CNT 5415 - Practical Applied Security

Department of Electrical & Computer Engineering

Florida International University

Fall 2018

Classroom	:	SASC- 202
Class Time	:	Tue / Thu (5:00 PM - 6:15 PM)
Instructor	:	Dr. Md Monirojjaman Monshi
Office Hours	:	Wed (3:00 PM - 4:30 PM) or by appointment
Office	:	EC 3265B
Phone	:	(305) 348-2807 (Dept Secretary)
E-mail	:	mmonshi@fiu.edu
Prerequisite	:	Graduate standing and basic knowledge about computer networks

Textbook : Stewart, James M. *Network Security, Firewalls, and VPNs*, 2nd ed., Burlington, MA: Jones & Bartlett, 2014

Course Summary

Course Description

This course offers an introduction to virtual private networks (VPNs) and firewalls for securing a network. Various network security-related issues are introduced and examined. Different types of VPNs for securing data in an organizational setup are discussed as well as the benefits and architecture of a VPN and how to implement a VPN. Other topics include the utility of firewalls in tackling security problems and the limitations of a firewall. In addition, instruction is also given on how to construct, configure, and administer a firewall and the functionality of a firewall.

Major Instructional Areas

1. Network security risks, threats, and vulnerabilities
2. Firewall types, functions, uses, and deployment strategies
3. VPN types, functions, uses, and deployment strategies
4. Network-centric TCP/IP protocols and applications
5. Layered network security strategies
6. Secure network design
7. Best practices and strategies for network security and incident response

Course Objectives

1. Explain the fundamental concepts of network security
2. Describe how network security is implemented and managed
3. Recognize the impact that malicious exploits and attacks have on network security
4. Identify Firewall and VPN basics and technologies
5. Follow the creation of an example Firewall on Client/Server
6. Follow the creation of an example VPN on Client/Server
7. Recognize prospectives, resources and future of network security

Learning Materials and References

Available Resources

- Stewart, James M. *Network Security, Firewalls, and VPNs*, 2nd ed. Burlington, MA: Jones & Bartlett, 2014 (ISBN: 9781284031676)
- Virtual Security Cloud Labs *
- Student Lab Manual (available within the virtual lab environment) *

* These resources are included in the textbook with given ISBN.

Recommended Resources

Books, Professional Journals

Please use the following author's names, book/article titles, Web sites, and/or keywords to search for supplementary information to augment your learning in this subject.

- Seymour Bosworth, et al.
  Computer Security Handbook, 5th ed. (Chapters 3, 21, and 26)

- Anne Henmi (ed).
  Firewall Policies and VPN Configurations (Chapters 2 and 5)

- John Mairs
  VPNs: A Beginner's Guide

- Noonan et al.
  Firewall Fundamentals

- James M. Stewart, et al.
  CISSP: Certified Information Systems Security Professional Study Guide, 5th ed.

- Michael E. Whitman et al.
  Guide to Firewalls and Network Security

- Ruixi Yuan
  Virtual Private Networks: Technologies and Solutions

- Elizabeth D. Zwicky et al.
  Building Internet Firewalls, 2nd ed.

Professional Associations

- *CERT*
  This Web site provides assistance in understanding and handling security vulnerabilities. It also provides research tools on long-term changes in networked systems and gives training assistance to improve security.
  http://www.cert.org/

- *National Institute of Standards and Technology (NIST)*

This Web site provides access to subject matter experts and also facilitates in research. It also provides career-building resources and opportunities. Pay special focus on Computer Security Resource Center.
http://www.nist.gov/index.html
http://csrc.nist.gov/

- *National Security Agency/Central Security Service (NSA/CSS)*
  This Web site provides guidance on information assurance security solutions and also provides insights on risks, vulnerabilities, mitigations, and threats. It also provides information on cryptologic support.
  http://www.nsa.gov/index.shtml

- *SANS: Computer Security Training, Network Research & Resources*
  This Web site provides information on computer security training through several delivery methods like live and virtual conferences, mentors, online, and onsite. It also provides certification and numerous free security resources.
  http://www.sans.org

Other References

- *Common Vulnerabilities and Exposures (CVE)*
  http://cve.mitre.org

- *Information Assurance Support Environment (IASE): Security Technical Implementation Guides (STIGS)*
  http://iase.disa.mil/stigs/Pages/index.aspx

- Chris May, et al.
  Advanced Information Assurance Handbook
  http://www.dtic.mil/dtic/tr/fulltext/u2/a443478.pdf

Information Search

Use the following keywords to search for additional online resources that may be used for supporting your work on the course assignments:

- Attacker
- C-I-A, C-I-A triad
  Confidentiality, Integrity, Availability
- Defense in Depth
- Demilitarized Zone (DMZ)
- Deny by Default, Allow by Exception
- Exploits
- Filtering
- Firewall
- Firewall Design

- Firewall Management
- Firewall Security
- Hacker
- Hijacking Attacks
- Identity and Access Management (IAM)
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Internet Protocol (IP)
- Load Balancer
- Malicious Code
- Malware
- NetWitness Investigator
- Network Protocol, Networking Protocol
- Network Security
- Nonrepudiation
- Packet Filter
- Policy, Policies
- Protocols
- Proxy Firewall
- Router
- Security
- Security Policies
- Stateful Firewall
- Switch
- TCP/IP
- Threats
- Trojan Horse
- Virtual Private Network (VPN)
- Virus
- VPN Design
- VPN Management
- VPN Security
- Vulnerabilities
- Web Server
- Wireshark
- Worm

Virtual Security Cloud Labs

The online Virtual Security Cloud Labs (VSCL) delivers a cloud computing environment (Accessible through http://www2.jblearning.com/my-account/login , Course Code: **73C9E3**). Students will be able to perform the lab exercises after gaining access to the VSCL by using the password provided in the textbook. These hands-on labs provide a fully immersive mock IT infrastructure enabling students to test their skills with realistic security scenarios; scenarios they will encounter in their future careers. **After finishing each lab exercise, the students should submit their lab reports to Canvas and should take the online assessment quizzes by the end of the week the lab is assigned.**

Course Plan

Suggested Learning Approach

In this course, you will be studying individually and within a group of your peers. As you work on the course deliverables, you are encouraged to share ideas with your peers and instructor, work collaboratively on projects and team assignments, raise critical questions, and provide constructive feedback.

Use the following advice to receive maximum learning benefits from your participation in this course:

DO	DON'T
▪ Do take a proactive learning approach ▪ Do share your thoughts on critical issues and potential problem solutions ▪ Do plan your course work in advance ▪ Do explore a variety of learning resources in addition to the textbook ▪ Do offer relevant examples from your experience ▪ Do make an effort to understand different points of view ▪ Do connect concepts explored in this course to real-life professional situations and your own experiences	▪ Don't assume there is only one correct answer to a question ▪ Don't be afraid to share your perspective on the issues analyzed in the course ▪ Don't be negative towards points of view that are different from yours ▪ Don't underestimate the impact of collaboration on your learning ▪ Don't limit your course experience to reading the textbook ▪ Don't postpone your work on the course deliverables – work on small assignment components every day

Tentative Course Outline

Course textbook: *Network Security, Firewalls, and VPNs*, 2nd edition (Stewart, 2014)

Note: Assignments in the following table are listed when they are due. Guidance/sheets will be provided one week in advance. Text Sheets for classroom discussions will be provided during the class or 2 days in advance.

Category	Activity Title	Week
Lesson 1: Fundamentals of Network Security		***Aug. 21 – 23***
Required Readings	▪ Chapter 1, "Fundamentals of Network Security"	
Discussion	D01. Familiar Domains	
Lesson 2: Firewall Fundamentals		***Aug. 28 – 30***
Required Readings	▪ Chapter 2, "Firewall Fundamentals"	
Discussion	D02. Ingress and Egress Filtering	
Assignment	A01. Selecting Security Countermeasures	
Lesson 3: VPN Fundamentals		***Sep. 4– 6***
Required Readings	▪ Chapter 3, "VPN Fundamentals"	
Assignment	A02. Types of Firewalls	
Lab	*L01. Analyzing IP Protocols with Wireshark*	
Lesson 4: Network Security Threats and Issues		***Sep. 11 - 13***
Required Readings	▪ Chapter 4, "Network Security Threats and Issues" ▪ NIST SP 800-30: Guide for Conducting Risk Assessments (http://csrc.nist.gov/publications/PubsSPs.html)	
Discussion	D03. Social Engineering Defense Issues	
Lab	*L02. Using Wireshark and NetWitness Investigator to Analyze Wireless Traffic*	
Lesson 5: Network Security Implementation		***Sep. 18 - 20***
Required Readings	▪ Chapter 5, "Network Security Implementation"	
Discussion	D04. System Hardening	
Lab	*L03. Configuring a pfSense Firewall on the Client*	

Category	Activity Title	Week
Lesson 6: Network Security Management		***Sep. 25 - 27***
Required Readings	▪ Chapter 6, "Network Security Management" ▪ NIST SP 800-61: Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/PubsSPs.html)	
Discussion	D05. Incident Response Strategies	
Assignment	A03. Security Concerns and Mitigation Strategies	
Lab	*L04. Configuring a pfSense Firewall for the Server*	
Lesson 7: Firewall Basics		***Oct. 2- 4***
Required Readings	▪ Chapter 7, "Firewall Basics"	
Assignment	A04. Post-incident Executive Summary Report	
Lab	*L05. Penetration Testing a pfSense Firewall*	
Lesson 8: Firewall Deployment Considerations		***Oct. 9- 11***
Required Readings	▪ Chapter 8, "Firewall Deployment Considerations"	
Discussion	D06. Firewall Security Strategies	
Lesson 9: Firewall Management and Security Concerns		***Oct. 16 - 18***
Required Readings	▪ Chapter 9, "Firewall Management and Security"	
Discussion Due to: Nov 2	D07. Firewall Implementation Planning	
Lab Due to: Nov 7	*L06. Using Social Engineering Techniques to Plan an Attack*	
Lesson 10: Using Common Firewalls		***Oct. 23 - 25***
Required Readings	▪ Chapter 10, "Using Common Firewalls"	
Exam	Midterm Examination	
Lesson 11: VPN Management		***Oct. 30 – Nov.1***

Category	Activity Title	Week
Required Readings	▪ Chapter 11, "VPN Management"	
Discussion Due to: Nov 16	D08. Developing a VPN Policy and Enforcing VPN Best Practices	
Lab Due to: Nov 14	*L07. Configuring a Virtual Private Network Server*	

Category	Activity Title	Week
Lesson 12: VPN Technologies		***Nov. 6 - 8***
Required Readings	▪ Chapter 12, "VPN Technologies"	
Discussion Due to: Nov 23	D09. Improving VPN Performance and Stability	
Assignment Due to: Nov 21	A05. Create a VPN Connectivity Troubleshooting Checklist	
Lab Due to: Nov 21	*L08. Configuring a VPN Client for Secure File Transfers*	
Lesson 13: Firewall Implementation		***Nov. 13- 15***
Required Readings	▪ Chapter 13, "Firewall Implementation"	
Discussion Due to: Nov 28	D10. What to Protect, Why, and How	
Assignment Due to: Nov 28	A06. Remote Access Security Plan and Documentation	
Lesson 14: Real-World VPNs		***Nov. 20***
Required Readings	▪ Chapter 14, "Real-World VPNs"	
Lab Due to: Dec 5	*L09. Attacking a Virtual Private Network*	
Lesson 15: Perspectives, Resources, and the Future		***Nov. 27 -29***
Required Readings	▪ Chapter 15, "Perspectives, Resources, and the Future"	
Lab Due to: Dec 1	*L10. Investigating and Responding to Security Incidents*	
Lesson 16: Final Examination		***Dec. 4***
Exam	Final Examination	

Academic Calendar

Please refer to the Academic Calendar for official holidays, add/drop/withdrawal dates, etc.

Canvas

The students will be informed of course activities, assignments, etc. through the course Canvas page
(**1178 - CNT5415 - Practical Applied Security - Section U01 - Fall 2018**).

Evaluation and Grading

Evaluation Criteria

The graded assignments will be evaluated using the following weighted categories:

Category	Weight
Attendance / Discussion Participation	10
Lab Reports and Assessment Quizzes	30
Assignments	18
Midterm Exam	17
Final Exam	25
TOTAL	**100**

Grade Letter	Grade Point
A	93+
A-	90
B+	86
B	82
B-	78
C+	74
C	70
D	60
F	59 and below

Academic Integrity

All students must comply with the policies that regulate all forms of academic dishonesty, or academic misconduct, including plagiarism, self-plagiarism, fabrication, deception, cheating, and sabotage.

University's Code of Academic Integrity

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions.

More information can be found at http://academic.fiu.edu/academic_misconduct.html

Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see the Instructor. All missed work must be finished before last two weeks of the following term.

University policies on sexual harassment, and religious holidays, and information on services for students with disabilities

Please visit the following websites:

http://academic.fiu.edu/
http://drc.fiu.edu

Course Policies

 Academic Misconduct: For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at

least a failing grade for the course.

- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade.
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to mmonshi@fiu.edu.
- **On Time:** As in the workplace, on time arrival and preparation are required. Two "lates" are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me in the office hours or by an appointment.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.
- **Any work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

Exam policy

1. Make sure to complete the assigned homeworks in order to do well in the exam.
2. All exams are closed book and closed notes.
3. Use of any electronic device with keyboard or touch screen is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

Good Luck !