CS 5781 Computer & Network Security (Fall 2020 v1.12)

Lectures: Tuesdays 6:00-8:45pm online via Canvas & Zoom **https://calstatela.zoom.us/j/275729130**

Instructor: Edmund Gean Email: egean@calstatela.edu

Office Hours: Tuesdays 5:30-6pm & 8:45-9:15pm

Description: This course exposes students to various techniques related to defending your computers and networks. Topics covered include Denial-Of-Service attacks, packet analyzers, host-based intrusion detection, firewalls, and VPN. Lab exercises and projects will be included to foster greater understanding in this field.

Course Goals:

At the end of the course, students will be able to:
-perform a security assessment of an organization's network via penetration test and identify vulnerabilities
-harden MS Windows and Unix operating systems
-install intrusion detection systems, firewalls, and VPNs

Prerequisites:

CS4471 (computer networks) or CS4470 (computer networking protocols)
http://cs3.calstatela.edu/~egean/cs4471/

Required textbook:

Counter Hack Reloaded by Ed Skoudis
http://cs3.calstatela.edu/~egean/cs5781/lecture-notes/counterhack/
ebook of textbook available at Safari Books online at https://calstatela.libguides.com/az.php?a=s
https://learning.oreilly.com/library/view/counter-hack-reloaded/9780131481046/

Recommended textbooks:

Network Security Principles and Practices by Saadat Malik
http://cs3.calstatela.edu/~egean/cs5781/ebooks/network-security-principles-and-practices.pdf
http://cs3.calstatela.edu/~egean/cs5781/lecture-notes/malik/
CEH v9: Certified Ethical Hacker Version 9 Study Guide / Edition 3
(lecture notes available online at http://cs3.calstatela.edu/~egean/cs5781/lecture-notes/CEHv9)

Personal computer with the following software installed:

Nmap/Zenmap/Ncat(netcat)/Nping https://nmap.org/download.html for Windows, Linux, & MacOS
Nessus https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true
Cisco Packet Tracer 7.3 https://www.netacad.com/courses/packet-tracer
Snort (http://www.snort.org)
VMware Workstation Player 15 for Windows
https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html or
Oracle VirtualBox 6.1 for Windows, Mac, or Linux http://virtualbox.org/
Kali Linux 2020 VM for VMware and VirtualBox
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
metaploitable2 Linux VM image https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Wireshark 3.2.6 https://www.wireshark.org/download.html

Putty 0.72 https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html
Solarwinds TFTP server software https://www.solarwinds.com/free-tools/free-tftp-server
various VM images (Ubuntu, Windows7, Windows server)
GNS3 VM image for Vmware ver 2.1.21 https://www.gns3.com/software/download-vm

References:

Free Safari Books online at https://calstatela.libguides.com/az.php?a=s
Documentation of Cisco equipment at http://www.cisco.com
YouTube videos

Topics:

Denial-Of-Service attacks & hacker techniques
Port scanning, penetration, and vulnerability testing
packet analyzers and sniffers
host and network-based intrusion detection
firewalls, packet filters, and access control lists
securing Unix and Window systems
authentication, authorization, and accounting
data integrity checking & encryption schemes

Lab Assignments: Students will gain practical experience through the following lab projects.
All student work should be submitted via Canvas https://calstatela.instructure.com

- scan a network to locate machines and open ports
- find vulnerabilities on machines
- configure firewall & setup VPN
- setup network-based intrusion detection system
- setup AAA server to perform authentication, authorization, and accounting
- use Metasploit to exploit vulnerability on Metasploitable VM

Grading policy: Overall grade will be comprised of the following components:
attendance (10%), lab assignments (40%), special project (10%), and final exam (40%)
A 90-100; B 80-89; C 65-79; D 50-64; F 0-49

Americans with Disabilities Act (ADA):

Reasonable accommodation will be provided to any student who is registered with the Office of Students with Disabilities and requests needed accommodation. For more information visit the Office for Students with Disabilities home page.

Extra Credit:

(up to 10%) register & participate in National Cyber League
https://www.nationalcyberleague.org/fall-season
After registering for NCL, student should assign Edmund Gean as faculty coach
https://cyberskyline.com/events/ncl/coach/Y1HD-JNYK-QRRC

(15%) pass Cisco CyberOps Associate Exam 200-201
https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.htm
https://proquest.safaribooksonline.com/book/certification/ccna/9780134609003
https://proquest.safaribooksonline.com/book/certification/ccna/9780134608938
http://www.pearsonvue.com/cisco/

(10%) pass EC-Council's Certified Ethical Hacker Exam (312-50)
http://proquest.safaribooksonline.com/book/certification/ceh/9781119252245
http://www.pearsonvue.com/eccouncil/

Academic Honesty: Students are expected to do their own work and to abide by the University Policy on academic honesty. You are expected to familiarize yourself with the Cal State LA Academic Honesty Policy including Appendix D – Academic Honesty and Appendix E - Student Conduct / Student Conduct Procedures. All work you submit must be your own scholarly and creative efforts. Cal State LA plagiarism as follows: "At Cal State LA, plagiarism is defined as the act of using ideas, words, or work of another person or persons as if they were one's own, without giving proper credit to the original sources."

CS 5781 Reading and Lab Project Assignments (Fall 2020 v1.12)

Week	Lecture	Lab Project
#1 Aug 25	Chapters 1,2 (Counter Hack) Introduction Network Overview Chapter 1,2,9 (CEH) Intro System Fundamentals Sniffers	Become familiar with creating a network using Cisco Packet Tracer. Enroll in Cisco Network Academy, view Introduction to Packet Tracer course, and download Packet Tracer at https://www.netacad.com/courses/packet-tracer or https://www.netacad.com/courses/packettracer/introduction-packet-tracer Create and configure a very simple network containing a computer and a server that is separated by just one router. Label each network interface with an appropriate unique IP address. Submit screenshot of your Packet Tracer network topology. Submit output of the router configuration (show running-config). Also submit a screenshot showing successful output of traceroute (tracert) from PC to server. Hints can be found at https://www.youtube.com/watch?v=Tp10jMxdbWk -security lab network topology -sign up for lab seating -lab computer login accounts and passwords -VM accounts and passwords
#2 Sep 1	Chapters 3,6 (Counter Hack) Unix Overview Scanning (eg nmap, Nessus) Chapter 4,5 (CEH) Footprinting (reconnaisance) Scanning(eg. Nmap)	**Port scanning & Packet Capture** Install nmap (or Zenmap) (http://nmap.org) port scanner onto your laptop or home computer and perform a TCP port scan and a UDP port scan of target scanme.nmap.org. Answer each of the following items. 1. Which TCP ports and services were open? What nmap option flags did you use to accomplish the TCP port scan? Provide nmap (or Zenmap) output as evidence. 2. Which UDP port and service was open? What nmap option flags did you use to accomplish the UDP port scan? Provide nmap (or Zenmap) output as evidence. 3. What is target's IP address and operating system? Provide supporting evidence from output of nmap (or Zenmap). 4. While performing a TCP connect scan (-sT) of scanme.nmap.org , use Wireshark to capture, filter, and decode packets associated with a TCP connection where the 3-way handshake completed successfully. What was the value of the absolute (raw) initial sequence number used by nmap(or Zenmap) ? What was the absolute (raw) initial sequence number used by scanme.nmap.org? (Hint: see slide 18 of chapter 6 and watch YouTube videos on Wireshark if needed)
#3 Sep 8	Chapter 4 & 5 (Counter Hack) Windows NT/2000 Overview Reconnaissance Chapter 3,6 (CEH) Cryptography Enumeration	**Penetration and Vulnerability testing** Install a network-based vulnerability scanner Nessus Essentials and activation code from www.nessus.org onto your computer. Afterwards run the Tenable Nessus web client https://localhost:8834 and perform a vulnerability scan of a few devices (computer, server, networked printer, and smartphone). Submit vulnerability report of the one device that has the highest security risk (services that pose medium or high security risk). Be sure to temporarily turn off any host-based firewall software if needed to get meaningful output.

#4 Sep 15	Chapters 5-8 (Malik) Secure Switching NAT Firewalls Cisco ASA firewall	**Firewall Lab Assignment** http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Cisco%20ASA%20Firewall%20Lab%20Assignment.pdf
#5 Sep 22	Chapter 7 (Counter Hack) Gaining Access via application/OS attacks Chapter 7,8 (CEH) System Hacking Malware	(NCL regular season registration 8/24-10/2) *test your knowledge in Open Source Intelligence, Cryptography and Steganography, Log Analysis, Network Traffic Analysis, Scanning and Reconnaissance, Password Cracking, Wireless Access Exploitation, Web Application Exploitation, Enumeration and Exploitation* https://www.nationalcyberleague.org/fall-season (NCL gymnasiums opens Sept 14, 2020)
#6 Sep 29	Chapters 10, & 13 (Malik) VPN IPSEC	**IPSec VPN** http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Cisco%20IPSec%20VPN%20Lab%20Assignment.pdf
#7 Oct 6	Chapter 8 (Counter Hack) Gaining access via network attacks Chapter 10,18,19 (CEH) Social Engineering Cloud Technology Physical Security	
#8 Oct 13	**TBA (NCL?)**	**Security Challenge** http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/security%20challenge.pdf (mandatory NCL Preseason game 10/12-10/19 for participants; submit score)
#9 Oct 20	Chapters 9, 14, & 15 (Malik) IOS firewall Network Intrusion Detection Cisco Secure IDS Chapter 17 (CEH) Evasion & IDS	(NCL regular season game weekend 10/23-10/25 for participants; submit score) **Network intrusion detection system** Install Snort (http://www.snort.org) onto your computer (or into Kali Linux or Ubuntu Desktop via apt-get install snort). Download latest Snort rules and modify configuration file snort.conf . Simulate two different network attacks against your computer. Turn in a listing of two different alerts that the snort IDS detected and submit printout of the two signature definitions Snort used from its "*.rules" signature definition files to detect the two types of attack.
#10 Oct 27	Chapter 9 (Counter Hack) Denial-of-Service attacks Chapter 11,12 (CEH) Denial of Service Session Hijacking	Special Project signup
#11 Nov 3	Chapters 16-18 (Malik) AAA TACACS+ RADIUS	**AAA** http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Cisco%20AAA%20Lab%20Assignment.pdf
#12 Nov 10	Oracle VirtualBox (or VMware), Kali Linux, Metasploit, Metasploitable	**Exploit code generation using Metasploit** http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Metasploit%20Lab%20Assignment.pdf

#13 Nov 17	Chapter 10 (Counter Hack) Maintaining Access Chapter 13,14 (CEH) Web Servers and Applications SQL Injection	**Web Application Security, Vulnerabilities, and Challenges**
#14 Nov 24	Fall Recess (no class)	
#15 Dec 1	Chapter 11 (Counter Hack) Covering Tracks and Hiding Chapter 15,16 (CEH) Hacking WiFi and Bluetooth Mobile Device Security	
#16 Dec 8	**Special Project Presentations**	
#17 Dec 15	**Final Exam (Dec 15, 2020) 6:00 pm**	