NorthWest Arkansas Community College
Business and Computer Information Course Outline

NTWK 2113 NETWORK SECURITY (S –Odd Years)

Catalog Description

This course is designed to provide instruction in security for network hardware, software, and data. Topics include: authentication, remote access, attacks and malicious code, security principles and procedures, firewalls, encryption, intrusion detection, and disaster planning and recovery. Outside lab time will be required.

Prerequisites

NTWK 2013 Networking and Information Systems
NTWK 2023 Network Administration I or Consent of instructor

Credit Hours: 3

Target Audience

- This course is a preferred course option of the Computer Networking A.A.S. Degree option
- Students preparing for a career in a CIS field which requires general Network Security knowledge
- Students who wish to enhance their understanding of Computer Networking
- Community members or professionals who wish to expand their understanding of Computer Network Security

General Course Objectives

- To offer curriculum and instructional methods that support student learning.
- To develop in each learner the skills and attitudes necessary for the attainment of academic and career goals.
- To develop in each learner the enjoyment of learning and the lifelong pursuit of knowledge.

Core Course Objectives

- The main goal of this course is to provide student with a fundamental understanding of Network Security principles and implementation. Students will learn about the technologies used and principles involved in creating a secure computer networking environment. Additional topics include authentication, the types of attacks and malicious code that may be used against your network, the threats and countermeasures for e-mail, Web applications, file and print services, and remote access.
- A variety of security topologies are discussed as well as technologies and concepts used for providing secure communications channels, secure internetworking devices, and network medium. Further, you will learn about intrusion detection systems, firewalls, physical security concepts, security policies, disaster recovery, and computer forensics.
- Aside from learning the technologies involved in security, understanding will be gained in daily tasks involved with managing and troubleshooting those technologies. Students will have a variety of hands-on and case project assignments that reinforce the concepts presented in class.

Required/Optional Texts and Student Resources

Required:

Security+ Guide to Network Security Fundamentals, 2nd edition,
Publisher: Course Technology: 2005. ISBN 0-619-21566-6.
Lab Manual for Security+ Guide to Network Security Fundamentals, 2nd edition,
Publisher: Course Technology Incorporated: 2005. ISBN 0-619-21536-4.

Optional:

Web-based resources as may be provided by the instructor during the course of the semester.

Required Forms of Assessment

- 20% of the grade is based on three examinations. The exams may be given in a multiple choice and short essay format. An in-class review will be held prior to each examination.
- 40% of the grade is based on completing the end of chapter case project assignments. An electronic version of the case project assignments can be downloaded from the course's Web site.
- 10% of the grade is based on quizzes. Quizzes are announced one day in advance and may vary from 3 to 5 questions that may be in any format.
- 30% of the grade is based on keeping a project notebook. Students are asked to obtain a small notebook or to use a lab notebook and keep notes on the results of the hands-on projects from the Lab manual. The notes should include comments that you can use once the class is over to help describe results of the hands-on-projects. Include any helpful tips or advice that you might use in the future.

Required Topics Covered

- ***Security Overview*** *(costs of intrusion, goals of network security, creating a secure network strategy)*
- **Authentication** (usernames and passwords, Kerberos, challenge handshake authentication, mutual authentication, digital certificates, security tokens, biometrics, multi-factor authentication)
- **Attacks and Malicious Code** (IP fragmentation attacks, DOS and DDOS attacks, spoofing, man in the middle, replays, TCP session hijacking, social engineering, attacks against encrypted data, software exploitation)
- **Remote Access** (IEEE 802.1X, VPN, Remote Authentication Dial-in User Service, Terminal access controller ACS, Point-to-Point tunneling protocol, layer two tunneling protocol, secure shell, IP security protocol, Telecommuting vulnerabilities)
- **E-mail** (secure E-mail encryption, how secure e-mail works, e-mail vulnerabilities, Spam, Hoaxes and chain letters)
- **Web Security** (SSL and TLS, HTTPS, Vulnerabilities of Web Tools, 8.3 file naming conventions)
- **Directory and File Transfer Services** (directory services, file transfer services, secure file transfer, file sharing)
- **Wireless and Instant Messaging** (the Alphabet Soup of 802.11, WAP 1.x and WAP 2.0, Wired equivalent privacy, conducting a wireless site survey, instant messaging)
- **Devices** (firewalls, routers, switches, wireless, modems, remote access services, telecom/private branch exchange, virtual private networks, intrusion detection systems, network monitoring and diagnostics, workstations and servers, mobile devices)
- **Media and Medium** (transmission media, securing transmission media, storage media, catastrophic loss, encryption, storing and destruction of media)
- **Network security topologies** (perimeter security topologies, DMZ, network address translation, tunneling, Virtual local area networks)
- **Intrusion Detection** (the value of intrusion detection, network-based and Host-based IDS, active detection and passive detection, incident response)
- **Security Baselines** (OS/NOS hardening, file system, network hardening, enabling and disabling of services and protocols, application hardening)

- **Cryptography** (algorithms, symmetric vs. asymmetric algorithms, concepts of using cryptography, certificates, key and certificate life cycle management)
- **Physical Security** (physical controls, technical controls)
- **Disaster Recovery and Business Continuity** (business continuity, disaster recovery planning process, policies and procedures, privilege management)

Optional Coverage

- **Computer Forensics and Advanced Topics** (computer forensics, risk management, education and training, auditing, documentation)