Western Technical College

10151101 Cybersecurity Essentials

Course Outcome Summary

Course Information

Description	Cybersecurity Essentials develops foundational understanding of cybersecurity and how it relates to information and network security. Students are introduced to characteristics of cyber crime, security principles, technologies, and procedures to defend networks and implement data confidentiality, integrity, availability and security controls on networks, servers and applications. This includes security principles, policies, e-discovery and cybersecurity laws.
Career Cluster	Law, Public Safety, Corrections and Security
Instructional Level	Associate Degree Courses
Total Credits	2
Total Hours	36

Textbooks

No textbook required.

Course Competencies

1. Examine the experts and criminals in the cybersecurity world.

Assessment Strategies

1.1. Packet Tracer - Creating a Cyber World
1.2. Packet Tracer - Communicating in a Cyber World
1.3. Lab - Cybersecurity Job Hunt
1.4. Lab - Threat Identification
1.5. Lab - Exploring the world of Cybersecurity Professionals

Criteria

You will know you are successful when

1.1. You meet the minimum standard score or greater on the packet tracer activities and labs.
1.2. You successfully complete the packet tracer activities.
1.3. You successfully complete the labs.

Learning Objectives

1.a. Describe the cybersecurity world.

1.b. Differentiate between cybersecurity criminals and cybersecurity specialists.
1.c. Identify common threats.
1.d. Review spreading cybersecurity threats.
1.e. Recognize how to create more experts.

2. Evaluate the cybersecurity cube.

Assessment Strategies

2.1. Packet Tracer - Exploring File and Data Encryption
2.2. Packet Tracer - Using File and Data Integrity Checks
2.3. Lab - Install a Virtual Machine on a Personal Computer
2.4. Lab - Exploring Authentication, Authorization, and Accounting

Criteria

You will know you are successful when

2.1. You meet the minimum standard score or greater on the packet tracer activities and labs.
2.2. You successfully complete the packet tracer activities.
2.3. You successfully complete the labs.

Learning Objectives

2.a. Explain the three dimensions of the cybersecurity cube.
2.b. Describe the CIA Triad.
2.c. Recognize the states of data.
2.d. Compare cybersecurity countermeasures.
2.e. Review the IT Security Management Framework.

3. Explore cybersecurity threats, vulnerabilities, and attacks.

Assessment Strategies

3.1. Packet Tracer - Configuring WEP/WPA2 PSK/WPA2 Radius
3.2. Lab - Detecting Threats and Vulnerabilities

Criteria

You will know you are successful when

3.1. You meet the minimum standard score or greater on the packet tracer activity and lab.
3.2. You successfully complete the packet tracer activity.
3.3. You successfully complete the lab.

Learning Objectives

3.a. Describe malware and malicious code.
3.b. Explain deception.
3.c. Identify attacks.

4. Characterize the art of protecting secrets.

Assessment Strategies

4.1. Packet Tracer - Configuring VPN Transport Mode
4.2. Packet Tracer - Configuring VPN Tunnel Mode
4.3. Lab - Using Stenography

Criteria

You will know you are successful when

4.1. You meet the minimum standard score or greater on the packet tracer activities and lab.
4.2. You successfully complete the packet tracer activities.
4.3. You successfully complete the lab.

Learning Objectives

4.a. Describe cryptography.
4.b. Compare access controls.
4.c. Differentiate methods to obscure data.

5. Summarize the art of ensuring integrity.

Assessment Strategies

5.1. Lab - Password Cracking
5.2. Lab - Using Digital Signatures
5.3. Lab - Remote Access

Criteria

You will know you are successful when

5.1. You meet the minimum standard score or greater on the lab.
5.2. You successfully complete the lab.

Learning Objectives

5.a. Explain types of data integrity controls.
5.b. Describe digital signatures.
5.c. Review certificates.
5.d. Describe database integrity enforcement.

6. Examine the five nines concept.

Assessment Strategies

6.1. Packet Tracer - Router and Switch Redundancy
6.2. Packet Tracer - Router and Switch Resilience

Criteria

You will know you are successful when

6.1. You meet the minimum standard score or greater on the packet tracer activities.
6.2. You successfully complete the packet tracer activities.

Learning Objectives

6.a. Explain high availability.
6.b. Compare measures to improve availability.
6.c. Describe incident response.
6.d. Review disaster recovery.

7. Explore protecting a cybersecurity domain.

Assessment Strategies

7.1. Packet Tracer - Server Firewalls and Router ACLs
7.2. Lab - Hardening a Linux System

Criteria

You will know you are successful when

7.1. You meet the minimum standard score or greater on the packet tracer and lab.
7.2. You successfully complete the packet tracer activity.
7.3. You successfully complete the lab.

Learning Objectives

7.a. Summarize defending systems and devices.
7.b. Explain server hardening.
7.c. Describe network hardening.
7.d. Identify physical security.

8. Evaluate becoming a cybersecurity specialist.

Assessment Strategies

8.1. Paper on Cybersecurity Domains
8.2. Presentation on Cybersecurity Domains

Criteria

You will know you are successful when

8.1. You meet the minimum standard score or greater on the paper and presentation.
8.2. You successfully complete the paper.

8.3. You successfully complete the presentation.

Learning Objectives

8.a. Identify the different cybersecurity domains.
8.b. Summarize the ethics of working in cybersecurity.
8.c. Explore the cyber security profession.