Western Technical College

10150118 Network Security 1

Course Outcome Summary

Course Information

Description	Provides an understanding of information security management and technical components of security. The material covers the history and terminology of security and an overview of how to manage an information security program. Topics include legal and ethical issues, risk management, security design (logical and physical) and maintenance. Case studies and hands-on scenarios provide students with opportunities to create solutions to security issues.
Career Cluster	Information Technology
Instructional Level	Associate Degree Courses
Total Credits	3
Total Hours	72

Textbooks

No textbook required.

Program Outcomes

1. Implement computer networks.
2. Implement client systems.
3. Implement server operating systems.
4. Implement network security components.
5. Develop technical documentation.
6. Troubleshoot network systems.

Course Competencies

1. Define the history of security and terminology definitions, assessing risks and security threats.

Criteria

You will know you are successful when

1.1. you identify types of risk
1.2. you identify potential threats to the network
1.3. you describe common security standards
1.4. you explain why a security policy is needed

Learning Objectives

1.a. Understand network security
1.b. Understand security threats and their ramifications
1.c. Understand the goals of network security
1.d. Determine the factors involved in a secure network strategy

2. Develop authentication policies and procedures.

Criteria

You will know you are successful when

2.1. you describe the role of Active Directory Services
2.2. you describe the authentication methods available
2.3. you have used Kerberos
2.4. you use CHAP as an authenticator
2.5. you describe the use of Biometric
2.6. you use encryption

Learning Objectives

2.a. Create strong passwords and store them securely
2.b. Understand how digital certificates are created and why they are used
2.c. Understand what tokens are and how they function
2.d. Understand Kerberos and CHAP

3. Identify attacks and malicious code, intrusion detection.

Criteria

You will know you are successful when

3.1. you describe denial-of-service (DoS) and counter measures
3.2. you describe SYN Flood
3.3. you describe Spoofing and its filters
3.4. you take measure to avoid software exploitation
3.5. you recognize the use of password cracking tools

Learning Objectives

3.a. Explain denial-of-service (DoS)) attacks
3.b. Understand the major types of spoofing attacks
3.c. Detail types of social-engineering attacks and there affects
3.d. List major types of malicious software and identify counter measures
3.e. Explain what honeypots are and how they are employed
3.f. Explain what detection systems are and identify intrusion detection software

4. Describe the concepts and practices of remote access.

Criteria

You will know you are successful when

4.1. you demonstrate the use of RADIUS authentication
4.2. you describe VPN technology and its uses for securing remote access to networks
4.3. you describe the different vulnerabilities associated with telecommuting
4.4. you demonstrate the use of PPTP, L2TP, SSH, IPSec

Learning Objectives

4.a. Understand VPN technology and its use for securing remote access
4.b. Understand the different vulnerabilities associated with telecommunicating
4.c. Understand TACACS, PPTP, L2TP, SSH, and IPSec

5. Plan email security and implement security safe guards.

Criteria

You will know you are successful when

5.1. you describe the need to secure e-mail
5.2. you demonstrate how to safeguard against e-mail vulnerabilities

5.3. you can install countermeasures against spam and hoaxes
5.4. you can install antivirus scanning, fill filtering mail attachments
5.5. you can configure mail clients

Learning Objectives

5.a. Understand the need to secure e-mail
5.b. Understand e-mail vulnerabilities and how to safeguard against them
5.c. Explain the dangers posed by email hoaxes and spam

6. Implement secure Web access.

Criteria

You will know you are successful when

6.1. you have installed safe guards against the vulnerabilities of JavaScript, ActiveX, cookies, CGI, and SMTP relay
6.2. you describe SSL/TLS protocols and implementation on the Internet
6.3. you demonstrated the use of instant messaging and identified the vulnerabilities associated with those applications

Learning Objectives

6.a. Understand the vulnerabilities of JavaScript, buffer overflow, ActiveX, cookies, applets, SMTP relay, and how they are exploited.
6.b. Understand SSLTLS protocols and HTTPS
6.c. Explore common uses of instant messaging

7. Implement secure file and print resources.

Criteria

You will know you are successful when

7.1. you have protected data using access control lists
7.2. you have protected data from viruses
7.3. you describe securing backup and restore procedures
7.4. you audit resource access

Learning Objectives

7.a. Explain the benefits of centralized enterprise directory services
7.b. Identify the major vulnerabilities of FTP
7.c. Secure Windows 2000 based computers

8. Define the role of routers, switches and firewalls in network security.

Criteria

You will know you are successful when

8.1. you install a firewall using zone alarm
8.2. you have installed access list on routers
8.3. you have installed intrusion detection systems (IDS)
8.4. you have implemented IPSec on a VPN

Learning Objectives

8.a. Understand the purpose of a network firewall and the different kinds of firewall available
8.b. Understand the role of routers and switches
8.c. Determine when VPN or RAS technology works to secure a network connection

9. Explore network topologies and media and their role in the network.

Criteria

You will know you are successful when

9.1. you demonstrate usage of various transmission media
9.2. you described how to safely dispose of storage media
9.3. you described the use of various storage media
9.4. you describe the demilitarized zone in the network
9.5. you setup a Network Address Translation (NAT)

9.6. you describe the procedure of tunneling

Learning Objectives

9.a. Spell out the role of tunneling in network security
9.b. Identify the place and role of the demilitarize zone in the network
9.c. Identify and discuss the various types of transmission media
9.d. Understand the various ways to encrypt data
9.e. Properly maintain and destroy stored data

10. Identify the basics of algorithms and how they are used in modern cryptography.

Criteria

You will know you are successful when

10.1. you have a basic understanding of the concepts of cryptography and how they relate to network security
10.2. you implement a key management and certificate lifecycle policy
10.3. you demonstrate the differences between asymmetric and symmetric algorithms
10.4. you demonstrate understanding of public key infrastructure (PKI)

Learning Objectives

10.a. Understand the basics of algorithms and how they are used in cryptography
10.b. Understand the implications of key management and a certificate's lifecycle
10.c. Identify the differences between asymmetric and symmetric algorithms

11. Discover the physical security of data and security.

Criteria

You will know you are successful when

11.1. you can discuss the impact of location on a facility's security
11.2. you can demonstrate the various biometric techniques used for access control
11.3. you explain the importance of fire safety and fire detection
11.4. you explain the importance of physical security
11.5. you explain the need for business continuity

Learning Objectives

11.a. Understand the importance of physical security
11.b. Identify the major material factors when constructing a facility
11.c. Understand how various physical barriers can enhance the protection of vital resources
11.d. Discuss the various biometric techniques used for access control
11.e. Understand the importance of fire safety and fire detection

12. Establish network security forensic identification, education and documentation.

Criteria

You will know you are successful when

12.1. you demonstrate basic forensic methods
12.2. you explain the role of auditing in network security
12.3. you identify assets, vulnerabilities and treats involved in risk management
12.4. you train users in the importance of education in security

Learning Objectives

12.a. Understand the basic computer forensics methods
12.b. Understand the importance of education in security
12.c. Understanding the role of auditing in network security
12.d. Identify how documentation enables and improves systems management and security
12.e. Identify assets, vulnerabilities, and threats involved in risk management
12.f. Understand the disaster recovery planning process