Spokane Falls Community College

COURSE LEARNING OUTCOMES AND OUTLINE

Prefix and Course Number CYBR 320
Course Title Ethical Hacking

Last Modified: Fall 2017

Course Learning Outcomes

By the end of this course, a student should be able to:

- Outline ethical considerations of hacking
- Outline legal considerations of hacking
- Assess an environment using footprinting
- Collect information using network scanning
- Identify methods to gain access to systems
- Analyze social engineering methods
- Explain common physical security weaknesses

Course Outline

1. Legal Issues
   1.1 Fourth Amendment
   1.2 Computer Fraud and Abuse Act
   1.3 Electronic Communications Privacy Act
   1.4 Federal Wire Tap
2. Ethical Considerations
   2.1 Consent
      2.1.1 Exceeding scope and authority
   2.2 Hack back
   2.3 Snooping
   2.4 Disruption of service
   2.5 Intent versus authorization
3. Historical review of hacking
4. Footprinting and Reconnaissance
   4.1 Open gathering
   4.2 Passive gathering
   4.3 Internet gathering
   4.4 Social Engineering
5. Scanning
   5.1 Types of scans
   5.2 OS Fingerprinting
   5.3 Proxies
   5.4 Network Diagramming
6. Enumeration
   6.1 Windows user and system gathering
   6.2 Unix and Linux system gathering
7. System compromise
   7.1 Hacking

- 7.2 Authentication
- 7.3 Covering your tracks
- 7.4 Malicious software and covert connections

8. Network traffic sniffing
   - 8.1 Current tools
   - 8.2 Switched network attacks
9. Social Engineering
   - 9.1 Phases of an attack
   - 9.2 Common targets
   - 9.3 Common sources of information
10. Web Servers and applications
    - 10.1 Common attacks and flaws
    - 10.2 Current tools
11. Physical Security
    - 11.1 Simple controls
    - 11.2 Mobile access and concerns