BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS 4410 Network Defense and Intrusion
3 Semester Credit Hours

Student Learning Outcomes and Enabling Objectives

1. Demonstrate proficiency performing penetration testing and threat hunting.
    a. Perform threat analysis.
    b. Conduct internal and external penetration testing.
    c. Detect threats using analytics and intelligence.

2. Apply risk mitigation strategies to monitor and protect systems while learning the importance of frameworks, policies, procedures, and controls.
    a. Describe the risk identification process used to support risk calculation, communication, and training.
    b. Explore approaches to monitor software and systems.
    c. Implement physical security controls to protect systems.
    d. Explore incident response planning procedures for various situations.

3. Perform reconnaissance countermeasures to monitor software and systems.
    a. Review web application security.
    b. Implement system hardening while disabling unnecessary services.
    c. Conduct system scanning to mitigate potential threats.
    d. Determine the types of vulnerabilities associated with different attack vectors.

4. Implement Identify and Access Management (IAM).
    a. Administer user accounts.
    b. Configure account policies and account control.
    c. Manage user-based and role-based access.

5. Demonstrate proficiency using an Intrusion Detection System (IDS).
    a. Detect threats using analytics and intelligence.
    b. Implement security controls using firewalls.
    c. Manage devices through Network Access Control (NAC).
    d. Implement defensive deceptive methods.

Big Ideas and Essential Questions

Big Ideas

- Penetration testing and threat hunting.
- Information Technology risk mitigation strategies.
- System hardening.
- Identity and access management.
- Data analysis to support threat identification.
- Incident response planning procedures.

Essential Questions

1. What are the most significant cybersecurity threats that industry and government face?
2. Why do Information Technology (IT) professionals need to worry about information security?
3. What strategies, tools, and procedures can be implemented to perform effective threat analysis?
4. Why is "data fluency" important in performing threat analysis?
5. Why is incident response critical following a security breach?

These SLOs are not approved for experiential credit.

Effective: Fall 2022