

Cybersecurity II

Level 3: Student explored previously; second pathway specific course

Pathway(s): Networking Systems & Security

Description

Cybersecurity II challenges students to develop advanced skills in concepts and terminology of cybersecurity. This course builds on previous concepts introduced in Cybersecurity I while expanding the content to include malware threats, cryptography, wireless technologies and organizational security. Upon completion of this course, proficient students will demonstrate an understanding of cybersecurity ethical decisions, malware threats, how to detect vulnerabilities, principles of cryptology, security techniques, contingency plan techniques, security analysis, risk management techniques, and advanced methods of cybersecurity.

Student Learning Outcomes

Legal and Ethical Concepts in Cybersecurity

- 1) Analyze current legislation that governs computer related crimes.
- 2) Research and report on current legal cases involving acts of computer crime.
- 3) Analyze methods used to collect evidence to support legal cases involving computer related crimes.

Malware Threats

- 4) Determine various forms of malware.
- 5) Analyze methods to handle malware.
 - a. Encryption techniques
 - b. Basic input/output system (BIOS) features
 - c. Strategies for dealing with malware

Threats and Vulnerabilities

- 6) Differentiate among various types of attacks on systems and networks.
 - a. Virus
 - b. Worms
 - c. Trojans
 - d. Unpatched software
 - e. Password cracking
 - f. Advanced persistent threat
 - g. Reconnaissance/footprinting
 - h. Infiltration
 - i. Network breach
 - j. Network exploitation
 - k. Attack for effects (e.g., deceive, disrupt, degrade, and destroy)
 - l. DoS/DDoS, session hijacking
 - m. HTTP spoofing

- n. DNS attacks
- o. Switch attacks
- p. Man-in-the-middle (MITM) attacks
- q. Cross site scripting
- r. Drive-by-attacks

Principles of Cryptology

- 7) Analyze cryptographic tools, procedures for use, and products.
 - a. PKI Certificates
 - b. PGP
 - c. Certificate authorities
- 8) Develop a simple public key infrastructure to be used in a small business.
- 9) Demonstrate the create of a self-signed certificate for use on a web server by using command line or online tools.

Wireless Security Techniques

- 10) Analyze attack methods on wireless networks.
- 11) Demonstrate the use of wireless security protocols.
- 12) Evaluate the capabilities of WPA, WPA-2, and WEP and the effectiveness of the security protocols and demonstrate how to use them appropriately.

Organizational Security Techniques

- 13) Analyze, define, and demonstrate the use of environmental controls.
- 14) Work collaboratively to develop simple policies that support the operations of security in an organization.
- 15) Research and analyze security awareness in organizations.
 - a. Security policy training and procedures
 - b. Personally identifiable information
 - c. Information classifications
 - d. Data labeling, handling, and disposal
 - e. Compliance with laws, best practices, and standards
 - f. User habits
 - g. Threat awareness
 - h. Use of social networking

Contingency Planning Techniques

- 16) Analyze and define the impact of security incidents on an organization.
- 17) Research and define what a disaster recovery (DR) plan is and how to develop one.
 - a. Preventative measures
 - b. Detective measures
 - c. Corrective measures

Security Analysis Evaluation

- 18) Explore and identify various assessment methods including but not limited to network penetration and vulnerability testing.
- 19) Identify and explain the use of security testing tools.

20) Demonstrate and compare effectiveness of Nessus and Nmap.

21) Demonstrate each of the following concepts:

- a. Evaluate the patch status on a machine.
- b. Demonstrate knowledge of packet-level analysis in order to install and view packets.
- c. Perform secure data destruction (e.g. Secure Erase, BCWipe).

Advanced Methods of Cybersecurity

22) Demonstrate proper secure network configuration and administration.

- a. Applying and implementing secure network administration principles.
- b. Demonstrating knowledge of how network services and protocols interact to provide network communications in order to securely implement and use common protocols.
- c. Identify commonly used default network ports.
- d. Setting up a Network Address Translation (NAT) device.
- e. Configuring a Virtual Private Network (VPN).
- f. Configuring a remote access policy Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP).
- g. Demonstrating knowledge protocols (e.g., Transmission Control Protocol and Internet Protocol (TCP/IP), Dynamic Host Configuration Protocol (DHCP) and directory services (e.g., Domain Name System (DNS) by setting up common protocols, e.g., Secure Shell (SSH), netstat, Simple Mail Transfer Protocol (SMTP), nslookup, Telnet, DNS/Bind, FTP, IIS/Web Pages, DHCP/DNS server).
- h. Locating open ports by completing a port scan.
- i. Demonstrating the knowledge and use of network statistics (netstat).