NEW YORK CITY COLLEGE OF TECHNOLOGY/CUNY

Computer Systems Technology Department

CST 3610 - Network Security Fundamentals (3 credits, 2 class hours, 2 lab hours)

Course Description

This course is designed to provide a comprehensive overview of network security. It covers authentication methods along with common network attacks and how to safeguard against them. It also teaches important communication security aspects related to the use of remote access, the Web, directory and file transfer, and wireless data. It introduces the students the pre-attack phases: reconnaissance, scanning and enumeration; layer 2 and 3 and TCP/IP attacks and vulnerabilities; major security vulnerabilities in web applications; Security Protocols; Firewalls and their implementation topologies; VPN, IDS, Wireless security and Honey net; Security Logging and Auditing.

Objective:
This is the second course of the information security module. It provides students with the basic network security knowledge they will need for success as information security professionals. The students will gain real-world network security practice.

Learning Outcomes:
At the end of the course, students should be able to:

- Demonstrate understanding of the network model and internetworking, internet services and security overview
- Demonstrate understanding of network security devices and their uses for securing remote access to the network.
- Demonstrate understanding of the benefits of centralized enterprise directory services over traditional authentication system.
- Demonstrate understanding of network security topologies and Intrusion Detection
- Demonstrate understanding of the security issues related to wireless data transfer

Prerequisites:
CST2410

Textbook:
Tom Thomas and Donald Stoddard, *Network Security First-Step,* 2nd Ed., Cisco Press, 2011. ISBN: 978-1-58720-4104.

Reference books:
Mark Ciampa, *Security+ Guide to Network Security Fundamentals,* 5th Ed., Course Technology, 2014. ISBN: 978-1305093911.

On-line Certificate: *Network Assurance*
https://teex.org/Pages/Class.aspx?course=AWR138&courseTitle=Network%20Assurance

Homework Assignments

Homework assignments will be based on chapter questions.

Project Assignments

Students should work in groups to finish and demonstrate three projects. All projects must be submitted on the due date.

Grade Requirement

Students must complete all project assignments, homework assignments, participate in all tests.

Course grading formula:

Four Projects	40%
Test	15%
Midterm Exam	15%
On-line Certificate: (Network Assurance)	15%
Final Exam	15%
	100%

Academic Integrity Policy:

The instructor of the course has the authority to give a grade of **F** if the student submits the work of another person in a manner that represents his/her work, or knowingly permits one’s work to be submitted by another person without the instructor’s permission (see College Catalog).

Progression Requirements

Students majoring in CIB must earn a grade of “C” or better in this course in order to progress to the next level courses (CST4710). If grade earned is less than “C”, the course must be repeated.

Letter Grade	A	A-	B+	B	B-	C+	C	D	F
Numerical Grade	93-100	90-92.9	87-89.9	83-86.9	80-82.9	77-79.9	70-76.9	60-69.9	<=59.9

Instructor: Prof. , email: tel:
Office Hours: . Office: N1000

Week	Topics	Reading/Assignment/Test
1-2	Week 1: Network Protocol TCP/IP Overview Layer names and their functions MAC, IP, port, ARP, ICMP, TTL, Sliding Window flow control, error control, TCP/UDP, mask and submask	Hands-out Test on TCP/IP

3-4	Weeks 3-4: Pre-attack phases Reconnaissance, Scanning, and Enumeration Introduction to Network Security Organizations Hands-on: Use the NMAP and NESSUS tools to scan a host/network and identify the possible vulnerable points in the hosts Install VisualRoute	Chapter 1 Project 1: NMAP & NESSUE
4-5	Weeks 4-5: Layer 2 and 3 attacks Introduction to LAN based attacks (layer 2 attacks or lower layer attacks) and security measures/methods used to prevent or mitigate the LAN based attacks Introduction to attacks to which routers (layer 3 devices) are vulnerable and the attacks detection/prevention	Hands-out Project 2: Various layers attacks
6	Week 6: Overview of Security Technologies Firewall: Packet Filtering, ACLs, Stateful Packet Inspection, Proxies, Application-Layer Protection Content filters Public Key Infrastructure AAA Technologies TACACS and RADIUS Two-factor and multifactor authentications	Chapter 5
7-8	Weeks 7-8: Security Protocols DES, 3-DES, AES Encryption: Strength and limitation MD5 Hash algorithm PPTP, L2TP, SSH, SHA, https, FTPS, DSA Hash function	Chapter 6 + Hands-out 1. Configure and Install Windows 2008 server as VPN server/client 2. Install and configure OpenSSH 3. Install FTPS
9	Week 9: Midterm review and Midterm	
10	Week 10: Network Security Standards / Firewall Cisco SAFE, Validated Design Program NSA security Configuration Guide Microsoft Security Firewall operational overview Implementations Determining the Access Policy Limitation	Chapter 4 and Chapter 7 Project 3
11	Week 11: IPsec Virtual Private Networks (VPNs) VPN overview IPsec VPNs Router configuration as VPN peer	Chapter 9

	Firewall VPN configuration for client access SSL VPN overview Comparing SSL and IPsec VPNs Remote-access VPN security considerations	
12	Week 12: IDS and Honeypots Introduction of Intrusion and Honeypots Types of IDS and their limitations Types of Honeypots	Hands-out Project 4: IDS -- Snort
13	Week 13: Wireless Security and Router Security	Hands-out and Chapter 8
14	Week 14: Project: On-line certificate ***Network Assurance***	Hands-out
15	Week 15: Review and final	