

Computer Information Department Course Outline

NTWK 2113 NETWORK SECURITY (On Demand)

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 2014 Networking and Information Systems
or Consent of instructor

Credit Hours/Contact Hours/Load Hours

3/3/3

Target Audience /Transferability

The target audience includes, but is not necessarily limited to, the following:

- Students preparing for a career in a CIS field which requires general Network Security knowledge
- Students who wish to enhance their understanding of Computer Network Security
- Community members or professionals who wish to expand their understanding of Computer Network Security

Student Learning Outcomes

Students completing this course will:

- Demonstrate a fundamental understanding of Network Security principles and implementation
- Demonstrate understanding of the technologies used and principles involved in creating a secure computer networking environment
- Demonstrate understanding of the technologies involved in security and will understand the daily tasks involved with managing and troubleshooting those technologies
- Learn to identify, detect and prevent network intrusions
- Identify security concerns and solutions
- Identify the costs of intrusion, and how they could affect the economic status of a business or even the nation
- Identify business and government security requirements in a 'wired' world
- Demonstrate an understanding of the interaction between security and system usability
- Use scanning and discovery techniques to identify vulnerabilities
- Use appropriate tools to remove malicious code
- Implement security at the following levels
 - TCP/IP
 - Firewalls
 - Operating systems
 - Network

- Audit security
- Cryptographic techniques
- Attacks and penetration

Topics

- **Security Overview** (*costs of intrusion, goals of network security, creating a secure network strategy, defense in depth, layering, usability, minimizing exposure*)
- **Authentication** (usernames and passwords, Kerberos, challenge handshake authentication, mutual authentication, digital certificates, security tokens, biometrics, multi-factor authentication)
- **Access Control** (least privilege, information classification)
- **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** (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, honeypots and honeynets)
- **Intrusion Detection** (the value of intrusion detection, network-based and Host-based IDS, active detection and passive detection, incident response, network monitoring and traffic analysis)
- **Security Baselines** (OS/NOS hardening, file system, network hardening, enabling and disabling of services and protocols, application hardening)
- **Cryptography** (algorithms, symmetric vs. asymmetric algorithms, encapsulation, concepts of using cryptography, certificates, key and certificate life cycle management)
- **Physical Security** (physical controls, technical controls, fail safe/fail secure)

Forms of Assessment

Lecture, lab assignments, homework assignments, online content in Blackboard, discussions, hands-on activities, projects, quizzes, final exam. Students will demonstrate proficiency by scoring 70% or above on all homework, quizzes, tests and lab assignments.