Montgomery College
Germantown Campus
NW173: Network Security
Master Course Syllabus

Course Description:

An examination of security issues involved in the use of wired networks Tools and techniques used to safeguard private and government enterprise computer organizations are addressed. (Germantown only)

Prerequisite: NW151 or consent of department

Two hours of lecture and three hours laboratory per week for 16 weeks.

Course Topics and Learning Objectives

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

1.Describe the challenge of security information

a. Today's attacks and Defenses
b. Difficulty in Defending against attacks
c. What is Information Security?
d. Information Security Terminology
  * Integrity- Availability- Confidentiality
  * Understanding system security vulnerabilities
e. Preventing Data Theft
f. Thwarting Identity Theft. Avoiding Legal Consequences
  * Health Insurance Portability and Accountability Act (HIPAA)
  * The Sarbanes-Oxley Act of 2002, The German –Leach-Bailey Act (GLBA)
  * USA Patriot ACT (2001)
g. Maintaining Productivity
h. Foiling Cyber terrorism
I. Who are the Attackers?
  * Hackers- Script Kiddies- Employees- Cybercriminals
j. Attacks and Limiting Defense Spies
  * Steps of an Attack
  *Defenses against Attacks (Layering—Diversity Obscurity-Simplicity)
k. Surviving Information Security Careers and the Security + Certification
  * Types of Information Security Jobs
  * CompTA Security + Certification

2. Systems Threats and Risks

a. Software-Based Attacks
b. Infection Malware
c. Concealing Malware (Trojan Horses-Root kits-Logic Bombs)
d. Privilege Escalation
e. Malware for Profit (Spam-Spyware-Key loggers
f. Bonnets
g. Internet Relay Chat
h. Hardware-Based Attacks
*Bios-USB Devices
i. Network Attached Storage (NAS)
j. Cell Phones
k. Attacks on Virtualized Systems
* What is Virtualized Systems? Attacks on Virtual systems

3. Protecting Systems

a. Hardening the Operating System
b. Managing Operating System Updates
* Update Terminology
c. Patch Management Techniques
d. Buffer Overflow Protection
e. Data Execution Prevention (DEP)
f. Address Space Layout Randomization (ASLR)
g. Configuring Operating System Protection
* Security Policy, Configuration baseline, Security Template, Deployment
h. Preventing Attacks that Target the Web Browser
* Cookies, JavaScript, Java and, Active X and Cross Site Scripting (XSS)
* Hardening Web Servers
i. Protecting Systems from Communications-Based Attacks
* Email TCP/IP protocol (SMTP, POP3 and Open Relays), IMAP (Internet Mail Access Protocol)
* Instant Messaging, fax E-mail security policy
j. Peer-to-Peer (P2P) Networks
k. Applying Software Security Applications
* Antivirus, Popup Blockers, Anti-Spam
l. Personal Software Firewalls
m. Host Intrusion Detection Systems (HIDS)

4.Network Vulnerabilities and Attacks

a. Media- Based-Vulnerabilities
b. Network Device Vulnerabilities, Weak Passwords, password management
c. Default Accounts
d. Back Doors
e. Privilege Escalation
f. Categories of Attacks
 * Denial of Service (DoS), Spoofing, Man-in-the-Middle, and replay
g. Method of Network Attacks
 * Protocol-Based Attacks
 * Antiquated Protocols
 * DNS Attack, DNS Spoofing, DNS Poisoning, ARP Poisoning, TCP/IP Hijacking
 * Wireless Attacks
 * Rogue Access Points, War Driving, Bluesnarfing and Blue Jacking, other Attacks & Frauds

5. Network Defenses

a. Crafting a Secure Network through Network Design
b. SubNetting using TCP/IP Protocol
c. Virtual LAN (VLAN)
d. Convergence in digital communications into a single mode of transmission
e. Demilitarization Zone (DMZ)
f. Network Address Translation (NAT)
g. Network Access Control (NAC)
 * using Microsoft Network Access Protection terminology
h. Applying Network Security Devices, applying network software, network protocol
 * Firewall
 * Proxy Server
 * Honey Pot
i. Network Intrusion Detection Systems (NIDS) and Host Network Intrusion Prevention Systems
Protocol Analyzers, Internet Content Filters
j. Integrated Network Security Hardware
 * Antispam, Antivirus, Encryption, Firewall, Instant Messaging System and Web filtering

6. Wireless Network Security

a. EEE.11 Wireless Security Protections, Controlling Access, Wired Equivalent Privacy (WEP)
b. Device Authentication
c. Vulnerabilities of IEEE.11 Security
d. MAC Address Filtering Weaknesses
e. Personal Wireless Security, WPA1 and WPA2
f. PSK Authentication, TKIP Encryption and AES-CCMP Encryption

g. Enterprise Wireless Security, IEEE.11, Enterprise Wireless Security Devices (Thin Access Point) Wireless VLANs

h. system software control

7. ACCESS Control Fundamentals

a. What is Access Control? And Terminology

b. Access Control Models

* Mandatory Access Control (MAC), Discretionary Access Control, Role Based Access Control (RBAC) and Rule Based Access Control (RBAC)

c. Separation of Duties, Job Rotation, Least Privilege and implicit Deny

d. Logical Access Control Methods

* Access Control Lists (ACLs)
* Group Policies
* Account Restrictions, Time of date restrictions and Account Expiration

e. Passwords, password Policy

* Attacks on Password, Password Policy, address security policy

f. Physical Access Control, Door Security, Computer Security. Physical Tokens, ID badge, RFID Mantraps, Video Surveillance and Physical Access Log

8. Authentication

a. definition of Authentication and Access Control Terminology (Authentication-Authorization-Accounting) AAA

b. Authentication Credentials

* One-Time Passwords, Standard Biometrics, Behavioral Biometrics
* Voice Recognition, Computer Foot printing

c. Authentication Models, Single and Multi-factor Authentication

* Single Sign-on, Windows Live ID, Windows Card Space

d. Authentication Servers, RADIUS, Kerberos, TACACS+ an industrial standard protocol

e. Lightweight Directory Access Protocol (LDAP), Extended Authentication Protocols (EAP)

f. Authentication Legacy Protocols

g. Remote Authentication and Security

* Remote Access Services
* Virtual Private Networks (VPNs)

h. Remote Access Policies

9. Performing Vulnerability Assessments

a. Risk Management, Assessment, and Mitigation

b. Steps in Risk Management, Hardware and Software Attribute

* Asset Identification, Threat Identification

c. Vulnerability Appraisal, Risk Management

d. Vulnerability Scanners, Network Mappers and protocol Analyzers
e. Open Vulnerability and Assessment Language
f. Password Crackers, penetration Testing

10. Conducting Security Audits

a. Privilege Auditing and Management
b. Assigning Privileges, Auditing System Security Settings, User Access and Review
c. Group Policies, Storage and Retention Policies
d. Usage Auditing
e. Log Management, Security Application Logs, Security Hardware Logs, Operating system Logs, aiding log
f. Change Management, Change Management Team
g. Monitoring Methodologies and Tools
*Anomaly-Based Monitoring, signature-Based Monitoring
* Monitoring Tools
* System Monitors, Applications, Databases, Desktops, Devices, Even Logs, Networks, Processes
h. Protocol Analyzers

11. Basic Cryptography

a. Defining Cryptography and Security
b. Cryptographic Algorithms, Hashing, Message Digest (MD), Secure Hash Algorithm, Whirlpool
c . Symmetric and Asymmetric Algorithms
d. Data Encryption Standard, Triple Data Encryption Standard, Advanced Encryption Standard
* RSA, Diffie-Hellmanand, Elliptic Curve Cryptography
* using Cryptography on File System and Disks
e. Pretty Good Privacy (PGP)
f. Microsoft Windows Encrypting File System
g. Windows BitLocker, Trusted Platform Module

12. Applying Cryptography

a. Digital Certificates
b. Authorizing, Storing, and working Digital Certificates
*Certificate Revocation List, Certificate Repository
c. Types of Digital Certificates, Personal, Servers, Software Publisher, single and Dual-sided, X.50 Key Infrastructure
d. Public Key Infrastructure (PKI), and PKCS
e. Trust Models, Hierarchical and Distributed and Bridge Trust Model
f. Managing PKI
g. Certificate Policy, Certificate Practice Statement (CPS), Certificate Life Cycle

h. Key Management, Key Storage, Key Usage, Key Handling Procedures
i. Cryptographic Transport Protocols File Transfer Protocols. Secure Sockets Layer (SSI) Transport Layer Security (TLS), Secure Shell (SSH)
j. Web Protocols, Point-to-Point Tunneling Protocol, Layer 2 Tunneling Protocol (L2TP)
k. IP Security (IPsec)

13. Business Continuity

a. Environmental Controls
* Fire Suppression
b. Electromagnetic Shielding, HVAC
c. Reducing Planning
* Servers, Storage (RAID)
d. Networks, Power (UPS)
e. Disaster Recovery Procedures, Planning (Levels,1,2,3), Recovery Team, Purpose and Scope, Preparing for Disaster,

f. Data Backups
g. Incident Response Procedures
* What is Forensics? Secure the Crime Scene, Preserve the Evidence, Establish the Chain of Custody, Examine for Evidence
* RAM Slack

14. Security Policies and Training

a. Organizational Security Policies, What is Security Policy?
b. Balancing Trust and Control
c. Designing a Security Policy
d. The Security Policy Cycle, Steps in Development
* steps in development, due care
f. Types of Security Policies, Acceptable Use Policy
g. Security-Related Human Resource Policy
h. Password Management and Complexity Policy
i. Personality Identifiable (PII) Policy, Disposal and Destruction policy, Service Level Agreement (SLA) policy, Classification of Information Policy, Ethic Policy
i. Education and Training
* Organizational Training
j. Reducing Risks of Social Engineering
Evaluation of Student Performance:

Instructional Materials:

Required Textbook:

Security + Guide to Network Security Fundamentals by Mark Ciampa

- ISBN-10: 1428340661
- ISBN-13: 978-1428340664

Evaluation:

Test 1- 25 %

Midterm - 25 %

Test2 - 25 %

Laboratory - 25 %

Total 100 %