Prerequisites: CS 2400 or CS 2420
Credits: 3
Schedule: Tuesday & Thursday: 3:30pm – 4:45pm.
Room: SE 5035
Instructor: Dr. G. Ndjatou
Email: ndjatoug@wpunj.edu
Office: Room 5026 Science East
Phone: 973-720-2515
Office Hours: Tuesday 5:00pm – 6:00pm & Wednesday 4:00 PM – 5:00 PM

Text Books:

Course Objectives:
- To explain how networks work, including the topics of LANs, WANs, service providers, packets, hubs, routers, switches, physical layers, and Internet protocols.
- To introduce students to Information Assurance and Security with a focus on the following information security and information system technologies categories: Firewall, Remote access protection, Access controls, Vulnerability assessment, Penetration testing, Forensics and anti-forensics, Client security, Perimeter defense, Server security, Intrusion detection, Network security, and cyber defense.

Grading:
- Lab Assignments ------ 30%
- Attendance, Homework, and class participation ------ 10%
- Tests 3 tests ------ 60%
- Last Test: (No final exam) Thursday, May 9, 2019 from 2:00pm to 4:30pm

The final letter grade will be assigned as follows: >= 90%: A; 88 - 89%: A-; 85 - 87%: B+; 80 - 84%: B; 78 - 79%: B-; 75 - 77%: C+; 70 - 74%: C; 68 - 69%: C-; 65 - 67%: D+; 60 - 64%: D; <60%: F

Additional Information:
- Last day to withdraw from a class: Wednesday, March 27, 2019.
- Thursday class is replaced by Monday class on February 21, 2019.
- Wednesday class is replaced by Monday class on April 10, 2019.
- Spring Break: March 10, 2019 – March 16, 2019

Learning Outcomes:
Upon completion of this course, students should be able to:
1. Compare and contrast the OSI and Internet models as they apply to contemporary communication protocols.
2. Explain the basic components and media of network systems and distinguish between LANs and WANs.
3. Discuss the concepts and the “building blocks” of today’s data communication networks such as switches, routers, and cabling.
4. Explain the operation and function of 802.1 devices and protocols.
5. Describe the necessary hardware (switches and routers) and components (routing algorithms and protocols) used to establish communication between multiple networks.
6. Define information security and key terms and critical concepts of information security
7. Enumerate the phases of the security systems development life cycle
8. Demonstrate that organizations have a business need for information security
9. Identify the threats posed to information security and the more common attacks associated with those threats, and differentiate threats to the information within systems from attacks against the information within systems
10. Describe the issues facing software developers, as well as the most common errors made by developers, and explain how software development programs can create software that is more secure and reliable.
11. Recognize the important role of access control in computerized information system, and identify and describe widely used authentication factors.
12. Describe firewall technology and the various approaches to firewall implementation.
13. Identify the various approaches to control remote and dial-up access by means of the authentication and authorization of users
14. Describe content filtering technology.
15. Describe the technology that enables the use of virtual private networks.
16. Define and describe the categories and operating models of intrusion detection and prevention systems
17. Define honeypots, honeynets, and padded cell systems.
18. Define the major categories of scanning and analysis tool and describe the specific tools used within each of these categories.
19. Explain the various methods of access control.
20. Explain the basic principles of cryptography.
21. Describe the operating principles of the most popular cryptographic tools.
22. Explicate the major protocols used for secure communications.
23. Describe the nature and execution of the dominant methods of attack used against cryptosystems.
24. Describe how vulnerability assessment and remediation ties into the information security maintenance.
25. Define digital forensics, and describe the management of the digital forensics functions.
26. Describe the process of acquiring, analyzing, and maintaining potential evidentiary material.

**Topical Outline of the Course Content**

1. Introduction to networking
   a. Key aspects of networking
   b. Public and the private parts of the internet
   c. Protocol suites and layering models
   d. How data passes through layers
   e. ISO and OSI seven layer reference model
2. Internet applications and network programming
3. Traditional internet applications
4. Access and interconnection technologies
5. Local area networks: packets, frames, and topologies
6. Wired LAN technology (Ethernet and 802.3)
7. Repeaters, bridges, and switches
8. WAN technologies and dynamic routing
9. Introduction to information security
   a. Layers of security to protect an organization.
   b. Key information security concepts.
   c. Critical characteristic of information
   d. CNSS security model
   e. Components of an information system
   f. Balancing information security and access.
   g. Approaches to information security implementation
   h. The security systems development life cycle.
   i. Security professionals and the organization.
   j. Data responsibility.
10. The need for security
a. Functions of the information security.
b. Threads: compromises to intellectual property; software attacks; deviation in quality of services; espionage or trespass; forces of nature; human error or failure; information extortion; missing, inadequate, or incomplete organizational policy or planning; sabotage or vandalism; theft; technical hardware failure or errors; technical software failure or errors; technological obsolescence.
c. Theft.
d. Attacks: malicious code; hoaxes; back doors; password crack; brute force; dictionary; DOS and DDOS; spoofing; man-in-the-middle; spam; mail bombing; sniffers; social engineering; phishing; pharming;
e. Software design principles
f. Software development security problems: buffer overruns; command injection; cross-site scripting; failure to handle errors; failure to protect network traffic; failure to store and protect data securely; failure to use cryptographically strong random numbers; format string problems; neglecting change control; improper file access; improper use of SSL; information leakage; integer bugs (overflows/underflows); race conditions; SQL injection; trusting network address resolution; unauthorized key exchange; use of magic URLs and Hidden forms; use of weak password-based systems.

11. Firewalls and VPNs
   a. Firewall processing modes
   b. Generations of firewalls
   c. Structures of firewalls
   d. Firewall architectures
   e. Configuring and managing firewalls
   f. Protecting remote connections
   g. Virtual private networks (VPNs)

12. Intrusion detection and prevention systems and other security tools
   a. Intrusion detection and prevention systems
   b. Types of IDPS
   c. IDPS detection methods
   d. Organizational requirements and constraints
   e. IDPSs product features and quality
   f. Strengths and limitations of IDPSs
   g. Deployment and implementation of an IDPS
   h. Measuring the effectiveness of IDPSs
   i. Honeypots, honeynets, and padded cell systems
   j. Scanning and analysis tools: port scanners; firewall analysis tools; operating system detection tools; vulnerability scanners; packets sniffers; wireless security tools.
   k. Biometric access controls

13. Cryptography
   a. Foundation of cryptology
   b. Cypher methods: substitution cypher; transposition cypher; exclusive OR; Vernam cipher; book or running key cypher; hash functions
   c. Cryptographic algorithms; symmetric encryption and asymmetric encryption
   d. Cryptographic tools: Public-key infrastructure; digital signatures; digital certificates; hybrid cryptography systems
   e. Protocols for secure communications
   f. Attacks on cryptosystems: man-in-the-middle attack; correlation attacks; dictionary attacks; timing attacks; defending against attacks

14. Vulnerability assessment and remediation
   a. Penetration testing
   b. Internet vulnerability assessment
   c. Intranet vulnerability assessment
   d. Platform security validation
   e. Wireless vulnerability assessment
   f. Modem vulnerability assessment
   g. Documenting vulnerabilities

15. Digital forensics
Course Policies

Student Conduct In Class Policy Any acts of classroom disruption that go beyond the normal rights of students to question and discuss with the instructor the educational process relative to subject content will not be tolerated, in accordance with the Academic Code of Conduct described in the Student Handbook.

Children In Class Policy Only in extreme cases are children allowed in classroom or laboratory facilities, and then only with the approval of the instructor prior to class.

Electronic Devices in Class Policy
- Cellular phones, pagers, CD players, radios, and similar devices are prohibited in the classroom and laboratory facilities.
- Cellular phones, pagers, calculators and computers are prohibited during examinations and quizzes.
- Reasonable laptop-size computers may be used in lectures for the purpose of taking notes.

Test and Quiz Policy
- No make-up tests. Tests are usually given at the beginning of a lecture.

Preparing for Examinations: Attend lectures, read the chapters and do the exercises assigned at the end of each section. At least 90% of the questions are taken directly from the in-class exercises and the homework exercises. Review the main concepts and the exercises done at the end of each section on which you are being tested.

In Case You Are Late or Absent: It is your responsibility to get the course notes, handouts, and laboratory assignments should you miss a class or be late.

Appeals Policy
- To appeal a grade, send an e-mail to your instructor's e-mail address within two weeks of the grade having been received. Overdue appeals will not be considered.

Incomplete Policy
- Students will not be given an incomplete grade in the course without sound reasons and documented evidence as described in the Student Handbook.
- In any case, for a student to receive an incomplete, he or she must be passing and must have completed a significant portion of the course.

Cheating Policy
- Students are expected to uphold the school’s standard of conduct relating to academic honesty. Students assume full responsibility for the content and integrity of the academic work they submit. The guiding principle of academic integrity shall be that a student's submitted work, examinations, reports, and projects must be that of the student's own work. Students shall be guilty of violating the honor code if they:
  1. Represent the work of others as their own.
  2. Use or obtain unauthorized assistance in any academic work.
  3. Give unauthorized assistance to other students.
  4. Modify, without instructor approval, an examination, paper, record, or report for the purpose of obtaining additional credit.
  5. Misrepresent the content of submitted work.

- The penalty for violating the honor code is severe. Any student violating the honor code is subject to receiving a failing grade for the course and will be reported to the Office of Student Affairs. If a student is unclear about whether a particular situation may constitute an honor code violation, the student should meet with the instructor to discuss the situation.
- For this class, it is permissible to assist classmates in general discussions of computing techniques. General advice and interaction are encouraged. Homework assignments must be completed in groups. However, each student must develop his or her own solutions to the assigned laboratory exercises.
- Students may not "work together" on graded lab assignments. Such collaboration constitutes cheating, unless it is a
A student may not use or copy (by any means) another's work (or portions of it) and represent it as his/her own.

Disabilities Policy
In compliance with the Americans with Disabilities Act (ADA), all qualified students enrolled in this course are entitled to “reasonable accommodations.” Please notify the instructor during the first week of class of any accommodations needed for the course.

Tutoring Assistance  Tutoring is available in the Computer Science department.

Extra Credit  Extra credit will not be accepted late.

Lecture, Laboratory, and Examination Schedule
- You are expected to read each assigned chapter prior to the lecture.
- Homework assignments must be handed the next class. Late homework assignments will not be accepted.
- Laboratory assignments must be handed in one week. Lab assignments that are more than two days late are not accepted. Late lab. assignments are penalized 25%.
- Homework and lab assignments must be handed BEFORE the beginning of the lecture.
- Plan to spend approximately six to eight hours each week on reading, homework, and laboratory assignments.
- Make sure your name and exercise number appear in the upper-left corner of the first page of the exercise.
- If an exercise has multiple sheets, then staple them together. Do not staple different assignments together. Disorganized assignments (pages out of order, mislabeled, unreadable, etc.) will receive a grade of zero. If there are multiple sheets to be handed in, sequence them according to the order you were told to print them in the exercise.