THE UNIVERSITY OF ARIZONA
Continuing and
Professional Education

Cyber Defense: Computer and Web Application Security Course

For most modules, you will need to pass a short quiz to demonstrate your understanding of the material before you can move on to the next module.

Labs are completed in a Cybersecurity Lab as a Service (CLaas) system, allowing students to safely simulate attacks and get hands-on experience with detection and mitigation tools, without compromising any real-world networks, computing systems, web applications or other technologies.

Information contained in the course may be subject to change, as deemed appropriate by the instructor.

Module 1: Overview of Computing Operating Systems

- Introduction to Operating Systems
- History and changes in operating systems
- Popular Operating Systems: Linux
- Popular Operating Systems: MacOS
- Popular Operating Systems: Windows
- Comparison between Linux, MacOS, and Windows
- Introduction to Unix/Linux Shell Commands
- Introduction to Windows Command Prompt Commands

Video lectures: 8 videos

Labs: none

Quizzes: 8 quizzes

Module 2: Computer Security

- Introduction to Computer Security
- Components of computer systems needing protection
- CIA: Confidentiality, Integrity & Availability
- Defense in Depth/Security through layers

Video lectures: 4 videos

Labs: This experiment will demonstrate the ways of attacking computers, guiding students to launch attacks that aim to compromise computers' Confidentiality, Integrity and Availability. In this lab, students will use three Virtual Machines to perform experiments. The first one acts as an attacker's computer, the second one as the target, and the last one acts as the user's personal computer.

Quizzes: 4 topic quizzes, 1 lab quiz

Module 3: Computer Attacks

- Malware attacks
- Phishing
- Viruses
- Buffer overflow attacks
- String formatting attacks
- Rootkits

Video lectures: 7 videos

Labs

- Ransomware: This experiment will demonstrate the effects of ransomware on target machines. In this lab, the students will target a user's machine, get access to it, and launch a ransomware on the target machine.
- Phishing: The goal of this experiment is to identify what phishing is and how it maliciously gathers personal information via deceptive emails.
- Viruses: During this experiment, you will simulate how computer viruses negatively affect computers – modifying system files and destroying the executable files at the local directory.
- Buffer overflow attacks: During this experiment, you will bypass a Bank's Authentication Program via its Buffer Overflow vulnerability to gain a customer's credit card information.
- Rootkits: During this experiment, you will demonstrate the effects of rootkits on target machines and gain a sense of how rootkits can be used by malicious attackers.

Quizzes: 6 topic quizzes, 5 lab quizzes

Module 4: Computer System Vulnerability Analysis

- Introduction to Computer Vulnerability Analysis
- Computer Vulnerability Analysis through Computer Vulnerability Analysis tools
- Introduction to OpenVas
- OpenVas usage
- Common Vulnerabilities and Exposures (CVE)

Video lectures: 5 videos

Labs: none

Quizzes: 5 quizzes

Module 5: Computer Intrusion Detection Tools

- Intrusion Detection Systems
- Host Intrusion Detection Systems
- Signature Based Intrusion Detection System: OSSEC
- Signature Based Intrusion Detection System: Tripwire

Video lectures: 4 videos

Labs: none

Quizzes: 4 quizzes

Module 6: Computer Security Policies

- Overview
- Security policies for Windows
- How security policies help secure attacks against Windows
- Security policies for Linux
- How security policies help secure attacks against Linux
- Security policies for Mac
- How security policies help secure attacks against Mac

Video lectures: 8 videos

Labs: none

Quizzes: 7 quizzes

Module 7: Secure Computing System Design and Configuration

- Computing system attack mitigation strategies
- Secure computing system designs and configurations
- System backup
- Disaster recovery planning
- Best Practices

Video lectures: 5 videos

Labs: None

Quizzes: 5 quizzes

Last updated: April 2021