IT-2730: INTRUSION DETECTION/PREVENTION SYSTEMS FUNDAMENTALS

Cuyahoga Community College

Viewing: IT-2730 : Intrusion Detection/Prevention Systems Fundamentals

Board of Trustees:

January 2021

Academic Term:

Fall 2021

Subject Code

IT - Information Technology

Course Number:

2730

Title:

Intrusion Detection/Prevention Systems Fundamentals

Catalog Description:

Covers the design, implementation, and administration of Intrusion Detection/Prevention Systems. Includes practical, hands-on experience working with these systems and analysis various attack signatures and the network traffic these systems collect.

Credit Hour(s):

3

Lecture Hour(s):

2

Lab Hour(s):

2

Requisites

Prerequisite and Corequisite

EET-2303 Cisco II and ITNT-2370 Network Security Fundamentals.

Outcomes

Course Outcome(s):

Implement and administer Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS) and the network traffic these systems collect.

Objective(s):

1. Differentiate between host-based and network-based Intrusion Detection Systems/Intrusion Prevention Systems.
2. Setup and administer an IDS in a working network.
3. Identify false positives and false negatives.
4. Demonstrate appropriate and ethical behavior and good work habits.

Course Outcome(s):

Analyze various attack signatures used to compromise computer systems.

Objective(s):

1. Setup and administer an IDS in a working network.
2. Dissect and analyze various types of normal and unusual traffic.
3. Identify false positives and false negatives.

Methods of Evaluation:

Evaluation can include any combination of the following:

1. Assignments
2. Quizzes
3. Exams
4. Lab Assignments
5. Projects
6. Reports
7. Oral Evaluations

Course Content Outline:

1. Introduction to Network Security Monitoring
   a. Understanding the concept of Defense-in-Depth
   b. Introduction to intrusion detection and prevention
2. Network and Host-Based Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS)
   a. Description of host-based IDS/IPS systems
   b. Description of network-based IDS/IPS systems
3. Fundamentals of Traffic Analysis
   a. The TCP/IP suite
   b. Dissecting a network packet
4. Advanced Traffic Analysis
   a. Packet sniffing
   b. Tcpdump basics
   c. Examining tcpdump output
5. Working with Filters/Rules for Network Monitoring
   a. Downloading and/or creating network monitoring filters/rules
   b. Managing network monitoring filters/rules
   c. Filter/rule execution
   d. Analyzing and Deconstructing Attack Signatures

Resources

Weaver, R. & Farwood, D. (2014) *Guide to Network Defense and Countermeasures.*, Boston: Cengage.

Pathan, A. (2016) *The State of the Art in Intrusion Prevention and Detection*, Boca Raton: CRC Press.

Mohammed, M. & Rehman, H. (2015) *Honeypots and Routers: Collecting Internet Attacks*, Boca Raton: CRC Press.

Stallings, W. & Brown L. (2018) *Computer Security: Principles and Practice*, New York: Pearson.

Sanders, C. *Intrusion Detection Honeypots: Detection Through Deception*. Oakwood, GA: Chris Sanders, 2020.

Top of page

Key: 2516