SYLLABUS

Course Description

COURSE DESCRIPTION

From the ODU Catalog

Introduction to networking and the Internet protocol stack; Vulnerable protocols such as HTTP, DNS, and BGP; Overview of wireless communications, vulnerabilities, and security protocols; Introduction to cryptography; Discussion of cyber threats and defenses; Firewalls and IDS/IPS; Kerberos; Transport Layer Security, including certificates; Network Layer Security.

Prerequisites

The main prerequisite for this course is CS 270 - Computer Architecture.

Course Overview

This is the first course in the Graduate Certificate Program in Cybersecurity. This course will introduce the networking and cybersecurity background that you'll need to suceed in the other courses in the certificate program.

Cybersecurity emphasizes prevention of attacks that are perpetrated using the Internet. It includes application security, information security, and network security. Because the foundations of cybersecurity rely so heavily on knowledge of networking, this course will cover networking background before discussing details of cybersecurity.

Course Readings

COURSE READINGS

Required Textbook

Kurose and Ross (2012), *Computer Networking: A Top-Down Approach*, 6th edition, Addison Wesley, 2012.

Recommended (Optional) Textbooks

- *Network Security Essentials*, 5th Edition, by William Stallings, 2014
  - This is the same textbook used for CS 564
- *Network Security: Private Communication in a Public World*, 2nd Edition, by Kaufman, Perlman, and Speciner, 2002
  - available free via ODU Library
- *Introduction to Computer Networks and Cybersecurity*, by Wu and Irwin, 2013
  - last year's textbook
  - available free via ODU Library

Other Requirements

As this is an online-only course, you must have access to a computer with high-speed Internet. If you are an on-campus student, you may use the university computer labs or Computer Science computer labs. Otherwise, you must provide your own computer and Internet access.

Course Goals and Objectives

COURSE GOALS AND OBJECTIVES

After completing this course, students should have a strong foundation in the principles of the Internet architecture, an awareness of vulnerabilities in the Internet protocol stack, and an introduction to issues in cybersecurity. They should be prepared to take follow-on courses in the CS CyberSecurity certificate. After successfully completing the entire certificate program (4 courses), students should be able to pass the CompTIA Security+ Certification Exam.

Upon successful completion of this course, students will:

- Gain experience with the online course system.
- Explain the general architecture of the Internet, including the main functions of end systems and routers.
- Describe the basic client-server architecture and how typical network applications (web, email) fit into the architecture
- Explain how web pages are requested and delivered using HTTP
- Explain in general how DNS enables our use of the Internet and, in particular, how hosts determine the IP address of network servers
- Explain how MAC addresses are used and assigned to a packet as it traverses a network
- Differentiate between wireless LANs and wired LANs
- Explain how IP CIDR addressing is performed and how an IP address is assigned from a group of available addresses
- Explain the core functions of TCP including details of connection setup
- Analyze and differentiate among types of malware and attacks
- Analyze and differentiate among types of wireless attacks and application attacks
- Identify vulnerabilities potentially present in DNS, databases, and web applications
- Summarize general cryptography concepts
- Describe how certificates can be used for authentication and encryption
- Explain how firewalls and VPNs can be used to protect a network

More specific objectives for each topic are listed within each module.

How the Course Works

HOW THE COURSE WORKS

Methods of Delivery/Learning Activities

This online course employs several methods of delivery and learning activities including online videos and screencasts, threaded discussions, readings, written assignments, self-assessment checks, and exams.

Course Outline

The course is divided into two main sections, covering networking and cybersecurity. The material is divided into modules, with each module lasting one week.

- Module 1 - Online Course Intro
- Module 2 - Whirlwind Intro to Internet
- Module 3 - Cybersecurity Overview
- Module 4 - Application Layer and HTTP
- Module 5 - DNS
- Module 6 - Transport Layer and Network Layer
- Module 7 - Routing
- Module 8 - Link Layer and Wireless
- Module 9 - MID-TERM EXAM
- Module 10 - Cryptography
- Module 11 - General Attack Types
- Module 12 - Application Attack Types
- Module 13 - Firewalls and IDS/IPS
- Module 14 - Network Access Control
- Module 15 - Transport and Network Layer Sec

- Module 16 - FINAL EXAM

Weekly Schedule

Sunday	New module begins
Wednesday	Initial discussion question posting (if any) due before 11:59pm
Saturday	Module ends. All materials (homework, discussion replies, feedback) due before 11:59pm.

Discussion Board Policy

Almost every week we will have a discussion question related to the material being covered that week or related to a recent cyber attack. Each student will be required to make initial replies to at least 3 of these discussion questions during the course of the semester. I will divide the class into groups based on last names and will assign groups to respond on particular weeks.

Students not assigned to make an initial reply will be encouraged to read and respond to their classmates' initial replies. Over the course of the semester, students are required to make 6 replies. These replies must be distributed over 6 different discussion questions (i.e., 6 different weeks).

In addition to the discussion question replies, CS 562 students are also required to research a recent cyber attack and write a discussion post about it. More information will be given during the 2nd half of the semester.

Grading Criteria

GRADING CRITERIA

Please note that requirements differ for graduate and undergraduate students. Graduate students will have an additional assignment (more information will be provided later in the semester).

Grading

Your grade in this class will be based on the following:

Homework Assignments
• not graded for correctness, answers will be provided after the due date
• rubric:
  ◦ 0 – not submitted, nonsense answers submitted, or any portion copied from textbook or Internet without reference
  ◦ 1 – submitted at most 1 day late, not all answers submitted, or contains excessive quoting
  ◦ 2 – all answers submitted on time
	20%

Discussion Participation
• 3 initial discussion postings (includes student introduction)
• 6 replies to initial postings (on 6 different weeks)
• rubric:
  ◦ 0 – not submitted, "me too" or nonsense posting, or any portion copied from textbook or Internet without reference
  ◦ 1 – submitted at most 1 day late, low quality posting or reply, or contains excessive quoting
  ◦ 2 – high quality posting or reply submitted on time
	CS 462: 30%
	CS 562: 20%

CS 562 Cyber Attack Post	CS 562: 10%
Mid-term Exam	25%
Final Exam	25%

Grading Scale

The grading scale is as follows (+ and - modifiers may be applied as appropriate):

- 90-100% A
- 80-89% B
- 70-79% C

CS 462 only

- 60-69% D
- 0-59% F

CS 562 only

- 0-69% F

Late Assignments

Any requirement submitted after its deadline is considered late. Late submissions receive no credit. There is a 1-day grace period, where submissions late by no more than 24 hours receive 50% credit.

Student Responsibilities

STUDENT RESPONSIBILITIES

Time Management

Students are expected to spend 10 hours per week on the course materials and assignments. Out of 10 hours, students are expected to spend approximately 5 hours/week to read the material, approximately another 4 hours/week for the homework, and another 1 hour/week for discussions.

Attendance

Since this is an on-line course, there is no mandatory attendance policy. However, students are expected to actively participate in the discussions, homework submissions, and feedback. Each of these components is graded and counted toward the final grade.

Academic Integrity / Honor Code

By attending Old Dominion University, you have accepted the responsibility to abide by the honor code and honor pledge. This is an institutional policy approved by the Board of Visitors. If you are uncertain about how the honor code applies to any course activity, you should request clarification from the instructor. The honor pledge is as follows:

> *"I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member if the academic community, it is my responsibility to turn in all suspected violators of the honor system. I will report to Honor Council hearings if summoned."*

Any evidence of an honor code violation (cheating) will result in a 0 grade for the assignment/exam, and the incident will be considered for further review. Evidence of cheating may include a student being unable to satisfactorily answer questions asked by the instructor about a submitted solution. Cheating includes not only receiving unauthorized assistance, but also giving unauthorized assistance.

Students may still provide legitimate assistance to one another. You are encouraged to form study groups to discuss course topics. *Students should avoid discussions of solutions to ongoing assignments or exams and should not, under any circumstances, share solutions for an ongoing assignment or exam.*

Read the Academic Integrity page for more information on what is considered cheating or plagiarism in the Department of Computer Science.

All students are responsible for knowing the rules. If you are unclear about whether a certain activity is allowed or not, please contact the instructor.

Course Policies

COURSE POLICIES

Online Classroom Conduct

As most of our interactions will be online, please follow proper online etiquette. The following is a list of general guidelines for this course:

- Check your grammar and spelling
- Keep your comments focused on the topic
- Strive to write succinctly and clearly
- Share your knowledge and include supportive evidence for your comments
- Do not use all capital letters, as that is viewed as shouting
- Disrespectful language is unacceptable

Getting Help

Please use the Hallway forum (on Blackboard) to ask questions about the course material or ask clarifying questions about an assignment. Feel free to answer questions that other students have posted in the Hallway forum.

If you need to contact the instructor about a private matter, the best way is through email, but do not expect or rely on an immediate response.

Attendance

Since this is an online course, there is no mandatory attendance policy. However, students are expected to actively participate in the discussions, homework submissions, and feedback. Each of these components is graded and counted towards the final grade.

Notification of Extenuating Circumstances

If a serious situation has occurred that will prevent you from submitting your work (assignments, exams, etc.) on time, notify your instructor 24 hours before the scheduled due date.

Disclaimer

Every attempt is made to provide a syllabus that is complete and that provides an accurate overview of the course. However, circumstances and events may make it necessary for the instructor to modify the syllabus during the semester. This may depend, in part, on the progress, needs, and experiences of the students.

University Policies

UNIVERSITY POLICIES

Honor Pledge

> *"I pledge to support the honor system of Old Dominion University. I will refrain from any form of academic dishonesty or deception, such as cheating or plagiarism. I am aware that as a member if the academic community, it is my responsibility to turn in all suspected violators of the honor system. I will report to Honor Council hearings if summoned."*

Special Needs

> Old Dominion University is committed to achieving equal educational opportunity and full participation for persons with disabilities. It is the university's policy that no qualified person be excluded from participation in any university program or activity, be denied the benefits of any university program or activity, or otherwise be subjected to discrimination with regard

to any university program or activity. This policy derives from the university's commitment to non-discrimination for all persons in employment, access to facilities, student programs, activities and services.

Disability Services

In compliance with PL94-142 and more recent federal legislation affirming the rights of disabled individuals, provisions will be made for students with special needs on an individual basis. Old Dominion University is committed to ensuring equal access to all qualified students with disabilities in accordance with the Americans with Disabilities Act. The Office of Educational Accessibility (OEA) is the campus office that works with students who have disabilities to provide and/or arrange reasonable accommodations.

- If you experience a disability which will impact your ability to access any aspect of my class, please present me with an accommodation letter from OEA so that we can work together to ensure that appropriate accommodations are available to you.
- If you feel that you will experience barriers to your ability to learn and/or testing in my class but do not have an accommodation letter, please consider scheduling an appointment with OEA to determine if academic accommodations are necessary.

The Office of Educational Accessibility is located at 1021 Student Success Center and their phone number is (757) 683-4655. Additional information is available at the OEA website: http://www.odu.edu/educationalaccessibility/