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

Pre/Corequisites

Prerequisite	10150130 Cisco 3: Advanced Routing & Switching OR 10151110 Cybersecurity Operations
Prerequisite	10150192 Windows Server Administration 1
Prerequisite	10150137 Linux Administration

Textbooks

No textbook required.

Success Abilities

1. Live Responsibly: Embrace Sustainability
2. Live Responsibly: Foster Accountability

3. Refine Professionalism: Act Ethically
4. Refine Professionalism: Practice Effective Communication

Program Outcomes

1. Identify security strategies
2. Implement secure infrastructures
3. Conduct security testing
4. Analyze security data
5. Mitigate risk
6. Develop security documentation

Course Competencies

1. Categorize cybersecurity threats and vulnerabilities

Criteria

You will know you are successful when

1.1. you describe the CIA triad and associated risk and control types
1.2. you describe federal privacy laws, IT security governance and management frameworks
1.3. you idenfity the core elements of effective IA end-user training
1.4. you identify malware types and their relationship with endpoint protection platforms
1.5. you analyse offensive attacks and social engineering tactics

Learning Objectives

1.a. Explain the practicality of a "Security Utopia"
1.b. Understand risk terminology and control types
1.c. List federal privacy laws and associated frameworks
1.d. Explain the topics and concepts required for an effective end-user IA training program
1.e. Explain how antimalware systems identify malware
1.f. Understand how Rootkits, Keyloggers, Buffer Overflows, XSS, SQL Injection, HTTP Form Injection, and Poisoning attacks operate

2. Implement an endpoint security and patch management solution

Criteria

You will know you are successful when

2.1. you deploy a windows update server
2.2. you configure group policy settings to require domain clients/servers to acquire updates from the windows update server
2.3. you deploy an endpoint antimalware solution
2.4. you configure clients and servers to be managed by an antimalware server

Learning Objectives

2.a. Deploy a server based windows update solution
2.b. Utilize group policy to configure microsoft clients to retrieve updates from a centralized update server
2.c. Deploy a centralized, managed endpoint protection server
2.d. Configure a microsoft client to be managed by an endpoint protection server

3. Implement a vulnerability scanner, port scanner and a honeypot

Criteria

You will know you are successful when

3.1. you describe the vulnerability management lifecycle
3.2. you demonstrate the use of a protocol analyzer, a port scanner, a vulnerability scanner and a honeypot

3.3. you deploy a commercial vulnerability scanner solution and scan a windows and Linux OS

Learning Objectives

3.a. Understand the Vulnerability Managemetn Lifecycle
3.b. Perform a Security Assessment Tool scan of a local machine and conduct a threat evaluation
3.c. Conduct a detailed port scan
3.d. Analyze ethernet traffic with a protocol analyzer and a traffic aggregator
3.e. Deploy a honeypot and analyze malicious activity
3.f. Differentiate between vulnerabilty scanners and pen testing
3.g. Deploy a Vulnerability Scanner and scan a virtual network with and without administrative credentials

4. Define Mirroring, TAPing, Firewall Types, Proxies and Anomaly/Intrusion Detection/Prevention

Criteria

You will know you are successful when

4.1. you describe the difference between a TAP, a Port Mirror and Bridge types
4.2. you describe the types of host and network firewalls
4.3. you describe the common VPN protocols
4.4. you differentiate between anomaly and intrusion detection and prevention

Learning Objectives

4.a. Identify configuration options for SPAN/Mirroring devices
4.b. Understand the difference between an aggregating and non-aggregating TAP
4.c. Understand capabilities of the Windows Firewall, including the use of IPSEC as an authentication filter
4.d. Deploy a Squid Proxy and configure client access rules
4.e. Identify popular, modern VPN protocols
4.f. Deploy an Intrusion Detection system and create a custom monitoring rule

5. Implement a Bridge for Monitoring and a Firewall with a Transparent HTTPS Proxy

Criteria

You will know you are successful when

5.1. you have installed a firewall and configured it as a transparent proxy/bridge
5.2. you have configured a proxy to block specific types of network traffic
5.3. you have configured a firewall to provide transparent HTTPS proxying

Learning Objectives

5.a. Configure a proxy firewall to act as a transparent proxy
5.b. Configure a firewall to intercept TLS traffic to decrypt and scan
5.c. Create a custom web filter and apply it to an access policy to filter network traffic and block malware
5.d. Create a bridge on a Windows operating system and deploy it as a monitoring device
5.e. Create a bridge on a Linux operating system and deploy it as a monitoring device

6. Explore Network Protocols, their Vulnerabilities, and native encryption with TLS/SSH

Criteria

You will know you are successful when

6.1. you describe why protocols like ICMP are vulnerable
6.2. you idenfity the shortcomings of SNMP v1 and v2 and how to utilize SNMP v3
6.3. you idenfity the primary weakness of DNS and UDP
6.4. you idenfity which protocols support native TLS and SSH encryption
6.5. you demonstrate how to protect vulnerable protocols with IPSEC

Learning Objectives

6.a. Identify how ICMP is manipulated to transmit traffic out-of-band
6.b. Understand the vulnerability of SNMP v1/v2 and the merits of v3
6.c. Identify how ettercap is used to poision ARP and DNS
6.d. Understand how SSL/TLS and SSH protect data in transit
6.e. Understand how iSCSI CHAP hashes are captured and cracked
6.f. Understand how to deploy IPSEC policies on Windows using the netsh advfirewall commands

7. Implement a Secure WebDAV and SFTP server

Criteria

You will know you are successful when

7.1. you deploy a WebDAV server and configure TLS encryption
7.2. you configure account lockout controls native to windows
7.3. you deploy a SFTP server and configure SSH encryption
7.4. you configure fail2ban to protect against brute force and dictionary attacks

Learning Objectives

7.a. Identify how and where private and public keys are stores in the windows certificate repository
7.b. Deploy an IIS WebDAV server with HTTPS
7.c. Deploy a Linux SFTP server with a chroot jail
7.d. Utilize Fail2Ban to protect against brute force and dictionary logon attacks

8. Identify Hahsing, Symmetric and Assymetric Encryption Methods

Criteria

You will know you are successful when

8.1. you have an intermediate understanding of the concepts of cryptography and hashing and how they relate to network security
8.2. you identify the differences between asymmetric and symmetric algorithms
8.3. you describe the difference between file/folder encryption and whole-disk encryption

Learning Objectives

8.a. Understand the difference between a random vs. a pseudorandom number
8.b. Understand how hashing is used for authentication and integrity
8.c. Identify the fundamentals of transpositon and substitution as it relates to choosing effective encryption settings
8.d. Perform public key encryption and private key decryption using the openssl cipher block chain
8.e. Perform file encryption using secret key encryption
8.f. Identify techniques to embed secret messages using Steganography
8.g. Understand the role of the TPM for encrypting files, folders and volumes

9. Implement a secure VPN Solution with whole Drive Encryption

Criteria

You will know you are successful when

9.1. you implement whole disk encryption on a windows workstation
9.2. you deploy and configure a VPN server on a network firewall
9.3. you configure a windows client to connect to a VPN server using a VPN client
9.4. you utilize a packet capture tool and a hex editor to verify network and disk encryption

Learning Objectives

9.a. Understand the purpose of whold disk encryption for confidentiality
9.b. Understand the configuration steps required for an OpenVPN client server connection
9.c. Determine the tools available for testing VPN connections and whole disk encryption

10. Define the history of security and terminology definitions, assessing risks and security threats. --EXPIRE

Criteria

You will know you are successful when

10.1. you identify types of risk
10.2. you identify potential threats to the network
10.3. you describe common security standards
10.4. you explain why a security policy is needed

Learning Objectives

10.a. Understand network security
10.b. Understand security threats and their ramifications
10.c. Understand the goals of network security

10.d. Determine the factors involved in a secure network strategy

11. Establish network security forensic identification, education and documentation. --EXPIRE

Criteria

You will know you are successful when

11.1. you demonstrate basic forensic methods
11.2. you explain the role of auditing in network security
11.3. you identify assets, vulnerabilities and treats involved in risk management
11.4. you train users in the importance of education in security

Learning Objectives

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

12. Discover the physical security of data and security. --EXPIRE

Criteria

You will know you are successful when

12.1. you can discuss the impact of location on a facility's security
12.2. you can demonstrate the various biometric techniques used for access control
12.3. you explain the importance of fire safety and fire detection
12.4. you explain the importance of physical security
12.5. you explain the need for business continuity

Learning Objectives

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