

CPSC 6126 Introduction to Cybersecurity

Course Objectives (CLO)

By the end of this course you should be able to:

1. Define and use key terms and concepts in the field of cybersecurity,
2. Identify and distinguish common threats to computer and network systems,
3. Match appropriate types of controls to defend against common threats to computer and network systems,
4. Explain how cryptography is used in securing information and communications,
5. Discuss the role of human in cybersecurity,
6. Explain the significance of an effective security policy and critique existing security policies,
7. Demonstrate basic technical skills in using tools to attack and defend computer systems and networks.

Module 1: Introduction

By the end of this module you should be able to:

1. Provide definitions for confidentiality, integrity and availability in the context of information security, (aligned with CLO1)
2. Apply definitions of confidentiality, integrity, availability in a given scenario, (aligned with CLO1)
3. Define and explain the relationship between threat, vulnerability, and risk, (aligned with CLO1, CLO2)
4. Demonstrate basic skills in using core commands in the operating system Linux. (aligned with CLO7)

Module 2: Authentication

1. Explain the role of identification and authentication in information security, (aligned with CLO3)
2. Explain pros and cons of various types of authentication mechanisms including biometric authentication, (aligned with CLO3)
3. Distinguish multi-factor authentication from non-multi-factor authentication, (aligned with CLO1, CLO3)
4. Distinguish mutual authentication from multi-factor authentication, (aligned with CLO1, CLO3)

5. Explain password storage mechanisms and attacks against passwords, (aligned with CLO3, CLO4)
6. Demonstrate basic skills in creating user accounts and groups in the Linux operating system, (aligned with CLO7)
7. Apply password cracking techniques in an isolated secure environment, (aligned with CLO7)

Module 3: Access Control

1. Explain the role of access control in implementing information security, (aligned with CLO1, CLO2, and CLO3).
2. Compare and contrast access control mechanisms including access control directory, matrix, list, and capabilities, (aligned with CLO1 and CLO3).
3. Examine the principles that underlie effective access control mechanisms (aligned with CLO1 and CLO3).
4. Demonstrate basic skills in setting up file permissions for access control in Linux (aligned with CLO7).

Module 4: Cryptography

1. Define encryption, decryption, plain text, cipher text, and can explain their role in cryptography. (aligned with CLO1, CLO4)
2. Use classical cipher methods such as Caesar cipher and substitution cipher to encrypt/decrypt data by hand. (aligned with CLO2 and CLO4)
3. Compare and contrast symmetric and asymmetric encryption. (aligned with CLO4)
4. Identify well-known algorithms of symmetric and asymmetric encryption. (aligned with CLO1 and CLO4)
5. Explain the use of hash functions in securing information. (aligned with CLO4)
6. Explain the use of digital signatures in securing information. (aligned with CLO4)
7. Explain the role of digital certificates and certificate authorities in secure communications. (aligned with CLO4)
8. Utilize tools to demonstrate how public key and symmetric key cryptography work. (aligned with CLO7)
9. Utilize tools to demonstrate how hashing works. (aligned with CLO7)

Module 5: Programming Vulnerabilities

1. Explain programming oversights including buffer overflows, off-by-one errors, incomplete mediation, time-of-check to time-of-use error and the impact they may have on a computer, (aligned with CLO1 and CLO2)
2. Compare and contrast different kinds of malware including viruses, worms, Trojan horses, ransomware (aligned with CLO2)
3. Discuss countermeasures against programming vulnerabilities (aligned with CLO3)
4. Demonstrate basic skills in using tools for analyzing malware (aligned with CLO7)

Module 6: OS Security

1. Explain the basic security functions provided by operating systems (aligned with CLO3)
2. Summarize operating system design principles (aligned with CLO1 and CLO3)
3. Describe how operating systems control access to resources (aligned with CLO1 and CLO3)
4. Explain characteristics of operating system rootkits (aligned with CLO2)
5. Demonstrate basic skills in using tools for analyzing rootkits (aligned with CLO7)

Module 7: Web User side

1. Describe and distinguish attacks against browsers, and to and from web sites, including attacks via email (aligned with CLO1 and CLO2)
2. Match countermeasures against various web attacks (aligned with CLO3)
3. Demonstrate a basic XSS injection attack. (aligned with CLO7)

Module 8: Network Security

1. Demonstrate a basic understanding and knowledge of the networking concepts of network transmission media, protocol layers, addressing and routing. (aligned with CLO1)
2. Describe and distinguish different types of threats to network communications including wiretapping, eavesdropping, port scanning, data corruption, and loss of service. (aligned with CLO2)
3. Explain the threats to wireless networks and defenses against these threats. (aligned with CLO2 and CLO3)
4. Explain how cryptography is used in securing networks. (aligned with CLO3 and CLO4)
5. Explain types of firewalls and how they work. (aligned with CLO3)
6. Explain how intrusion detection and prevention systems work. (CO3)
7. Demonstrate how some of the network attacks work in a simulated environment. (aligned with CLO7)

8. Utilize network defense tools in a simulated environment. (aligned with CLO7)

Module 9: Cloud Computing

1. Define what a cloud service is (aligned with CLO1)
2. Explain the risks to consider when choosing cloud services (aligned with CLO2)
3. Compare and contrast security concerns in traditional networks and cloud services (aligned with CLO2 and CLO3)

Module 10: Human Aspects and Policy

1. Examine privacy principles and policies in the cyberspace (aligned with CLO1 and CLO5)
2. Explain threats to privacy and countermeasures against them in the cyberspace (aligned with CLO2 and CLO5)
3. Discuss the human factor in cybersecurity and measures for defending against it. (aligned with CLO5)
4. Explain the significance of policies in protecting information, (aligned with CLO6)
5. Evaluate a security policy to identify vulnerabilities. (aligned with CLO6)