THE UNIVERSITY OF ARIZONA
Continuing and Professional Education

Cyber Defense: Network Security Course

Each module includes an estimate of the amount of time it will take you to complete each group of activities: watching video lectures, completing quizzes and completing labs. Each activity may take you more or less time depending on your learning speed.

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: Network Design and Protocol

- Network Design
- IP addressing, segmentation and filtering
- Transport Layer Protocols
- ARP, ICMP, DNS and HTML Protocol
- Network address translation
- Setting up a local area network

Video lectures: 1 hour 30 minutes

Labs: 3 hours

Lab 1: The purpose of this lab is to familiarize the student with the basic operations of computer networks. In this lab you learn to set IP addresses (static IP and dynamic IP), subnet masks and gateways.

Lab 2: The purpose of this lab is to explain the benefits of using VLAN, how a VLAN is set up and how it works.

Quizzes: 1 hour

Total: 5 hours 30 minutes

Module 2: Introduction to Network Security

- Basics of cyber security
- Network attack classification
- Attacks on IP layer
- Attacks on transport layer
- Implementation of security through encryption
- Implementation of security through firewalls
- Virtual Private Networks (VPN)
- IP Security

Video lectures: 1 hour 20 minutes

Labs: 3 hours

Lab 3: The purpose of this lab is to help the student understanding network packets and protocols and to practice using Wireshark to capture and analyze network packets.

Lab 4: The purpose of this lab is to understand Denial of Service (DoS) and Distributed DoS (DDoS) attacks, focusing on exploiting vulnerabilities in different layers (network layer, application layer; and to further the student's understanding of the TCP/IP stack.

Lab 5: The purpose of this lab is to familiarize the student with the basics of port scanning. The student will perform port scanning attacks using NMAP. The students will also use NMAP to identify different services running on the target system.

Lab 6: The purpose of this lab is to familiarize the student with the basic operations of firewalls. The lab will teach students to configure and set up a firewall in a Linux environment. The lab will also teach students to allow certain traffic and block malicious traffic in a Linux environment.

Quizzes: 1 hour

Total: 5 hours 20 minutes

Module 3: VPN

- Overview of VPN
- How VPN works
- Implementations of VPN
- Advantages and Disadvantages of VPN
- Applications of VPN

Video lectures: 30 minutes

Labs: 2 hours 30 minutes

Lab 7: The purpose of this lab is to explain the functions, benefits and how to set up secure and encrypted connections by using VPN protocol (e.g., IPSEC).

Quizzes: 1 hour

Total: 4 hours

Module 4: Network Monitoring Tools

- Wireshark and Tshark
- Tcpdump
- IPTraf
- Arpwatch
- P0f

Video lectures: 21 minutes

Labs: 1 hour

Quizzes: 1 hour

Lab 8: The purpose of this lab is to familiarize the student with different tools that are used to monitor the network and to practice using the following tools: TCPdump, IPtraf, P0f.

Total: 2 hours 21 minutes

Module 5: Network Vulnerability

- Introduction to Network Vulnerability Analysis
- Network Vulnerability Analysis through Network Analysis Tools
- Introduction to OpenVas
- OpenVas Usage
- Common Vulnerabilities and Exposures (CVE)

Video lectures: 30 minutes

Labs: 4 hours 30 minutes

Lab 9: The purpose of this lab is to use OpenVas to scan a vulnerable Virtual Machine and to generate a vulnerability report.

Quizzes: 1 hour

Total: 6 hours

Module 6: Network Attacks

- Attacks on DNS Protocol
- ARP Cache Poisoning
- Attacks on Wi-Fi Protocol

Video lectures: 17 minutes

Labs: 3 hours

Lab 10: The purpose of this lab is to understand the insecurities of the Domain Name System (DNS) protocol and how they can be exploited.

Quizzes: 1 hour

Total: 4 hours 17 minutes

Module 7: Network Intrusion Detection Systems

- Intrusion Detection Systems
- Signature based Intrusion Detection Systems: Snort
- Signature based Intrusion Detection Systems: Suricata
- Anomaly Based Intrusion Detection System

Video lectures: 25 minutes

Labs: 3 hours

Lab 11: The purpose of this lab is to familiarize the student with the basic operations of Snort.

Quizzes: 1 hour

Total: 4 hours 25 minutes

Module 8: Unified Network Management and Security

- Mitigation techniques for DoS/DDoS attacks
- Network attack mitigation strategies
- Security network design
- Securing network using Avirtek Autonomic Cyber Security ACS

Video lectures: 24 mins

Labs: none

Quizzes: 1 hour

Total: 1 hour 24 minutes