C S 53A: CYBERSECURITY FUNDAMENTALS

Foothill College Course Outline of Record

Heading	Value
Effective Term:	Summer 2021
Units:	4.5
Hours:	4 lecture, 2 laboratory per week (72 total per quarter)
Advisory:	C S 50A.
Degree & Credit Status:	Degree-Applicable Credit Course
Foothill GE:	Non-GE
Transferable:	CSU
Grade Type:	Letter Grade (Request for Pass/No Pass)
Repeatability:	Not Repeatable

Student Learning Outcomes

- A successful student will be able to demonstrate an understanding of the role certificates and be able to explain basic concepts of Key Management and Certificate Lifecycles
- A successful student will be able to recognize and understand the administration of basic remote access security technologies

Description

The fundamental aspects of computer and network security as it pertains to policy deployment and network defense. Core topics include cryptography, public key infrastructure, standards and protocols, physical security, infrastructure security, remote access, messaging, intrusion detection and system baselines. Industry-specific topics include certifications for CompTIA's Security+, ISC2, SSCP.

Course Objectives

The student will be able to:
A. Recognize and explain access control models.
B. Recognize the common attacks and specify the appropriate actions to take to mitigate vulnerability.
C. Recognize and understand the administration of remote access technologies.
D. Recognize and understand the administration of internet security concepts.
E. Understand security concerns and concepts for common network devices.
F. Understand security concerns regarding various network media.
G. Identify and explain common cryptographic algorithms.
H. Understand and explain the concepts of key management and certificate lifecycles.
I. Understand the basic concepts of physical security.
J. Understand the uses of written security policies and procedures.
K. Understand and explain specific documentation concepts.

Course Content

A. Access control models
1. MAC (Mandatory Access Control)
2. DAC (Discretionary Access Control)
3. RBAC (Role Based Access Control)
B. Attacks and the appropriate actions to take to mitigate vulnerability
1. DOS/DDOS (Denial of Service/Distributed Denial of Service)
2. Spoofing of addresses
3. Password guessing
C. Remote access technologies
1. 802x1x
2. VPN
3. RADIUS
4. TACACSIPSec
D. Administration of web security
1. SSL/TLS
2. HTTPS
3. Instant messaging vulnerabilities
E. Network device security
1. Firewalls
2. Switches
3. Routers
4. Workstations
5. Servers
F. Network media and security
1. Coaxial cable
2. UTP/STP
3. Fiber optic cable
G. Cryptographic algorithms
1. Hashing
2. Symmetric
3. Asymmetric
H. Key management and certificate lifecycles
1. Centralized vs. decentralized
2. Storage
3. Escrow
4. Expiration and revocation
5. Renewal
I. Physical security
1. Access control
2. Social engineering
3. Environment
J. Security policies and procedures
1. Security policy
2. Incident response policy
K. Documentation required to support security
1. Standards and guidelines
2. Systems architecture
3. Change documentation
4. Retention/storage
5. Destruction

Lab Content

A. Network devices and technologies - capturing network traffic
1. Use tcpdump to capture network traffic
2. Capture and analyze traffic with Wireshark
3. Capture and analyze traffic with Network Miner
B. Secure network administration principles - log analysis
1. Perform log analysis in Linux using Grep
2. Perform log analysis in Linux using Gawk
3. Perform log analysis in Windows using Find
C. Protocols and default network ports - transferring data using TCP/IP
1. Use HTTP to transfer files
2. Use FTP to transfer files
3. Transfer files securely using SCP

D. Connect to a remote system to analyze protocols and default network ports
1. Connect to a Windows system through the command line
2. Connect to a Linux system through the command line
3. Analyze network traffic using a remote connection
E. Secure implementation of wireless networking
1. Examine plain text traffic
2. Crack and examine WEP traffic
3. Crack and examine WPA traffic
F. Incident response procedures - compliance and operational security
1. Using db_autopwn to attack a remote system
2. Collect volatile data
3. View network logs
G. Configure the pfSense firewall
1. Configure ICMP on the firewall
2. Redirect traffic to internal hosts on the network
3. Set up a Virtual Private Network
H. Configure backups - compliance and operational security
1. Back-up files to a network drive
2. Back-up files to an FTP server
3. Back-up files using SCP
I. Analyze and differentiate types of malware - threats and vulnerabilities
1. Use Netcat to send a reverse shell
2. Use Ncat to send a reverse shell
3. Send a Bash shell to a Windows machine using NetCat
J. Analyze and differentiate types of attacks using Windows CLI commands - threats and vulnerabilities
1. View network resources
2. Use PSEXEC to connect to a remote system
3. Stop, start, and remove services
K. Analyze and differentiate types of application attacks - threats and vulnerabilities
1. Scan the network for vulnerable systems
2. Use Metasploit and explore its use as a framework for exploitation
3. Attack a remote system utilizing Armitage
L. Mitigation and deterrent techniques - anti forensic threats and vulnerabilities
1. Use the Windows Event Viewer
a. Enabling auditing
b. Clear the event logs
M. Mitigation and deterrent techniques applied to password cracking
1. Crack Linux passwords
2. Scan the network for vulnerable systems
3. Use Nessus to search for vulnerable systems
N. Importance of data security - data theft
1. Using Metasploit to attack a remote system
2. Steal data using FTP and HTTP
3. Steal data using Meterpreter
O. Importance of data security - securing data using encryption software
1. Install TrueCrypt
2. Create a TrueCrypt container
3. Open and view data within a TrueCrypt container
P. Authentication, authorization and access control
1. Add users, groups, and passwords to Windows and Linux systems
2. Use symbolic permissions
3. Use absolute permissions
Q. Access controls
1. Configure ICMP on the firewall
2. Configure auditing for object access
3. View the security log to determine security incidents
R. General cryptography concepts
1. Hide a picture within a picture using S-Tools
2. Hide a media file within a picture using S-Tools
3. Reveal hidden data using S-Tools
4. Encrypt files with the Microsoft Encrypted File System
5. Back-up Encrypted File System keys
6. Recovery Encrypted File System files

Special Facilities and/or Equipment

A. Access to a network laboratory with current Cisco network equipment host computers required to support the class.
B. A website or course management system with an assignment posting component (through which all lab assignments are to be submitted) and a forum component (where students can discuss course material and receive help from the instructor). This applies to all sections, including on-campus (i.e., face-to-face) offerings.
C. When taught via Foothill Global Access on the Internet, the college will provide a fully functional and maintained course management system through which the instructor and students can interact.
D. When taught via Foothill Global Access on the Internet, students must have currently existing email accounts and ongoing access to computers with internet capabilities.

Method(s) of Evaluation

Methods of Evaluation may include but are not limited to the following:

Tests and quizzes
Written laboratory assignments
Final examination

Method(s) of Instruction

Methods of Instruction may include but are not limited to the following:

Lectures which include motivation for the architecture of the specific topics being discussed
In-person or online labs (for all sections, including those meeting face-to-face/on-campus), consisting of:
1. An assignment webpage located on a college-hosted course management system or other department-approved internet environment. Here, the students will review the specification of each assignment and submit their completed lab work
2. A discussion webpage located on a college-hosted course management system or other department-approved internet environment. Here, students can request assistance from the instructor and interact publicly with other class members
Detailed review of laboratory assignments which includes model solutions and specific comments on the student submissions
In-person or online discussion which engages students and instructor in an ongoing dialog pertaining to all aspects of designing, implementing and analyzing programs
When course is taught fully online:
1. Instructor-authored lecture materials, handouts, syllabus, assignments, tests, and other relevant course material will be delivered through a college-hosted course management system or other department-approved internet environment
2. Additional instructional guidelines for this course are listed in the attached addendum of CS department online practices

Representative Text(s) and Other Materials

Gibson, Darril. CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, 4th ed.. 2017.

Types and/or Examples of Required Reading, Writing, and Outside of Class Assignments

A. Reading
1. Textbook assigned reading averaging 30 pages per week.
2. Online curriculum averaging 20 pages per week.
3. Online resources as directed by instructor though links pertinent to networking.
4. Library and reference material directed by instructor through course handouts.
B. Writing
1. Technical prose documentation that supports and describes the laboratory exercises that are submitted for grades.

Discipline(s)

Computer Science