BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS4310 Network Offense
3 Semester Hours

Student Learning Outcomes & Enabling Objectives

1. Demonstrate the skills and knowledge related to the profession of offensive security in a networked and local environment.
    a. Describe and demonstrate the steps required to enumerate a target system of unknown parameters.
    b. Describe the various tools used to perform an enumeration of a target system with minimal or no detection by intrusion detection systems.

2. Demonstrate how to acquire administrator level privileges on a local target server from a remote connection.
    a. Acquire and enumerate account names from a remote system
    b. Recover a basic password using basic penetration testing and vulnerability assessment tools as provided in the Kali or Parrot suite

3. Demonstrate how to deliver a compromising payload to a target system.
    a. Demonstrate and document the steps necessary to perform a XSS attack against a predetermined server
    b. Demonstrate and document the steps necessary to gain access to a local system using a selected tool from either Kali or Parrot tool suite.

4. Demonstrate results from a vulnerability assessment or penetration test event.
    a. Complete a vulnerability assessment checklist and record identified areas of vulnerability in a target system or network.
    b. Document open ports and services from a vulnerability assessment.

CAE-CD Foundational Knowledge Units: Cybersecurity Principles (CSP)
These SLOs are approved for experiential credit.

Effective: Spring 2021