

COURSE OUTLINE

CMSY-164

Introduction to Intrusion Detection Systems

3 Semester Hours

HOWARD COMMUNITY COLLEGE

Description

From this introduction to intrusion detection systems, students will develop a solid foundation for understanding IDS and how they function. Students will have hands-on experience with implementing and configuring IDS in a network infrastructure. This course is designed with a computer administrator operator in mind; a computer professional with an MCSE or equivalent would have adequate background. Prerequisites: Completion of CMSY-162 or CMSY-163 or possess a fairly extensive background in computer administration. (3 hours lecture, 1 hour lab)

Overall Course Objectives

Upon completion of this course, the student will be able to:

1. Define what an IDS is and how it functions.
2. Determine where IDS should be placed in a network.
3. Employ a packet sniffer and identify the critical parts of a TCP/IP packet.
4. Identify attack signatures and relate them to specific attacks.
5. Identify false-positives and false-negatives, and have the ability to determine what causes them.
6. Define and identify the different types of IDS including:
 - a. Host based IDS
 - b. Network based IDS
 - c. Hybrid IDS.
7. Build and implement an open-source IDS system.

Major Topics

- I. IDS systems
 - A. Define host based IDS
 - B. Define network based IDS
 - C. Introduce different IDS systems and how they function
 - D. Introduce the version of software we will be using during the course
 - E. Compare host based vs. network based IDS and when to deploy them
 - F. Define hybrid systems
- II. TCP/IP
 - A. Introduce packet sniffing
 - B. Define a TCP/IP packet, and isolate the critical parts of a packet
 - C. Show how IDS systems function similar to a packet sniffer
- III. Security technology
 - A. Show where different technologies fit within a secure network
 - B. Determine where an IDS system should be within the structure
- IV. Attacks
 - A. Define the type of attacks that may occur on critical systems
 - B. Show how attacks may breach other network security devices
- V. Attack signatures
 - A. Introduce attack signatures, and how they are structured to determine an attack
 - B. Compare an attack signature to packets captured via a sniffer
 - C. Define and write custom attack signatures to capture specific traffic

- VI. False Positives/False Negatives
 - A. Define the terms for IDS understanding
 - B. Show how to limit the level of false positives and negatives
 - C. Learn how to determine if a packet indicates a false positive, or a true attack
- VII. Alerting and Attack Response
 - A. Learn how an IDS alerts when attacked
 - B. Determine how to structure alerts so that an admin is not overwhelmed
 - C. Discuss the differences between alerting and logging
 - D. Show incident procedures, and what should be done when an attack is occurring or has occurred.
- VIII. Passive IDS/Active IDS
 - A. Compare a IDS system that interacts with security policy, and one that does not
 - B. Show why it is often recommended that IDS work as a passive device
 - C. Show upcoming technology that will allow for more active devices
- IX. IDS Implementation
 - A. Install and configure an IDS system
 - B. Learn to manage the system
 - C. Simulate attacks on the system, and respond accordingly
 - D. Adjust the system for functionality on different parts of the network
 - E. Evaluate the data to determine correct actions

Course Requirements

Grading/exams/projects: This course is more advanced than the introductory course. It will have much more extensive hands-on labs and configuration of network systems. During the course, the students will be exposed to IDS and be expected to be able to set it up properly. Grading will be based upon a combination of exams and labs. The labs will be hands-on system configuration with the students having to properly configure and implement working IDS.

Other Course Information

Mapping of CISSP Domains:

- Access Control Systems and Methodology
 - Access Control Techniques
 - Access Control Administration
 - Access Control Models
- Applications and Systems Development
 - Malicious Code
- Physical Security
 - Threats, Vulnerabilities, and Countermeasures related to physically protecting the enterprise's sensitive information assets
 - The risk to people, facilities, data, media, equipment, support systems, and supplies as the risk applies to Computer Physical Security
- Security Architecture and Models
 - Network Protocol Stack Functions
 - Common flaws and security issues associated with system architectures and designs
- Telecommunications, Network and Internet Security
 - International Standards Organization/Open Systems Interconnection (ISO/OSI) Layers and Characteristics
 - Communications and Network Security
 - Internet/Intranet/Extranet
 - Security boundaries and how to translate security policy to controls
 - Network Attacks and Countermeasures