The Peninsula's Community College

Course Content Summary
ITN 263 – Internet/Intranet Firewalls and E-Commerce Security (4 Credits)

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

Course Description:

Gives an in-depth exploration of firewall, Web security, and e-commerce security. Explores firewall concepts, types, topology and the firewall's relationship to the TCP/IP protocol. Includes client/server architecture, the Web server, HTML and HTTP in relation to Web Security, and digital certification, D.509, and public key infrastructure (PKI).
Lecture 4 hours per week.

Statement of Purpose:

This course focuses on general network security, providing essential terminology, current threats, methods of protection, and future trends. In addition, the course covers firewalls, virtual private networking fundamentals, and best practices. The purpose of this course is to allow the student to develop additional knowledge and skills on perimeter network defenses, including firewalls and intrusion detection systems. 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:

Network Security, Firewalls, and VPNs, second edition.
Author: Stewart, J. M.
Publisher: Jones & Bartlett Learning.

COURSE OBJECTIVES

1.0 Explain the fundamental concepts of network security.
2.0 Describe the fundamental functions performed by firewalls.
3.0 Describe the foundational concepts of VPNs.
4.0 Recognize the impact that malicious exploits and attacks have on network security.
5.0 Describe network security implementation strategies and the roles each can play within the security life cycle.
6.0 Identify network security management best practices and strategies for responding when security measures fail.
7.0 Manage and monitor firewalls, and understand their limitations.
8.0 Assess firewall design strategies.
9.0 Apply firewall management best practices.
10.0 Appraise the firewall and other security options available for personal and small office/home office (SOHO) environments.
11.0 Appraise the elements of VPN implementation and management.
12.0 Describe common VPN technologies.
13.0 Follow the creation of an example firewall implementation.
14.0 Follow the creation of an example VPN implementation.
15.0 Evaluate available resources and trends in network security.

STUDENT LEARNING OUTCOMES

1.0 Fundamentals of Network Security

1.1 Describe the key concepts and terms associated with network security.
1.2 Describe the importance of a written security policy and explain how policies help mitigate risk exposure and threats to a network infrastructure.
1.3 Define network security roles and responsibilities and who within an IT organization is accountable for these security implementations.
1.4 Identify examples of network security concerns or threats that require enhanced security countermeasures to properly mitigate risk exposure and threats. **(CD5)**
1.5 Describe the security requirements needed for wired versus wireless LAN infrastructures in order to provide an enhanced level of security.
1.6 Compare and contrast common network security components and devices and their use throughout the IT infrastructure.

2.0 Firewall Fundamentals (NC4)

2.1 Define firewalls.
2.2 Explain the need for firewalls.
2.3 Describe types of firewalls, including network router/interface firewall, hardware appliance firewall, and host software firewall.
2.4 Explain standard filtering methods, include static packet filtering, NAT services, application proxy filtering, circuit proxy filtering, dynamic packet filtering, stateful inspection filtering, and content filtering.
2.5 Define the meaning of ingress and egress filtering.
2.6 Compare and contrast software and hardware firewalls.
2.7 Illustrate on a typical business network diagram possible placements for a firewall.
2.8 Compare and contrast dual and triple-homed firewalls.

3.0 VPN Fundamentals (NC4)

3.1 Define VPNs.
3.2 Explain the business and personal uses of VPNs.
3.3 Describe the pros and cons of VPNs.
3.4 Illustrate deployment models or architectures of VPNs, including an edge-router, a corporate firewall, a VPN appliance, a remote access server, a site-to-site VPN and supporting devices, and a host-to-host VPN and supporting devices.
3.5 Differentiate between a transport mode VPN and tunnel mode VPN.
3.6 Describe the importance of encryption, authentication, and authorization to VPNs.

4.0 Network Security Threats and Issues

4.1 Describe the motivations of hackers and other malicious computer network intruders.
4.2 Compare and contrast threats from internal and external sources. **(CT9)**
4.3 Describe how accidents, natural disasters, and ignorance affect network security. **(CT9)**
4.4 Explain the risk posed by malicious code.
4.5 Explain the effects of wired and wireless connectivity on network security.
4.6 Describe common network security exploits and attacks, including replay attacks, insertion attacks, fragmentation attacks, buffer overflow attacks, XSS attacks, man-in-the-middle attacks, hijacking attacks, spoofing attacks, covert channels, DoS, DDoS, botnet attacks, and social engineering attacks. **(CT9)**
4.7 Demonstrate how hacker tools exploit vulnerable targets. **(CT9)**

5.0 Network Security Implementation

5.1 Describe elements of network security design. **(FS9)**
5.2 Compare and contrast public and private addressing as well as static and dynamic addressing.
5.3 State the importance of system hardening.
5.4 Describe why authentication, authorization, accounting, and encryption are essential for network security.
5.5 Identify the security concerns of local hosts as well as remote and mobile hosts.
5.6 Define the elements of node security.

6.0 Network Security Management

6.1 List examples of network security best practices.
6.2 Describe the importance of physical security.
6.3 Compose a procedure for incident response.
6.4 Enumerate key components of an effective network security installation.
6.5 Describe the methods of network security assessment.

7.0 Firewall Basics

7.1 Construct examples of common firewall rules. **(SA5)**
7.2 Design a policy to guide effective firewall monitoring and logging.
7.3 Explain the limitations and weaknesses of firewalls.
7.4 Describe methods to manage firewall performance.
7.5 Define the concerns of encryption related to firewalls.
7.6 Evaluate the benefits and drawbacks of firewall enhancements.
7.7 Demonstrate how to access and use firewall management interfaces. **(SA5)**

8.0 Firewall Deployment Considerations (IT5)

8.1 Compose a firewall policy defining what to allow and what to block.
8.2 Describe various firewall security strategies.
8.3 Define the pros and cons of reverse proxy and port forwarding.
8.4 Explain the importance of a bastion host.
8.5 Assess the business impact of security over availability and performance.

9.0 Firewall Management and Security (IT5)

9.1 Describe firewall management best practices.
9.2 Select the best firewall for a given network scenario.
9.3 Demonstrate the use of tools for managing and monitoring a firewall.
9.4 Troubleshoot common firewall problems.
9.5 Write a firewall installation plan.

10.0 Using Common Firewalls

10.1 Configure the firewall on Windows 7.
10.2 Setup a broadband connection device firewall.

11.0 VPN Management (IT5)

11.1 Describe VPN best practices.
11.2 Write a VPN policy.
11.3 Describe the issues involved with deployment, placement, and implementation of a VPN.
11.4 Appraise the threats and attacks against VPNs.
11.5 Contrast the needs and features of personal and enterprise or network VPNs.
11.6 Compare anonymity and privacy.
11.7 Compose an introductory VPN training program for users.
11.8 Formulate a procedure for troubleshooting VPNs.

12.0 VPN Technologies (IT5)

12.1 Contrast hardware and software VPN solutions.
12.2 Describe VPN protocols, their uses, their features, and their problems.
12.3 Explain the problem of using VPNs with NAT.
12.4 Evaluate hardware VPN devices.

13.0 Firewall Implementation

13.1 Install a host software firewall.
13.2 Explain the feature set of the SmoothWall open source firewall software.
13.3 Explain how to install and configure the SmoothWall open source firewall software.
13.4 Explain performance testing with SmoothWall open source firewall software.

14.0 Real-World VPNs

14.1 Create a remote control VPN using remote desktop.
14.2 Evaluate hardware VPN devices.
14.3 Experiment with TOR.
14.4 Setup an internet café VPN client.
14.5 Assess online remote control products, such as GoToMyPC and LogMein.
14.6 Configure an IPSec VPN.

15.0 Perspectives, Resources, and the Future

15.1 Discuss the different types of integrated and specialized firewalls, as well as the advantages and disadvantages of each.
15.2 List additional sources of information related to network security.
15.3 Describe emerging IT and security trends and their impact on network security.
15.4 Identify challenges and advantages presented by the new technologies and emerging threats to network security.
15.5 Explain the difference between an IDS and an IPS.
15.6 Discuss the future of network security, firewalls, and VPNs.

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 2014 KU mapping matrix (Excel file).