BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS4110 Network Defense
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Demonstrate the skills, knowledge related to network monitoring, traffic visualization tools, and techniques.
    a. Describe the fundamental concepts, technologies tools and issues related to network monitoring and defensive techniques.
    b. Identify a security compromise event in a Windows or Linux server.
2. Design a defensive network strategy and policy that will provide an acceptable level of competency that specific types of attacks can be both detected and mitigated.
    a. Determine and report on where to deploy security sensors in an enterprise network based on traffic analysis.
    b. Identify and demonstrate how to detect an attack against a network device.
3. Demonstrate competency in configuration and deployment of a selected IDS system.
    a. Use an open source intrusion detection system to monitor, detect, mitigate and report on an instructor-invoked security compromises (e.g., Snort, Security Onion tools).
    b. Map a network using Nmap and other commonly used tools.
4. Identify how to perform a threat hunting operation of an enterprise network.
    a. Identify and describe how to use common tools for threat hunting.
    b. Identify and describe how to correlate an IDS detection with server event logs.

Big Ideas and Essential Questions

Big Ideas

-

Essential Questions

1.

CAE-CD Technical Core: Network Defense

These SLOs are approved for experiential credit.

Effective: Fall 2020