C S 53C: ETHICAL HACKING

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 53A.
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 perform footprinting to learn about a company and its network
- A successful student will be able to explain what an ethical hacker can and can not do legally, and explain the credentials and roles of penetration testers

Description

Surveys current techniques used by malicious hackers to attack computers and networks, and develops the defenses that security professionals use to defend Windows and Linux systems from such attacks. Topics will be presented in the context of legal restrictions and ethical guidelines. Hands-on labs, playing the role of both attacker and defender, using port scans, footprinting, buffer overflow exploits, SQL injection, privilege escalation, Trojans, and backdoors.

Course Objectives

The student will be able to:
A. Explain what an ethical hacker can and cannot do legally, and explain the credentials and roles of penetration testers.
B. Understand the basics of the TCP/IP protocol suite.
C. Define the types of malicious software found in modem networks.
D. Explain the threats and countermeasures for physical security and social engineering.
E. Perform footprinting to learn about a company and its network.
F. Perform port scans to locate potential entry points to servers and networks.
G. Perform enumeration (finding resources, accounts, and passwords) on Microsoft and Unix/Linux targets.
H. Perform very simple scripting and coding tasks, specifically oriented towards the needs of network security professionals.
I. Identify Microsoft Windows vulnerabilities and understand how to harden systems.
J. Identify Linux vulnerabilities and understand how to protect servers.
K. Describe how to take control of web servers, and how to protect them.
L. Locate and hack into wireless networks, and protect them.
M. Explain how cryptography and hashing work, and perform attacks against them such as password cracking and man-in-the-middle attacks.
N. Describe and deploy security devices, including routers, firewalls, intrusion detection systems, and honeypots.

Course Content

A. Ethical hacking overview
1. What is ethical hacking?
a. The role of security audits and penetration testers
b. Penetration testing methodology
c. Certification programs for network security personnel
2. Legal background
a. State and Federal laws
b. Recent cases
c. The legality of port scanning
d. How to protect ethical hackers and clients with a written contract
B. TCP/IP concepts review
1. The TCP/IP protocol stack
a. The four layers
b. Essential protocols and ports
2. IP addressing
3. Decimal, binary, octal, and hexadecimal numbering systems
C. Network and computer attacks
1. Malware
a. Viruses and worms
b. Trojans
c. Spyware and adware
2. Protecting against malware attacks
a. Technical measures including antivirus and antispyware programs
b. How to educate users without scaring them
3. Internet attacks
a. Denial of Service attacks
b. Buffer overflow
c. Ping of Death
d. Session hijacking
4. Physical security
a. Keyloggers
b. Lock picking
D. Footprinting
1. Gathering information about a company
a. Analyzing a website
b. Searching the web for email addresses
c. Using HTTP headers
2. DNS zone transfers
E. Social engineering
1. Shoulder surfing
2. Dumpster diving
3. Piggybacking to enter secure areas
F. Port scanning
1. Types of port scans, such as SYN, Connect, NULL, XMAS, ACK, FIN, UDP
2. Port-scanning tools, such as NMAP, UnicornScan, Netscan Tools Pro, Nessus
3. Ping sweeps
4. Shell scripting
G. Enumeration
1. Microsoft Windows systems
a. Windows versions
b. NETBIOS tools including nbtstat, NetScanTools Pro, DumpSec, Hyena, NessusWX
2. Unix/Linux systems
a. Versions of UNIX and Linux
b. Tools including finger
H. Scripting and coding for security professionals
1. Fundamentals
2. Writing a webpage in HTML

3. Writing a Perl script
4. Object-oriented programming
5. Using the Win32 API
I. Microsoft operating system vulnerabilities
1. Tools to identify vulnerabilities in Microsoft systems, such as Microsoft Baseline Security Analyzer, HFNetChk, Winfingerprint
2. Types of Microsoft vulnerabilities, such as Remote Procedure Calls, NetBIOS, SMB, Common Internet File System, Samba, default installations, password policies
3. Vulnerabilities in Microsoft services
4. Hardening Microsoft systems
J. Linux operating system vulnerabilities
1. Linux fundamentals, including directory structure, file system, commands
2. Linux OS vulnerabilities
a. Nesus, Samba vulnerabilities, remote access attacks
b. Installing, finding, and removing rootkits, finding rootkits
c. Creating buffer overflow programs
d. Using a sniffer
K. Hacking web servers
1. Web application components
a. Forms, CGI scripts, ASP
b. Scripting in PHP, ColdFusion, VBScript, JavaScript
c. Connecting to databases with ODBE, OLE DB, and ADO
2. Application vulnerabilities and countermeasures
a. Open Web Application Security Project (OWASP)
b. Assessing web applications for vulnerabilities
3. Tools of web attacks and security testers, such as Cgiscan, phfscan, wfetch
L. Hacking wireless networks
1. Components of a wireless network, including access points, SSIDs, Wireless NICs
2. Wireless network standards, including 802.11, 802.lla, b, e, g, I, Bluetooth
3. Authentication
a. 802.IX, PPP, EAP, PEAP
b. WEP and WPA
4. Wardriving such as Netstumbler and Kismet
5. Wireless hacking tools such as AirSnort, WEPCrack
6. Countermeasures for wireless attacks
M. Cryptography
1. Cryptography basics
2. Symmetric algorithms such as DES, 3DES, AES, IDEA, Blowfish and RC5
3. Asymmetric algorithms such as RSA, Diffie-Hellman, Elliptic-Curve Cryptosystems, Elgamal
4. Digital signatures, including DSS and PGP
5. Hashing algorithms, including MD2, MD4, MD5, SHA, HAVAL
6. Public key infrastructure
7. Cryptography attacks, including Birthday, mathematical, brute force, man-in-the-middle, dictionary, replay
8. Password cracking tools, including John the Ripper, Hydra, EXPECT, LOphtcrack, Pwdump
N. Protecting networks with security devices
1. Routers
a. Cisco router configuration
b. Access control lists
2. Firewalls
a. NAT, ACL, packet filtering, stateful packet inspection
b. Demilitarized Zone
c. PIX firewall
d. Microsoft ISA
3. Intrusion detection systems network and host-based
4. Honeypots

Lab Content

A. Using active and passive techniques to enumerate network hosts
1. Introduction to ethical hacking
2. Scan networks
3. Perform enumeration
4. Explore packet sniffers
B. Conduct active and passive reconnaissance against a target
1. Become familiar with ethical hacking
2. Perform footprinting and reconnaissance
3. Scan networks
4. Investigate social engineering techniques
C. Use the SYSTEM account
1. Hack the SYSTEM account
D. Poison Ivy remote access Trojan
1. Perform system hacking
2. Explore Trojans and backdoors
3. Explore the differences between viruses and worms
E. Using the SHARK Remote Administration Tool
1. Explore how the tool supports system hacking
2. Use the tool to explore Trojans and backdoors
3. Use the tool to viruses and worms
F. Utilizing malware - DarkComet
1. Explore DarkComet as a system hacking tool
2. Use DarkComet to detect Trojans and backdoors
3. Use DarkComet to detect viruses and worms
G. Breaking Windows passwords
1. Perform system password hacking
H. Using John the Ripper to crack Linux passwords
1. Perform system hacking
I. Using spear phishing to target an organization
1. Perform system hacking
2. Explore spear phishing's use as a social engineering tool
3. Perform session hijacking
J. Break WEP and WPA encryption
1. Hack wireless networks
K. Use Metasploit to attack a remote system
1. Perform network scanning
2. Perform numeration
3. Explore the various sniffers
4. Evade IDS, firewalls, and honeypots
L. Use Armitage to attack the network
1. Review its use in ethical hacking
2. Use it to perform footprinting and reconnaissance
3. Scan networks
4. Perform system hacking
5. Perform penetration testing
M. Exploit IPv6 networks
1. System hacking
N. Creating MSFPAYLOAD
1. System hacking
2. Explore Trojans and backdoors
3. Detect viruses and worms
4. Perform penetration testing
O. Abusing SYSTEMS
1. Perform a denial of service attack
P. SQL injection
1. Describe how the hack web servers
2. Hacking web applications
3. Explore SQL injection attacks

Q. The buffer overflow attack
1. Explain its use in system hacking
2. Launch a buffer overflow attack
R. Intrusion detection
1. Explore how to use IDS
2. Explore how to use firewalls
3. Explore the use of honeypots
S. Use certificates to encrypt email
1. Encrypt and decrypt emails

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

Tests and quizzes
Written laboratory assignments
Final examination

Method(s) of Instruction

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

Velu, Vijay, and Robert Beggs. Mastering Kali Linux for Advanced Penetration Testing, 3rd ed.. 2019.

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