Western Technical College

10151110 Cisco 3: Cybersecurity Operations

Course Outcome Summary

Course Information

Description	Cybersecurity Operations covers the knowledge and skills needed for a Security Analyst working with a Security Operations Center team. It imparts the core security skills needed for monitoring, detecting, investigating, analyzing and responding to security events in order to protect systems and organizations from cybersecurity risks, threats and vulnerabilities.
Career Cluster	Law, Public Safety, Corrections and Security
Instructional Level	Associate Degree Courses
Total Credits	3
Total Hours	90

Textbooks

No textbook required.

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. Identify the role of the Cybersecurity Operations Analyst in the enterprise.

Assessment Strategies

1.1. Lab - Cybersecurity Case Studies
1.2. Lab - Learning the Details of Attacks

1.3. Lab - Becoming a Defender

Criteria

You will know you are successful when

1.1. you explain why networks and data are attacked
1.2. you explain how to prepare for a career in Cybersecurity operations.
1.3. you identify skills needed to become a network defender

Learning Objectives

1.a. Explore why networks and data are attacked
1.b. Examine career preparation opportunities in Cybersecurity operations.
1.c. Research what it takes to become a network defender

2. Describe the features and characteristics of Windows Operating Systems.

Assessment Strategies

2.1. Lab - Exploring Processes, Threads, Handles, and Windows Registry
2.2. Lab - Monitor and Manage System Resources in Windows
2.3. Lab - Windows Task Manager

Criteria

You will know you are successful when

2.1. you explain the operation of the Windows Operating System.
2.2. you explain how to secure Windows endpoints
2.3. you manage processes from within Task Manager

Learning Objectives

2.a. Examine the operation of the Windows Operating System.
2.b. Identify how to secure Windows endpoints
2.c. Explore Task Manager and manage processes from within Task Manager

3. Describe the features and characteristics of Linux Operating Systems.

Assessment Strategies

3.1. Lab - Working with Text files in the Linux CLI
3.2. Lab - Getting Familiar with the Linux Shell
3.3. Lab - Locating Log Files
3.4. Lab - Linux Servers

Criteria

You will know you are successful when

3.1. you explain basic operations in the Linux shell
3.2. you execute basic Linux administration tasks.
3.3. you execute basic security-related tasks to protect a Linux host.

Learning Objectives

3.a. Explore basic operations in the Linux shell
3.b. Use basic Linux administration tasks.
3.c. Use basic security-related tasks on a Linux host.

4. Analyze the operation of network protocols and services.

Assessment Strategies

4.1. Lab - Tracing a Route
4.2. Lab - Using Wireshark to Examine Ethernet Frames
4.3. Lab - Using wireshark to Observe the TCP 3-Way Handshake
4.4. Lab - Exploring Nmap

Criteria

You will know you are successful when

4.1. you explain how protocols enable network operations.
4.2. you explain how the Ethernet and IP protocols support network communication.

4.3. you explain how transport layer protocols and network services support network functionality.
4.4. you apply common testing utilities to verify and test network connectivity.

Learning Objectives

4.a. Explore how protocols enable network operations.
4.b. Examine how the Ethernet and IP protocols support network communication.
4.c. Use common testing utilities to verify and test network connectivity.
4.d. Examine how transport layer protocols and network services support network functionality.

5. Use network monitoring tools to identify attacks against network protocols and services

Assessment Strategies

5.1. Lab - Anatomy of Malware
5.2. Lab - Social Engineering
5.3. Lab - Exploring DNS Traffic
5.4. Lab - Attacking MySQL Database
5.5. Lab - Reading Server Logs

Criteria

You will know you are successful when

5.1. you explain network traffic monitoring.
5.2. you explain how TCP/IP vulnerabilities enable network attacks.
5.3. you describe how common network applications and services are vulnerable to attack.

Learning Objectives

5.a. Explore network traffic monitoring.
5.b. Reasearch how TCP/IP vulnerabilities enable network attacks.
5.c. Examine ways common network applications and services are vulnerable to attack.

6. Use various methods to prevent malicious access to computer networks, hosts, and data

Assessment Strategies

6.1. Lab - Encrypting and Decrypting Data Using OpenSSL
6.2. Lab - Encrypting and Decrypting Data Using a Hacker Tool
6.3. Lab - Examining Telnet and SSH in Wireshark
6.4. Packet Tracer - Identify Packet Flow

Criteria

You will know you are successful when

6.1. you explain approaches to network security defense.
6.2. you explain access control as a method of protecting a network.
6.3. you explain how firewalls and other devices prevent network intrusions.
6.4. you summarize how content filtering prevents unwanted data from entering the network.
6.5. you apply various intelligence sources to locate current security threats.

Learning Objectives

6.a. Research approaches to network security defense.
6.b. Explore access control as a method of protecting a network.
6.c. Identify how firewalls and other devices prevent network intrusions.
6.d. Identify how content filtering prevents unwanted data from entering the network.
6.e. Research various intelligence sources to locate current security threats.

7. Investigate endpoint vulnerabilities and attacks

Assessment Strategies

7.1. Lab - Setup a Mulit-VM Environment
7.2. Packet Tracer - Explore a NetFlow Implementation
7.3. Packet Tracer - Logging from Multiple Sources

Criteria

You will know you are successful when

7.1. you use a tool to generate a malware analysis report.
7.2. you classify endpoint vulnerability assessment information.

Learning Objectives

7.a. Research tools to generate malware analysis reports.
7.b. Classify endpoint vulnerability assessment information.

8. Evaluate network security alerts

Assessment Strategies

8.1. Lab - Setup a Multi-VM Environment
8.2. Packet Tracer - Logging network Activity

Criteria

You will know you are successful when

8.1. you explain how security technologies affect security monitoring.
8.2. you explain the types of log files used in security monitoring
8.3. you generate log files.

Learning Objectives

8.a. Explore how security technologies affect security monitoring.
8.b. Explore the types of log files used in security monitoring

9. Analyze network intrusion data to identify compromised hosts and vulnerabilities

Assessment Strategies

9.1. Lab - Snort and Firewall Rules
9.2. Lab - Convert Data into a Universal Format
9.3. Lab - Regular Expression Tutorial
9.4. Lab - Extract an Executable from a PCAP
9.5. Lab - Interpret HTTP and DNS Data to Isolate Threat Actor
9.6. Lab - Isolate Compromised Host using 5-Tuple

Criteria

You will know you are successful when

9.1. you explain how security-related data is collected.
9.2. you arrange a variety of log files in preparation for intrusion data analysis
9.3. you analyze intrusion data to determine the source of an attack.

Learning Objectives

9.a. Examine how security-related data is collected.
9.b. Research a variety of log files in preparation for intrusion data analysis
9.c. Identify intrusion data to determine the source of an attack.

10. Apply incident response models to manage network security incidents

Assessment Strategies

10.1. Lab - Incident Handling

Criteria

You will know you are successful when

10.1. you apply incident response models to an intrusion event.
10.2. you identify a threat actor and recommend an incident response plan.

Learning Objectives

10.a. Research incident response models to an intrusion event.
10.b. Examine a threat actor and incident response plan.