Virginia Western Community College
ITN 266
Network Security Layers

Prerequisites
ITN 260

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.

Semester Credits: 3 Lecture Hours: 3 Lab/Clinical/Internship Hours: 0

Required Materials

Textbook:
Corporate Computer Security by Boyle 9780133545197 (Pearson)

Other Required Materials:
none

Course Outcomes

At the completion of this course, the student should be able to:

Physical Security

1.1 Understand the operating environment of the network and the need for physical security.
1.2 Identify the threats to security that are unique to physicals security.
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.

1.9 Understand the necessity to maintain an accurate physical inventory of all computer and network services.

Personnel Security

2.1 Understand how the organization's employment policies support organizational security.

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, interviews.
2.5 Understand the impact of employee education, employee relationships and management and supervisory practices upon security.
2.6 Understand how continuous employee observation, job rotations, access control and adherence to standards impact security.
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.

Computer System Security

3.0 Identify and explain the key Linux security components.
3.1 Identify and explain the Linux file systems controls.
3.2 Identify and explain the Linux files used to manage network functions.
3.3 Identify and explain Linux network running process and networking commands.
3.4 Describe the various techniques for hardening Linux operating system applications.
3.5 Identify and explain the key Windows server security components.
3.6 Identify and explain the value of the Active Directory and its role in security.
3.7 Identify and explain Windows server authentication methods.
3.8 Identify and explain Windows server user and group security methodologies.
3.9 Understand the Windows server security configuration tools, file and folder security, EFS, NAT, and IPSec (CD4)
3.10 Understand the importance of patching and maintaining O/S updates and vulnerability windows. (CD10, CD11, CD13).
3.11 Demonstrate the application of cyber defense methods to prepare a Linux or Windows system to repel attacks.*

Local Area Network Security

4.0 Understand the design of the network and its impact upon network security.
4.1 Understand and explain the components relating to end user access.
4.2 Describe the value associated with policy based security management of the network.
4.3 Understand the impact on network security of IP address assignment.
4.4 Understand the different network media types, their threats and how best to secure them.
4.5 Explain the impact of cable installation on security particularly with regard to plenum cables and risers.

4.6 Understand the threats against routers, hubs and switches and how best to secure them. (IT3, IT4)
4.7 Understand the employment of firewalls, IDS and auditing in securing the network.

Application Software Security

5.0 Understand and explain the software development life cycle and its relation to security.
5.1 Understand and explain software quality assurance and its relation to security.
5.2 Understand and explain software configuration management and its relation to security.
5.3 Understand and explain software testing and its relation to security.
5.4 Identify and explain the various type of malicious code.
5.5 Understand the buffer overflow problem and the threat it poses to security.
5.6 Understand the importance of maintaining application patches and updates. (CD11)
5.7 Understand the importance of hardening applications and resources available (i.e. DISA STIGs).

Communication Security

6.0 Understand the OSI seven layer communication model and the TCP model.
6.1 Identify and explain the threats various attacks against the communication systems and their countermeasures.
6.2 Discuss the process of encryption and its key terms.
6.3 Understand the difference between symmetric and asymmetric encryption.
6.4 Understand digital signatures and Public key Encryption (PKE). (CD4)
6.5 Understand IPSec and Virtual Private Networks (VPN). (CD4)
6.6 Understand and explain the issues surrounding email security and privacy.

Database Security

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

Topical Description

- The danger to the network presented by trusted employees
- The concept and principles of in-depth security
- Physical and personnel security
- Operating system, application software, and database security

1.0 Physical Security
2.0 Personnel Security
3.0 Computer System Security
4.0 Local Area Network Security
5.0 Application Software Security
6.0 Communication Security
7.0 Database Security

Notes to Instructors

- none