Masters of Science in Cybersecurity

Syllabus for CYB 703 Network Security

NOTE: This syllabus document contains the basic information of this course. The most current syllabus is available in the full course.

This course examines network architectures, threats, and attack surfaces exploited by these threats. Students will look at network traffic inspection, common attacks and defensive techniques like encryption, network segmentation, firewalls, application proxies, honeypots, DMZs, monitoring networks using: intrusion detection and intrusion prevention systems, and network access control

Prerequisite(s)

None

Program Outcomes

This course addresses the following competencies and program outcomes of the Masters of Science in Cybersecurity:

- Program Outcome 1: Interpret and analyze operating system and machine level structures
- Program Outcome 2: Interpret and analyze network protocols Program Outcome 11: Assess trends in computer criminology and social behaviors related to technology use including physical security
- Program Outcome 3: Design, evaluate, and test systems including networks, computers, and hardware for security requirements

Course Outcomes

Upon completing this course, you will be able to do the following:

- Understand essential Transmission Control Protocol/Internet Protocol (TCP/IP) behavior and applications used in IP networking
- Explain the fundamental concepts of network security
- Recognize the impact that malicious exploits and attacks have on network security
- Identify network security tools and discuss techniques for network protection
- Describe the fundamental functions performed by firewalls
- Assess firewall design strategies
- Describe the foundational concepts of VPNs
- Describe network security implementation strategies and the roles each can play within the security life cycle
- Appraise the elements of firewall and VPN implementation and management
- Identify network security management best practices and strategies for responding when security measures fail
- Grasp layered network security strategies, secure network design and best practices and strategies for network security and incident response

Course Requirements/Components

Knowledge Check Quizzes

There are 10 knowledge check quiz consisting of randomized multiple-choice and true/false questions based on the readings for that module. These quizzes are meant to ensure that you have an understanding of foundational concepts and terms related to network security.

Discussions

There are four discussions related to the topic being explored for particular modules.

Lab Assignments

There are three major lab assignments that will require you to access a virtual desktop to complete tasks related to analyzing network protocols and conducting penetration tests. The labs can take a substantial amount of time to complete so don't wait until the last minute to attempt them. I suggest that you play around with the lab tasks in the weeks leading up to the submission deadline.

Final Project

You will be required to design and explain network infrastructure for a mock company. Requirements will be provided in the form of an asset list along with typical functions. You will then have to design the topology and network schematics along with detailed firewall settings

Course Outline

Module 1: Essential TCP/IP Network Protocols and Applications

- TCP/IP Networking and OSI Reference Model
- TCP/IP Protocol Suite & Characteristics

Module 2: Network Security Basics

- Fundamentals of Network Security
- Familiar Domains
- Selecting Security Countermeasures

Module 3: Network Security Threats

- Network Security Threats and Issues
- NIST SP 800-30: Guide for Conducting Risk Assessments
- Social Engineering Defense Issues

Module 4: Network Security Tools and Techniques

- Network Security Implementation
- Firewall Basics
- Host-Based vs. Network-Based IDSs/IPSs

Module 5: Firewall Fundamentals

- Firewall Fundamentals
- Ingress and Egress Filtering

Module 6: Firewall Design Strategies

- Firewall Basics
- Firewall Deployment Considerations
- Firewall Security Strategies

Module 7: VPN Fundamentals

- VPN Fundamentals
- VPN Management
- VPN Technologies

Module 8: Network Security Implementation Strategies

- Network Security Implementation
- System Hardening
- Security Concerns and Mitigation Strategies

Module 9: Firewall and VPN Implementation and Management

- Firewall Management and Security
- Using Common Firewalls
- Firewall Implementation
- Real-world VPNs

Module 10: Network Security Management

- Network Security Management
- Perspectives, Resources, and the Future
- NIST SP 800-61: Computer Security Incident Handling Guide

Module 11: Final Project

Grading

The following grading scale will be used to evaluate all course requirements and to determine your final grade:

Grade	Percentage Range
A	93% or greater
A-	90% - < 93%
B+	87% - < 90%
B	83% - < 87%
B-	80% - < 83%
C+	77% - < 80%
C	73% - < 77%
C-	70% - < 73%
F	0 - < 70%

Assignments	Percentage
Quizzes	20%
Lab Assignments	30%
Class Discussions	30%
Final Project	20%
Total	100%