ITIS 120: CYBERSECURITY: ETHICAL HACKING

Citrus College Course Outline of Record

Heading	Value
Effective Term:	Fall 2021
Credits:	3
Total Contact Hours:	90
Lecture Hours :	36
Lab Hours:	54
Hours Arranged:	0
Outside of Class Hours:	72
Strongly Recommended:	ITIS 107 and ITIS 109.
Transferable to CSU:	Yes
Transferable to UC:	No
Grading Method:	Standard Letter, Pass/No Pass

Catalog Course Description

This course provides an overview of information systems security, specifically system penetration. Students will be introduced to the concepts, principles, and techniques for attacking and disabling a network within the context of properly securing it. General concepts covered include aspects of computer and cyber crime, cyber crime investigation, security policies, sample attacks, and testing. Students will receive hands-on training using various tools for penetration testing. 36 lecture hours, 54 lab hours.

Course Objectives

- Identify and categorize the types of cyber threats, attacks, and intrusions currently in use by completing case studies, scenarios, and completing group projects.
- Demonstrate basic computer forensics and know what to do if attacked through real-word simulations.
- Identify basic concepts and issues in cyber security by completing individual and group projects, quizzes and exams.
- Identify the basic concepts of cyber terrorism and cyber warfare by completing case studies, scenarios, and completing group projects.
- Identify and recognize the importance of security policies by completing individual group projects, quizzes, and exams.

Major Course Content

1. Introduction to Information Security
    a. Basic Security Terminology
    b. Online Security Resources
2. Identifying and Categorizing Threats
    a. DoS, Malware
    b. Session Hijacking
    c. Malicious Code and Activity
3. Industrial Espionage in Cyber Space
4. Cyber Terrorism
    a. Information Warfare
    b. Economic Attacks
5. Computer Security Technology
    a. Firewalls
    b. Wi-Fi Security
    c. Virus Scanners
    d. IDS
6. Securing Information Systems
    a. Ethics and Legality
    b. Auditing and Testing
    c. Digital Signatures
    d. Networks and Telecommunications
    e. Computer Forensics
7. Information Security Standards
    a. Training and Professional Certifications
    b. U.S. Compliance Laws

Lab Content

1. Footprinting and Scanning
    a. Identifying Active Machines
    b. Finding Open Ports and Access Points
    c. OS Fingerprinting
2. Trojans and Backdoors
    a. Trojan Types and Tools
    b. Effects of Trojans
    c. Backdoor Countermeasures
3. Web Security
    a. Web Tracking
    b. Web Server Hacking
    c. Web Application Hacking
    d. Cross-site Scripting Attacks
4. Network Security
    a. TCP/IP Attack
    b. Local DNS Attack
    c. Session Hacking
    d. Sniffers
5. Intrusion Detection Systems
6. Firewalls
7. Cryptographic Attacks and Defenses
8. Digital Forensics
    a. Recovering a Deleted File

Suggested Reading Other Than Required Textbook

Online articles focusing on cyber security from NSA (National Security Agency), DHS (Department of Homeland Security), and NICE (National Initiative for Cyber Security Education).

Examples of Required Writing Assignments

Locate an online article on a cyber security event (cyber terrorism, virus intrusion, cyber stalking, etc.) via a qualified news reporting agency (i.e., CNN, MSN News, BBC News, etc.). Write a synopsis (2-5 pages) describing the event and what detrimental effects it has caused or will cause. In your own words, explain how this event could have been

prevented and what steps should now be taken to stop it from happening again.

Examples of Outside Assignments

Apply data processing techniques on data collected by the U.S. Defense Advanced Research Project Agency (DARPA) in order to train and test an IDS (Information Detection System).

Instruction Type(s)

Lecture, Lab, Online Education Lecture, Online Education Lab