The Peninsula's Community College

Course Content Summary
ITN 266 – Network Security Layers (3 Credits)

TNCC Cybersecurity Program web page: http://tncc.edu/programs/cyber-security

Course Description:

Provides an in-depth exploration of various security layers needed to protect the network. Explores Network Security from the viewpoint of the environment in which the network operates and the necessity to secure that environment to lower the security risk to the network. Includes physical security, personnel security, operating system security, software security and database security. Lecture 3 hours per week.

Statement of Purpose:

This course focuses on providing students with a working knowledge of the concepts and tools used to protect network assets at different layers. Students will be expected to understand how to install and use tools such as Nmap port scanner, AxCrypt encryption, inSSIDer wireless network manager, and several others for the purpose of understanding and implementing network security in the enterprise network environment. This course also includes content, as indicated below in parenthesis behind each learning objective that directly maps to DHS/NSA's Center of Academic Excellence – 2 Year (CAE2Y) criteria.

Course Prerequisites / Corequisites:

ITN 260.

Required Text:

Corporate Computer Security, latest edition.
Author: Boyle, R. J. and Panko, R. R.
Publisher: Pearson.

COURSE OBJECTIVES

Upon completion of this course, the student will have a working knowledge of:

A. The danger to the network presented by various threat agents
B. The concept and principles of in-depth security
C. Physical and personnel security
D. Operating system, application software, and database security

STUDENT LEARNING OUTCOMES

1.0 Physical Security

1.1 Understand the network operating environment and the need for physical security. **(FS9)**
1.2 Identify the threats to security that are unique to physical security. **(CT3)**
1.3 Identify and explain the access controls necessary to physically secure a network facility.
1.4 Understand the necessity for a fire safety program in securing the physical facility.
1.5 Identify and describe the components of fire detection and response.
1.6 Understand the necessity to secure the supporting facilities such as heating, air conditioning, temperature, humidity, etc.
1.7 Understand the technical details associated with Uninterruptible Power Supplies (UPS) and their ability to increase availability.
1.8 Understand and explain the countermeasures to the physical theft of computer or network devices. **(IT8)**
1.9 Understand the necessity to maintain an accurate physical inventory of all computer and network devices.

2.0 Personnel Security

2.1 Understand how employment policies support organizational security. **(FS9) (CT3)**
2.2 Understand the need for the separation of duties.
2.3 Understand the relationship and interaction between the employee job description, performance evaluation, the standards manual and security.
2.4 Understand the relationship between reference checks, background investigations, and interviews.
2.5 Understand the impact of employee education, employee relationships and management and supervisory practices upon security. **(FS12)**
2.6 Understand how continuous employee observation, job rotations, access control and adherence to standards impact security. **(FS12)**
2.7 Understand how terminations due to events such as promotion, resignation, death, retirement, layoff and firing (hostile terminations) should be handled and their potential impact upon security.

3.0 Computer System Security

3.1 Identify and explain the key Linux security components.
3.2 Identify and explain the Linux file systems controls.
3.3 Identify and explain the Linux files used to manage network functions.
3.4 Identify and explain Linux network running process and networking commands.
3.5 Describe the various techniques for hardening Linux operating system applications.
3.6 Identify and explain the key Windows server security components. **(CD6)**
3.7 Identify and explain the value of the Active Directory and its role in security.
3.8 Identify and explain Windows server authentication methods.
3.9 Identify and explain Windows server user and group security methodologies.
3.10 Understand the Windows server security configuration tools, file and folder security, EFS, NAT, and IPSec. **(CD5)**
3.11 Understand the importance of patching and maintaining O/S updates and vulnerability windows. **(CD8) (CD9) (CD10)**
3.12 Demonstrate the application of cyber defense methods to prepare a Linux or Windows system to repel attacks. **(FS9)**

4.0 Local Area Network Security

4.1 Understand the design of the network and its impact upon network security. **(FS9)**
4.2 Understand and explain the components relating to end user access.
4.3 Describe the value associated with policy based security management of the network.
4.4 Understand the impact on network security of IP address assignment.
4.5 Understand the different network media types, their threats and how best to secure them.
4.6 Explain the impact of cable installation on security particularly with regard to plenum cables and risers.
4.7 Understand the threats against routers, hubs and switches and how best to secure them. **(IT5)**
4.8 Understand the employment of firewalls, IDS and auditing in securing the network. **(CT5)**

5.0 Application Software Security

5.1 Understand and explain the software development life cycle and its relation to security. **(FS9)**
5.2 Understand and explain software quality assurance and its relation to security. **(FS9)**
5.3 Understand and explain software configuration management and its relation to security. **(FS9)**
5.4 Understand and explain software testing and its relation to security. **(FS9)**
5.5 Identify and explain the various type of malicious code.
5.6 Understand the buffer overflow problem and the threat it poses to security.
5.7 Understand the importance of maintaining application patches and updates. **(CD8)**
5.8 Understand the importance of hardening applications and resources available (i.e. DISA STIGs).

6.0 Communication Security (FS9)

6.1 Understand the OSI seven layer communication model and the TCP model.
6.2 Identify and explain the various attacks against the communication systems and their countermeasures. **(CT9)**
6.3 Discuss the process of encryption and its key terms.
6.4 Understand the difference between symmetric and asymmetric encryption.
6.5 Explain common cryptographic protocols and discuss how they are applied. **(IC8) (IT5)**
6.6 Understand digital signatures and Public key Encryption. **(CD5)**
6.7 Understand IPSec and Virtual Private Networks. **(CD5)**
6.8 Understand and explain the issues surrounding email security and privacy. **(CD3)**

7.0 Database Security (FS9)

7.1 Understand the concept of a database and the database terms (including aggregation, polyinstantiation, data mining, inference, etc.).
7.2 Understand the different type database and the components that compose database.
7.3 Understand the issues associated with physical database integrity, logical database integrity, element integrity, auditability, access control, user authentication and availability. **(IC10)**
7.4 Understand and explain the issue of two-phase, data redundancy and internal consistency.
7.5 Understand the issue associated with indirect attacks against databases that report only statistical data.
7.6 Understand the security issues associated with multilevel database. **(IC10)**
7.7 Understand the importance of hardening a database and resources available (i.e. DISA STIGs).

CAE2Y Knowledge Unit Domain Index

Course Content KU Indicator	CAE2Y KU Full Domain Name
BD	**Basic Data Analysis**
BS	**Basic Scripting**
CD	**Cyber Defense**
CT	**Cyber Threats**
FS	**Fundamental Security Design Principles**
IA	**Information Assurance Fundamentals**
IC	**Introduction to Cryptography**
IT	**Information Technology System Components**
NC	**Networking Concepts**
PL	**Policy legal Ethics and Compliance**
SA	**Systems Administration**

NOTE: the number following the KU Indicator represents the KU Domain topic as shown in the KU mapping matrix (Excel file).