ROCHESTER COMMUNITY AND TECHNICAL COLLEGE COMMON COURSE OUTLINE

Course discipline/number/title: COMP 1080: Networking Protocols and Analysis

A. CATALOG DESCRIPTION
1. Credits: 4
2. Hours/Week: 4 hours lecture
3. Prerequisites (Course discipline/number): COMP 1150, MATH 0099
4. Other requirements: None
5. MnTC Goals (if any): NA

B. COURSE DESCRIPTION: This class examines the basic principles of networking, transitioning from protocols (TCP, UDP, ICMP, and IP), network architecture, and the OSI model into network defense. Networks are the lifeblood of an organization as packets transition from one device to another through internal and external communications. Cybersecurity professionals must have a strong understanding of network processes, protocols, and administration. This course will focus on developing skills in creating network architecture, network administration, network analysis, and how to apply this knowledge to improve the network security posture through defense in depth.

C. DATE LAST REVISED (Month, year): November, 2023

D. OUTLINE OF MAJOR CONTENT AREAS:
1. Introduction to Networking Fundamentals
   a) Basic Networking Concepts
   b) Network Services and Connections
2. Network Topologies and Cloud Technologies
   a) Types of Network Topologies
   b) Introduction to Cloud Networking
3. Routing Technologies and Devices
   a) Ethernet, LAN, and WAN
   b) SDN, NAT, and Wireless Networking
4. Network Protocols: TCP, UDP, ICMP, and IP
   a) OSI Model Overview
   b) Protocol Classification and Roles
5. Identifying Threats to Networks
   a) System Protection Strategies
   b) Introduction to Cryptography
6. Wireless Security
   a) Wireless Protocols and Risks
   b) Secure Wireless Configuration
7. Monitoring and Optimization
   a) Network Monitoring Tools
   b) Optimization for Business Continuity
8. Disaster Planning in Network Security
   a) Disaster Planning Strategies
   b) Risk Analysis in Networking
9. Policy Development and Physical Security
   a) Policy Guidelines and Implementation
   b) Role of Physical Security
10. The Economics and Ethics of Network Security
    a) Cost-Benefit Analysis
    b) Legal and Ethical Considerations
11. Common Network Troubleshooting Techniques
    a) Connectivity Issues
    b) Software Challenges
12. Network Hardening Practices
    a) Best Practices for Secure Configuration
    b) Security Impact Assessment

E. LEARNING OUTCOMES (GENERAL): The student will be able to:
1. Design network architecture focusing on security and performance.
2. Classify networking devices and their impacts to network security at an organizational level.
3. Distinguish between the seven layers of the OSI model and what protocols are involved at the various levels.
4. Interpret network packets and identify signs of threats to the organization.
5. Identify network threats through protocol and device analysis and the impacts on the security of the enterprise.
6. Define and implement network hardening practices.
7. Discern the differences between and analyze TCP, UDP, IP, ICMP, and other networking protocols.

F. LEARNING OUTCOMES (MNTC): NA

G. METHODS FOR EVALUATION OF STUDENT LEARNING: Methods may include but are not limited to:
1. Tests
2. Lab Exercises
3. Programming assignments
4. Comprehensive Final Exam

H. RCTC CORE OUTCOME(S). This course contributes to meeting the following RCTC Core Outcome(s): Critical Thinking. Students will think systematically and explore information thoroughly before accepting or formulating a position or conclusion.

I. SPECIAL INFORMATION (if any): None