BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS3250A Hardening Systems
3 Semester Hours

Student Learning Outcomes and Enabling Objectives

1. Apply hardening techniques with computer accounts, files, and shares
    a. Distinguish between user and administrative accounts
    b. Associate permissions to workstation files
    c. Associate permissions to workstation shares
2. Apply hardening techniques to workstation computers to protect from threats
    a. Modify firewall rules on workstation computers
    b. Explore antivirus protection to workstation computers
    c. Explore updates to a workstation computer
3. Employ preventative hardening techniques
    a. Explore disk encryption on a workstation computer
    b. Discuss network encryption that secures communication
    c. Apply user access control to limit changes to a workstation computer
    d. Associate permissions and restrictions on applications
    e. Explore local policy operations to improve security profile
4. Employ investigative tools and techniques to isolate security issues
    a. Explore computer events using Event Viewer
    b. Apply auditing controls on computing resources
    c. Explore auditing events on computing resources
5. Build a standard operating procedure (SOP)
    a. Discuss the necessity for documenting procedures
    b. Create a procedure guide for computer security
    c. Examine Defense Information Systems Agency Security Technical Implementation Guides
    d. Explore SOP implementation

Big Ideas and Essential Questions

Big Ideas

- Implement workstation hardening techniques using tools available on personal computers
- Recognize that existing workstation hardening techniques apply across enterprise computing systems

Essential Questions

1. How is a workstation protected from internal and external threats?
2. How is a workstation postured to reduce the potential for damage if compromised?

These SLOs are approved for experiential credit.

Effective: Fall 2022