Montgomery County Community College
CIS 208
Implementing CISCO Cyber Operations
3-2-2

COURSE DESCRIPTION:
This course will teach a student the knowledge and skills required to build, scale, secure, and defend the networks that are used in our businesses and daily lives. Students will also focus on various types of cyber-attacks and use tools and techniques in a virtual machine environment that allows them to create, implement, monitor, and detect malicious activity. The hands-on training is performed in this environment so that students can gain the necessary skills and knowledge needed to thwart these and future cyber-attacks in a Security Operations Center environment This course will prepare a student for entry level cyber security jobs and aligns with the CISCO CyberOps Associate certification.

PREREQUISITE(S):
CIS 171 - Switching, Routing and Wireless Essentials with a “C” or higher

COREQUISITE(S):
CIS 141 – Introduction to Linux

Upon successful completion of this course, the student will be able to:

LEARNING OUTCOMES	LEARNING ACTIVITIES	EVALUATION METHODS
1. Identify the security threats and issues facing modern Network infrastructures.	Lecture/Discussion Hands-On Lab Exercises Homework Assignments Assigned readings Research	Discussion/Questions Chapter Quiz Lab Completion Reports
2. Use the Windows Operating System and Linux OS features and characteristics needed to support cybersecurity analyses.	Lecture/Discussion Hands-On Lab Exercises Homework Assignments Assigned readings Research	Discussion/Questions Chapter Quiz Lab Completion Reports
3. Identify the operation of the network infrastructure and monitoring tools to identify attacks against network protocols and services.	Lecture/Discussion Hands-On Lab Exercises Homework Assignments Assigned readings Research	Discussion/Questions Chapter Quiz Lab Completion Reports
4. Demonstrate how to prevent malicious access to computer	Lecture/Discussion Hands-On Lab Exercises Homework Assignments	Discussion/Questions Chapter Quiz Lab Completion Reports

networks, hosts, and data.	Assigned readings Research	
5. Demonstrate the use of cryptography and encryption to implement network and file security.	Lecture/Discussion Hands-On Lab Exercises Homework Assignments Assigned readings Research	Discussion/Questions Chapter Quiz Lab Completion Reports
6. Apply incident response models to manage network security incidents	Lecture/Discussion Skills-based assessment Homework Assignments Assigned readings Research	Results of final Skills based assessment and written final exam.

At the conclusion of each semester/session, assessment of the learning outcomes will be completed by course faculty using the listed evaluation method(s). Aggregated results will be submitted to the Director of Educational Effectiveness. The benchmark for each learning outcome is that 70% of students will meet or exceed outcome criteria.

SEQUENCE OF TOPICS:

Module/Topics	Goals/Objectives
1. The Danger	Explain why networks and data are attacked.
2. Fighters in the War Against Cybercrime	Explain how to prepare for a career in cybersecurity operations.
3. The Windows Operating System	Explain the security features of the Windows operating system
4. Linux Overview	Implement basic Linux security.
5. Network Protocols	Explain how protocols enable network operations.
6. Ethernet and Internet Protocol (IP)	Explain how the ethernet and IP protocols support network communications.
7. Principles of Network Security	Connectivity Verification
8. Address Resolution Protocol	Analyze address resolution protocol PDUs on a network.
9. The Transport Layer	Explain how transport layer protocols support network functionality.
10. Network Services	Explain how network services enable network functionality
11. Network Communication Devices	Explain how network devices enable wired and wireless network communication.
12. Network Security Infrastructure	Explain how network devices and services are used to enhance network security.
13. Attackers and Their Tools	Explain how networks are attacked.
14. Common Threats and Attacks	Explain the various types of threats and attacks

15. Observing Network Operation	Explain network traffic monitoring.
16. Attacking the Foundation	Explain how TCP/IP vulnerabilities enable network attacks.
17. Attacking What We Do	Explain how common network applications and services are vulnerable to attack
18. Understanding Defense	Explain approaches to network security defense.
19. Access Control	Explain access control as a method of protecting a network.
20. Threat Intelligence	Use various intelligence sources to locate current security threats.
21. Cryptography	Explain how the public key infrastructure supports network security.
22. Endpoint Protection	Explain how a malware analysis website generates a malware analysis report.
23. Endpoint Vulnerability Assessment	Explain how endpoint vulnerabilities are assessed and managed
24. Technologies and Protocols	Explain how security technologies affect security monitoring.
25. Network Security Data	Explain the types of network security data used in security monitoring.
26. Evaluating Alerts	Explain the process of evaluating alerts.
27. Working with Network Security Data	Interpret data to determine the source of an alert.
28. Digital Forensics and Incident Analysis and Response	Explain how the CyberOps Associate responds to cybersecurity incidents.

LEARNING MATERIALS:

- Cisco NetAcademy
- NDG Online Labs - Cisco CyberOps Associate - Online Courses & Labs Training | NDG (netdevgroup.com)
- CEH Certified Ethical Hacker Cert Guide, 4th Edition, Michael Gregg, Pearson Technology Group, 2022, ISBN-13: 978-0-13-748998-5

COURSE APPROVAL:

Prepared by: Marie Hartlein Date: 2/11/2020

VPAA/Provost or designee Compliance Verification:

Victoria Bastecki-Perez, Ed.D. Date: 2/12/2020

Revised by: Anthony E. Stevens Date: 10/03/2022

VPAA or designee Compliance Verification: Date: 2/22/2023

This course is consistent with Montgomery County Community College's mission. It was developed, approved and will be delivered in full compliance with the policies and procedures established by the College.