Course Title: CSCI 43xx Network Defense

Note: The design of this course is mainly based on the accreditation guidelines provided in the Center of Academic Excellence – Cyber Defense (CAE-CD) designation requirements documents about knowledge units of various topics. [++]

Classroom Instruction time: 12 weeks (3 hours per week)

Note: for a regular long semester course, 2-3 weeks can be used for exams, hands-on, or projects.

Prerequisite: Basic understanding of networking technologies (e.g., CSCI 4312 Network Protocols, ITEC 3365 Network Fundamentals) and introduction to cybersecurity (e.g., CSCI 4391 Select Topic - Cyber Attacks and Defense, ITEC 3388 Cyber Security I), or instructor's approval

- **Course Description:**
  This course provides an essential study of network defense, related vulnerability and security issues, and common tools available for network packet analysis and exploitations. Topics to be covered include review of basic concepts and principles related to network defense (networking protocols and cryptography, mission assurance, network policy development and enforcement, etc.), secure network development (network access control, DMZs / proxy servers, network hardening, implementing firewalls, VPNs, etc.), and advanced network defense techniques (honeypots, honeynets, network monitoring, implementing IDS/IPS, etc.)

- **Learning Outcomes:**

  The student, after having successfully completed the class, should be able to
  1. Understand fundamental security issues in computer networks
  2. Understand the common mechanisms used in securing a network
  3. Design a TCP/IP network with IP Security
  4. Design and deploy firewalls to secure a private network
  5. Design and deploy a virtual private network to secure remote connections
  6. Select appropriate methods to detect and counter intrusions to a network
  7. Understand other advanced issues related to network security

- **Course Modules, Submodules, and units***
  * Time required to cover a course unit depends on the content, varying from 30 minutes to 3 hours.

  Module 1: Network Defense Basics and Principles

  Submodule 1 – Network Security Basics

  Unit ND_1: Introduction to Network Security (Review of the OSI Network Reference Model, IP Addressing)
  Unit ND_2: Network Attacks (e.g., session hijacking, Man-in-the-Middle)
  Unit ND_3: DNS and attacks
  Unit ND_4: Cryptography
  Unit ND_5: Security Services (Confidentiality, Data integrity, Origin integrity, Availability, and Non-Repudiability)

Submodule 2 – Defense Principles

Unit ND_6: Network Defense Principles (Minimizing Exposure, Defense in Depth)

Module 2: Network Defense Mechanisms

Submodule 3 – Network Defense Mechanisms (part 1)

Unit ND_7: Network Access Control (internal and external)
Unit ND_8: Firewalls, Proxy Server
Unit ND_9: Implementing Firewall, DMZs
Unit ND_10: Application-layer security: HTTPS
Unit ND_11: Network-layer security: IPSec

Submodule 4 – Network Defense Mechanisms (part 2)

Unit ND_12: Implementing IDS/IPS
Unit ND_13: Network Monitoring
Unit ND_14: Honeypots and Honeynets
Unit ND_15: Network Traffic Analysis

Module 3: Policy, Operation, and Assurance

Unit ND_16: Network Policy Development and Enforcement
Unit ND_17: Network Operational Procedures
Unit ND_18: Mission Assurance

Module 4: Network Defense Hands-on activities

Unit ND_19: lab - Network sniffing using Wireshark
Unit ND_20: lab - Implementing IPSec
Unit ND_21: lab - Setting up honeypots
Unit ND_22: lab - Securing a web server
Unit ND_23: lab – configuring firewall policies
…

- **Textbooks**
  - Chuck Easttom. *Network Defense and Countermeasures: Principles and Practices (3rd Edition) (Pearson IT Cybersecurity Curriculum (ITCC)) 3rd Edition*, Pearson, 2018. ISBN-10: 0789759969; ISBN-13: 978-0789759962
  - Michael Gregg, *The Network Security Test Lab: a step-by-step guide*, Wiley, 2015. ISBN-10: 1118987055; ISBN-13: 978-1118987056

- **Reference Books**
  - James Forshaw, *Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation*, No Starch Press, 2017. ISBN-10: 1593277504; ISBN-13: 978-1593277505
  - Chris Sander, *Practical Packet Analysis, 3E: Using Wireshark to Solve Real-World Network Problems, 3rd Edition*, No Starch Press, 2017. ISBN-10: 1593278020; ISBN-13: 978-1593278021
  - Nainar, Ramdoss, and Orzach, *Network Analysis Using Wireshark 2 Cookbook: Practical recipes to analyze and secure your network using Wireshark 2, 2nd Edition*, Packt Publishing, 2018. ISBN-10: 1786461676; ISBN-13: 978-1786461674

- Matthew Monte, *Network Attacks and Exploitation: A Framework*, Wiley, 2015. ISBN-10: 1118987128; ISBN-13: 978-1118987124

- **Sample Course Outline**

Weeks	Topics
1	Unit ND_1: Review of the OSI Network Reference Model Unit ND_2: Network Attacks (e.g., session hijacking, Man-in-the-Middle)
2	Unit ND_3: Cryptography and Security Services (Confidentiality, Data integrity, Origin integrity, Availability, and Non-Repudiability)
3	Unit ND_4: Network Defense Principles (Minimizing Exposure, Defense in Depth) Unit ND_5: Network Hardening
4	Unit ND_6: Network Analysis Tools Unit ND_7: Network Access Control (internal and external)
5	Unit ND_8: DMZs / Proxy Servers Unit ND_9: Implementing Firewalls and VPNs
6	Unit ND_10: Application-layer security: HTTPS Unit ND_11: Network-layer security: IPSec
7	Unit ND_12: Implementing IDS/IPS
8	Unit ND_13: Network Monitoring
9	Unit ND_14: Honeypots and Honeynets
10	Unit ND_15: Network Traffic Analysis
11	Unit ND_16: Network Policy Development and Enforcement
12	Unit ND_17: Network Operational Procedures Unit ND_18: Mission Assurance

- **Evaluation**

category	percentage
Hands-on projects (3)	30%
Exam #1	25%
Exam #2	30%
Paper	10%
Participation	5%

++ Source: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

CAE-CD Technical Core KUs

- Basic Cryptography
- Basic Networking
- Basic Scripting and Programming
- Network Defense
- Operating Systems Concepts

Network Defense (NDF)

The intent of the Network Defense Knowledge Unit is to provide students with knowledge of the concepts used in defending a network, and the basic tools and techniques that can be taken to protect a network and communication assets from cyber threats.

Topics

Because of the nature of the material - All topics and sub topics are required in this KU

1. Outline concepts of network defense, such as:
    a. Defense in Depth
    b. Network attacks
    c. Network Hardening
    d. Minimizing Exposure (Attack Surface and Vectors)
2. Network defense/monitoring tools:
    a. Implementing Firewalls
    b. DMZs / Proxy Servers
    c. VPNs
    d. Honeypots and Honeynets
    e. Implementing IDS/IPS
3. Network Operations
    a. Network Security Monitoring
    b. Network Traffic Analysis
4. Network security policies as they relate to network defense/security:
    a. Network Access Control (internal and external)
    b. Network Policy Development and Enforcement

NICE Framework Categories

Securely Provision (SP)	Operate and Maintain (OM)	Oversee and Govern (OV)
Protect and Defend (PR)	Analyze (AN)	Collect and Operate (CO)
Investigate (IN)		