows: points earned divided by possible points in each category will be multiplied by the contribution percentages shown to yield a total course percentage score between 0% and 100%. Letter grades will be assigned as:

| | | | | |
|----------------|----------------|----------------|----------------|----------------|
| A = 90% - 100% | A- = 88% - 90% | B+ = 86%-88% | B = 80% - 86% | B- = 78% - 80% |
| C+ = 76% - 78% | C = 70% - 76% | C- = 68% - 70% | D+ = 66% - 68% | D = 60% - 66% |
| | | F = 0% - 60% | | |

Class schedule and topics

| Week | Class date | Tentative Topics | NetAcad ItN Readings | Tentative Assignment dates |
|------|-------------|--|---------------------------|-------------------------------------|
| 1 | 7 January | Course overview | 1.1 – 1.5 | |
| | 9 January | Network basics & Cabling | 1.2 3.1 – 3.3 & 4.1 – 4.2 | Technical report explained in class |
| 2 | 14 January | Wired Ethernet and Switching | 4.3-4.4 | Lab 1 posted |
| | 16 January | Wi-Fi Networks | 5.1-5.3 | HW 1 posted |
| 3 | 21 January | IP addressing and DHCP | 2.1, 2.2.1, 2.3 & 6.1 | Lab 1 due |
| | 23 January | In-class Quiz TCP and packet analysis | 7.1, 7.3 9.1, 9.2 | HW 1 due |
| 4 | 28 January | IP subnets and routing | 6.2 | Lab 2 posted |
| | 30 January | Subnetting | 8.1-8.3 | HW 2 posted |
| 5 | 4 February | Routers and Switches Sample problems and review | 6.3-6.4 | Lab 2 due |
| | 6 February | Midterm exam | 6.3-6.4 | HW 2 due |
| 6 | 11 February | Midterm recap (answers & discussion) NAT | | |
| | 13 February | NAT & port management | | Lab 3 posted |
| 7 | 18 February | IPv6 | 6.1.4 | HW 3 posted |
| | 20 February | DNS, Internet Applications | 7.2 & 8.3 | |
| 8 | 25 February | Privacy and Network Security | 10.1-10.2 | Lab 3 due |
| | 27 February | Integrity and Encryption | 11.1 | HW 3 due |
| 9 | 3 March | Network Vulnerabilities | 1.4.3 | |
| | 5 March | Authentication & Firewalls | 11.2 | |
| 10 | 10 March | Virtual Private Networks (VPNs) | | Technical report due |
| | 12 March | Course review and Final Exam preparation | | |
| 11 | 19 March | Final Exam 11:30 am – 1:45 pm | | |

Liberal Studies Domain Information

IT 263 is included in the Liberal Studies program as a course with credit in the Scientific Inquiry domain. Courses in the Scientific Inquiry domain are designed to provide students with an opportunity to learn the methods of modern science and its impact in understanding the world around us. Courses are designed to help students develop a more complete perspective about science and the scientific process, including: an understanding of the major principles guiding modern scientific thought; a comprehension of the varying approaches and aspects of science; an appreciation of the connection among the sciences and the fundamental role of mathematics in practicing science; an awareness of the roles and limitations of theories and models in interpreting, understanding, and predicting natural phenomena; and a realization of how these theories and models change or are supplanted as our knowledge increases.

Learning Outcomes

After completing this course, students will be able to:

- Understand foundational networking topics and concepts
- Analyze and maintain Local Area Networks
- Plan IP address assignments through subnetting
- Discuss various types of security attacks and how to mitigate them
- Understand how to secure a network from common attacks
- Use tools such as Wireshark to analyze network traffic

Learning Outcomes for Scientific Inquiry-Elective (SI-Elective) courses

- Students will be able to apply appropriate concepts, tools, and techniques of scientific inquiry.
- Students will be able to describe how natural scientific, mathematical, and/or computational methodologies function as mechanisms for inquiry.
- Students will be able to explain the interaction between the content of their SI-Elective course and other scientific disciplines or the broader society.

These learning outcomes will be met through homework and lab assignments that will include: short answer questions that will require the application of networking concepts covered in class, labs in which the student will observe and analyze how traffic passes through a network, situational problem-solving, and researching recent security hacks and vulnerabilities.

Course evaluations

During the course, your feedback on how well the course is running (pace, difficulty, resources, etc) will be solicited. This is a vital component of improving and tailoring this course to your learning objectives. While all students are expected to achieve the learning outcomes highlighted above, each of us inevitably learn differently. This course is designed to meet the aforementioned learning outcomes, and I will endeavor to incorporate different activities (e.g., Kinesthetic learning) to improve the learning experience.

If you have any concerns about how the course is running, or would like to suggest an improvement, feel free to reach out to me. Also, on week 10, we will hold the official course evaluations in class.