BAKER COLLEGE
STUDENT LEARNING OUTCOMES

ITS3510 Ethical Hacking I
3 Semester Hours

Student Learning Outcomes & Enabling Objectives

1. Explain the history and current state of hacking and penetration testing, including ethical and legal implications.
2. Identify fundamental TCP/IP concepts and technologies related to networking.
3. Identify and remove common types of malware, spyware, adware, etc.) from infected systems.
4. Identify common information gathering tools and techniques.
5. Analyze how port scanning and fingerprinting are used by hackers.
6. Analyze how enumeration is used in conjunction with system hacking on Windows and Linux systems
7. Examine computer languages and programming
8. Discuss vulnerabilities for windows and Linux, how to fix them and techniques to harden.
9. Explore the vulnerabilities of Embedded OSs
10. Understand web applications, their vulnerabilities and tools for attackers and security testers.
11. Analyze wireless network vulnerabilities exploited by hackers.
12. Describe cryptographic systems and methods.
13. Compare and contrast defensive technologies

Big Ideas and Essential Questions

Big Ideas

- Information Technology
- Information Technology Security

Essential Questions

1. How do we protect wired networks
2. How do we protect wireless networks
3. How do maximize the effectiveness are firewalls?
4. How does the threat level of an organization impact the IS department within a business?
5. What role does network protection strategy play in information systems?

Effective: Fall 2020

These SLOs are not approved for experiential credit.