Montgomery College
Germantown Campus
NW246: Network Defense and Countermeasures
Master Course Syllabus

Course Description:

The purpose of this course is to prepare students for Level One of the Security Certified Program (SCP). The text maps clearly to the exam objectives for the current Security Certified Network Professional (SCNP) exam. Designed to help students develop beyond the Security+ certification, this course provides a solid foundation in network security fundamentals, but assumes familiarity with basic concepts. The course focuses on how to protect a range of different operating systems against attacks, how to develop more effective security strategies, and how to handle emergencies.

Course Learning Objectives

Upon successful completion of this course, the student will be able to:

1. Performing Risk Analysis
    a. Explain the fundamental concepts of risk analysis
    b. Describe different approaches to risk analysis
    c. Explain the process of risk analysis
    d. Describe techniques to minimize risk
2. Creating Security Policies
    a. Explain important concepts in security policies
    b. Identify security policy categories
    c. Define incident-handling procedures
3. Penetration Testing Techniques
    a. Describe the process of network reconnaissance
    b. Describe common network attack techniques
    c. Explain types of malicious code attacks
4. Analyzing Packet Structures
    a. Explain the Common Vulnerabilities and Exposures (CVE) standard
    b. Describe how signature analysis is used in examining network traffic
    c. Detect normal and suspicious traffic signatures
    d. Describe packet capture and analysis
    e. Explain ways to identify suspicious events
5. Cryptography
    a. Describe key events in cryptography history
    b. Explain components of cryptographic protocols
    c. Explain common cryptography standards
    d. Describe modern cryptanalysis methods
6. Internet and Web Security
    a. Describe weak points in the structure of the Internet
    b. Explain attack techniques against Web sites and Web users
    c. Explain methods for hardening Web and Internet resources
7. Hardening Linux Systems
    a. Explain how to navigate the Linux file system
    b. Describe methods of secure system management

    c. Describe ways to manage security for user accounts, directories, and files
    d. Install and secure network services, such as Kerberos, Network File System, Network Information System, and Samba
    e. Describe methods of managing security for services, processes, and system integrity
8. Windows Server 2003 Security Fundamentals
    a. Describe the Windows Server 2003 infrastructure
    b. Explain Windows Server 2003 authentication methods
    c. Describe auditing and logging in Windows Server 2003
9. Configuring Windows Server 2003 Security
    a. Describe how to configure Windows Server 2003 resource security
    b. Explain how to use Windows Server 2003 security configuration tools
    c. Describe how to configure Windows Server 2003 network security for remote access and virtual private network services

Range of Subject Matter – Model Course Outline:

1. Performing Risk Analysis
    a. Concepts
        i. Risk Analysis Factors
    b. Methods
        i. Survivable Network Analysis
        ii. Threat and Risk Assessment
    c. Process
        i. General Activities to Follow
        ii. Analyzing Economic Impacts
    d. Attacks
    e. Techniques for Minimizing Risk
        i. Securing Hardware
        ii. Rankin Resources to be Protected
        iii. Using Encryption
        iv. Securing Information
        v. Conducting Routine Risk Analysis

2. Creating Security Policies
    a. General Security Policy Best Practices
    b. Security Policy Development
        i. Steps to Creating a Security Policy
        ii. Identifying Security Policy Categories (Email, fax, biometrics, passwords, internet, wireless, etc.)
    b. Handling Security Incidents
        i. Assembling a Response Team
        ii. Specifying Escalation procedures
        iii. Responding to Security Incidents
        iv. Including Worst-Case Scenarios
        v. Updating the Security Policy
    c. Configuration / Change Management

3. Penetration Testing Techniques
    a. Network Reconnaissance
        i. Footprinting
        ii. Scanning
        iii. Enumeration
        iv. Social-Engineering Techniques
    b. Network Attack Techniques
        i. Privilege Escalation and Unauthorized Access
        ii. Buffer Overflow Attacks
        iii. Keystroke Logging
        iv. Denial-of-service Attacks
        v. Password Exploitation
    c. Malicious Code Attacks
        i. Viruses
        ii. Worms
        iii. Trojans
        iv. Spyware
        v. Macros
        vi. Reducing Malware Risks
    d. Software and Tools
    e. Countermeasures
        i. LAN Security
        ii. Wireless Security
        iii. Hardening of Systems

4. Analyzing Packet Structures
    a. Common Vulnerabilities and Exposures (CVE) Standard
        i. How it Works
        ii. Scanning CVE Vunerability Descriptions
    b. Signature analysis
        i. Bad Header Information
        ii. Suspicious Data Payload
        iii. Single-Packet Attacks
        iv. Multiple-Packet Attacks
        v. Components of a Packet Capture
    c. Detecting Network Traffic Signatures
        i. Normal traffic signatures
        ii. Abnormal traffic signatures
        iii. Nmap Scans
    d. Understanding Packet-Capturing Techniques
        i. Tools
        ii. Analyzing Captured Packets
    e. Identifying Suspicious Events
        i. Packet Header Discrepancies
        ii. Advanced Attacks
        iii. Remote Procedure Call (RPC) Attacks

5. Cryptography
    a. History of Cryptography Techniques

b. Components of Cryptographic Protocols
    i. Cryptographic Primitives
    ii. Types of Encryption Algorighms
    iii. Hashing Algorithms
    iv. Digital Signatures
    v. Key Management
b. Cryptographic Standards
    i. Data Encryption Standard (DES)
    ii. Triple DES
    iii. Advanced Encryption Standard (AES)
    iv. International Data Encryption Algorithm
    v. Wireless network Cryptography
    vi. Internet Protocol Security (IPSec)
    vii. Internet and Web Standards (SSL, TLS)
c. Modern Cryptanalysis Methods
    i. Side Channel Attacks
    ii. Passive Attacks
    iii. Chosen Ciphertext and Chose Plaintext Attacks
    iv. XSL Attacks
    v. Random Number Generator Attacks
    vi. Related Key Attacks
    vii. Integral Cryptanalysis
    viii. Differential Cryptanalysis

6. Internet and Web Security
    a. Internet Structure
        i. Understanding the Structure of the Internet
        ii. Understanding Weak Points in the Internet's Structure
    b. Web Attack Techniques
        i. Attack Techniques Against Web Servers
        ii. Attack Techniques Against Web Users
    c. Hardening Web and Internet Resources
        i. Hardening DNS Servers
        ii. Hardening Web Servers

7. Hardening Linux Systems
    a. Linux File System and Navigation
        i. File System Basics
        ii. Linux Command Line
        iii. Commands for Directory and File Navigation
    b. Security System Management
        i. Using Secure Shell instead of Telnet
        ii. Ensuring Root Security
        iii. Integrity Checking and Removing Unnecessary Packages
        iv. Maintaining System Patching
        v. Configuring System Accounting
        vi. Configuring Auditing and Logging
        vii. Using Antivirus Solutions
    c. User and File System Security

i. Configuring User Accounts and Groups
ii. Monitoring User Account Activity
iii. Managing Password Security and Password Restrictions
iv. Using the Shadow File
v. Configuring File and Directory Permissions
vi. Configuring File and Directory Ownership

d. Network Configuring Security
i. Enabling Kerberos Authentication
ii. Using Network File System
iii. Using Network Information System
iv. Using Samba

e. Securing Linux
i. Closing Network Ports by Configuring a Firewall
ii. Removing Unused Services
iii. Stopping Rogue Processes
iv. Other Linux Security Tools

8. Windows Server 2003 Security Fundamentals
a. Windows Server 2003 Infrastructure
i. Active Directory Deployment
ii. Managing Groups

b. Understanding Windows Server 2003 Authentication
i. User Authentication
ii. Client Authentication
iii. Session Authentication
iv. Authentication Methods
v. Remote User Authentication

c. Windows Server 2003 Auditing and Logging
i. Determining What to Audit
ii. Managing Event Logs

9. Configuring Windows Server 2003 Security
a. Windows Server 2003 Configuration
i. The importance of Backups (System and Data)
ii. FAT and NTFS
iii. Folder and File Attributes in FAT and NTFS
iv. Setting File and Folder Permissions
v. Security
vi. Folders, File Auditing, and Sharing Folders Configuration
vii. Printer Security Configuration
viii. Registry Security Configuration

b. Windows Server 2003 Configuration Tools
i. Account Security Configuration
ii. Security Configuration and Analysis Tools

c. Windows Server 2003 Network Security
i. Securing Routing and Remote Access Services and VPNs
ii. NAT Configuration

10. Network Defense Fundamentals

a. Describe network defense / perimeter security approach
b. Overview of network protocols
c. Identify defensive technologies
    i. Firewalls
    ii. VPNs
    iii. Proxy servers
    iv. Bastion hosts
    v. Honeypots
    vi. IDSs/IPSs
    vii. Antivirus
d. Identify the impact of defense
e. Identify network security contermeasures

Instructional Materials:

Required Textbook: Randy Weaver, Guide to Strategic Infrastructure Security. Course Technology Incorporated, 2008, ISBN: 1-4188-3661-3. ISBN-13: 978-1-4188-3661-0.

Evaluation:

Research Paper - 20 Points
Team Project - 25 Points
Quizzes - 15 Points
Midterm - 20 Points
Final Exam - 20 Points