# Cybersecurity II Course No. 10900 Credit: 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Student name:**  |  | **Graduation Date:** |  |

Pathways and CIP Codes:Programming & Software Development (11.0201); Network Systems (11.0901); Information Support & Services (11.0301)

Course Description: **Application Level:** a course that 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. This should be a dual enrollment course with the student completing post-secondary credit hours in the Computer Support Specialist certification track (KBOR). Students should be completing preparatory competencies toward successful completion of the CompTIA Security+ exam and attainment of certification. **\*\*Prerequisite: Cybersecurity I or demonstration of all competencies therein.**

Directions:The following competencies are required for full approval of this course. Check the appropriate number to indicate the level of competency reached for learner evaluation.

**RATING SCALE:**

4. Exemplary Achievement: Student possesses outstanding knowledge, skills or professional attitude.

3. Proficient Achievement:Student demonstrates good knowledge, skills or professional attitude. Requires limited supervision.

2. Limited Achievement:Student demonstrates fragmented knowledge, skills or professional attitude. Requires close supervision.

1. Inadequate Achievement:Student lacks knowledge, skills or professional attitude.

0. No Instruction/Training:Student has not received instruction or training in this area.

## Benchmark 1: Working knowledge of the types of malware and methods of cyberattack.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 1.1 | Conduct research to determine various forms of malware and analyze methods to handle malware, such as how to control access to secured resources and computer resources. |  |
| 1.2 | Analyze and differentiate among various types of attacks on systems and networks. Different types of attacks can include but are not limited to: a. Virus; b. Worms, c. Trojans, d. Unpatched software, e. Password cracking, f. Advanced persistent threat, g. Reconnaissance/foot printing, 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, and r. Drive-by-attack. |  |

## Benchmark 2: Basic knowledge of cryptography and its role in cybersecurity.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 2.1 | Analyze cryptographic tools, procedures for use, and products including but not limited to: PKI, Certificates, PGP, and Certificate authorities. |  |

## Benchmark 3: Working knowledge of cybersecurity protocols and security awareness.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 3.1 | Analyze attack methods on wireless networks and demonstrate the use of wireless security protocols. Evaluate the capabilities of WPA, WPA-2, and WEP and the effectiveness of the security protocols and demonstrate how to use them appropriately. |  |
| 3.2 | Research and analyze security awareness in an organization. Demonstrate knowledge of the mitigation of the following, including but not limited to: 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, and h. Use of social networking. |  |
| 3.3 | Analyze and define the impact of security incidents on an organization. Define what a disaster recovery (DR) plan is and how to develop one. |  |
| 3.4 | Explore and identify various assessment methods including but not limited to network penetration and vulnerability testing. |  |
| 3.5 | Identify and explain the uses for security testing tools. Demonstrate and compare the effectiveness of Nessus and Nmap. |  |
| 3.6 | Demonstrate each of the following concepts: a. Evaluate the patch status of a machine, b. Demonstrate knowledge of packet-level analysis in order to install and view packets, and c. Perform secure data destruction (e.g., Secure Erase, BCWipe). |  |
| 3.7 | Utilizing prior fundamentals, demonstrate proper secure network configuration and administration. Use common tools and design a network utilizing secure protocols, and evaluate the network upon completion. The plan should address, but is not limited, to the following: 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. Identifying 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 of network 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), lookup, Telnet, DNS/Bind, FTP, IIS/Web Pages, DHCP/DNS server, h. Locating open ports by completing a port scan, and i. Demonstrating the knowledge and use of network statistics (netstat). |  |

## Benchmark 4: Working toward CompTIA Security+ certification.

### Competencies

| **#** | **DESCRIPTION** | **RATING** |
| --- | --- | --- |
| 4.1 | Assess the security posture of an enterprise environment and recommend and implement appropriate security solutions. |  |
| 4.2 | Monitor and secure hybrid environments, including cloud, mobile, and IoT. |  |
| 4.3 | Operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance. |  |
| 4.4 | Identify, analyze, and respond to security events and incidents |  |

I certify that the student has received training in the areas indicated.

Instructor Signature:

For more information, contact:

CTE Pathways Help Desk

(785) 296-4908

pathwayshelpdesk@ksde.org



900 S.W. Jackson Street, Suite 102

Topeka, Kansas 66612-1212

[https://www.ksde.org](https://www.ksde.org/)

The Kansas State Department of Education does not discriminate on the basis of race, color, national origin, sex, disability or age in its programs and activities and provides equal access to any group officially affiliated with the Boy Scouts of America and other designated youth groups. The following person has been designated to handle inquiries regarding the nondiscrimination policies: KSDE General Counsel, Office of General Counsel, KSDE, Landon State Office Building, 900 S.W. Jackson, Suite 102, Topeka, KS 66612, (785) 296-3201.