Cybersecurity Syllabus

Course Description

Coursework covers implementation and monitoring of security on network and computer systems. including how to identify and protect against security threats such as hackers, eavesdropping and network attacks, as well as the basics of cryptography. Hands-on labs provide practice in the configuration and mitigation of system vulnerabilities.

Learning Objectives:

Upon conclusion, students will be able to:

- identify and mitigate security threats
- harden internal systems and services
- harden internetwork devices and services
- secure network communications
- manage a PKI
- manage certificates
- enforce an organizational security policy
- monitor the security infrastructure

***** Ethics agreement must be signed by Student and Parent in first week of class. Topics on ethics /cyber law will be integrated across the curriculum.**

1. NETWORK CONCEPTS

1.1. Virtualization

1.2. Network Naming and Connections

1.3. IP Addressing

1.4. DNS and Network Address Translation

1.5. Packet Delivery

1.6. Using Terminal Commands

- *Labs: Windows & Linux client configuration, Net Topology Puzzles, Who's in My IP Club, GangNet, Wireshark Traffic Analysis*

2. Introduction to Security Concepts

2.1. Core principles of CIA = Confidentiality, Integrity & Availability

2.2. Tools to achieve CIA: AAA = authentication, access control and auditing

2.3. Methods of authentication: Tokens , Biometrics, Username / Password , Multi-factor , Mutual

2.4. Remote authentication: PAP, CHAP, Kerberos

- *Labs: Matt Honan's Epic Hacking, Hashes, Password Cracking*

3. Social Engineering

3.1. Define: acquire sensitive data through deception including non-digital techniques

3.2. Statistics on social engineering as largest security risk

3.3. Investigation of current social networking breaches

3.4. OSINT (Open Source Intelligence) and Phishing

3.5. Mitigating Human Risk

- *Project: student videos on social engineering techniques, Project: Phishing with Family, SANS Clean Desk Policy*

4. Reconnaissance

4.1. Online tools for non-interactive recon - Google Dorking

4.2. Scanning - Operating system footprinting and service identification

4.3. Vulnerability assessment

- *Labs: Using Recon Tools - GHDB, whois, nmap, OpenVAS, Nessus*

5. Identifying Security Threats

5.1. Identify the types and characteristics of network attacks

5.2. Define the methods of passwords attacks

5.3. Identify the types and characteristics of malware/software attacks

5.4. Identify the tools available for protection against malware

- *Labs: Man in the Middle attacks, Trojan attacks, Backdoor with Netcat, SYN Flood DoS attack, Cobalt Strike, Metasploit with Armitage*
- *Project: Research and present on assigned historic malware event.*

6. Cryptography and Public Key Infrastructure

6.1. Symmetric vs asymmetric encryption

6.2. Public key encryption

6.3. Hashing to assure message integrity and non-repudiation with digital signatures

6.4. Certificates and PKI (Public Key Infrastructure) in enterprise and on Internet

6.5. Full Disk Encryption and Trusted Platform Module

6.6. Steganography

- *Labs: Basic Crypto Scavenger Hunt, Using SSH and SCP, Implement Certificate Authority/SSL, Message Digests, GPG, Steghide*
- *Project: Privacy vs Security Debate*

7. Hardening Systems and Networks

7.1. Key concepts in closing attack vectors

7.2. Best practices for secure OS configuration - planning and benchmarks

7.3. Hardening with Updates and Local Security Policy configuration

- *Labs: Securing the System Bingo, MBSA Scans, Enumerate with Pass the Hash, DoS with Remote Desktop Connection, Updates with WSUS, Local Security Policies configurations.*

8. Defensive Tools and Techniques

8.1. Firewalls, Intrusion Detection and Intrusion Prevention Systems

8.2. Malware detection methods - anomaly, misuse and signature

8.3. Auditing and Log Analysis

8.4. Defensive hardware tools - VLANS, DMZ, VPN and Honeypots

- *Labs: Configuring IP tables, Snort, Windows System Restore, VPNs, Honeypot configuration*

9. Securing Online Communications

9.1. Vulnerabilities of SSL/TLS - Heartbleed, POODLE, FREAK and LogJam

9.2. Weaknesses of browser plug-ins : Java Applets, Adobe Flash Player and Active X

9.3. Web proxies and Form / Cookie manipulation

9.4. Web code attacks - Buffer Overflows, SQL Injection, Path Traversal, Cross-Site Scripting

9.5. Input validation as a key mitigation technique and fuzzing as a tool to test.

- *Labs using WebDojo VM: Session Fixation, Spoofing a Cookie, Path Traversal, SQL Injection, Buffer Overflows, Burp Proxy Suite*

10. Wireless Security

10.1. Review wireless network concepts and standards

10.2. Identify the risks associated with wireless networking

10.3. Site Surveys to identify wireless network vulnerabilities

- *Labs: Cracking WEP and WPA, Secure WAP Configuration, Site Survey of School Infrastructure.*

11. <u>Cybersecurity - Legal + Ethics + Policies</u>

11.1. Contrast existing cyber laws vs ethics of cyber actions

11.2. Components of effective policies for network and enterprise use.

- *Culminating Project: research assigned cybercrime to assess what laws were broken, consequences imposed (if any) and directly relate crime to class ethics agreement.*

Recommended Lab Manual: Principles of Computer Security Lab Manual

Author: By Vincent Nestler and Keith Harrison and Matthew Hirsch and Wm. Arthur Conklin

Publisher: McGraw Hill, 2015

Note: this lab manual uses Windows 7 and Windows 2008 Server virtual machines. These Operating systems are outdated but this is the only lab manual I have ever found with valuable, well written cybersecurity labs. I highly recommend getting a copy to use as a reference to create your own labs with more modern operating systems.