# CS 5781 Computer & Network Security (Fall 2024 v1.5)

**Lectures:** Mon & Wed 6:00-7:15pm FA 218 and possibly online via Zoom meeting ID 815 4671 3747 and passcode 578124
https://calstatela.zoom.us/j/81546713747?pwd=bF8GgPxWDjA90pReN0aH9Qz4hkodUY.1

**Instructor:** Edmund Gean Email: egean@calstatela.edu

**Office Hours:** Mon & Wed 6:00-7:15pm FA 218

**Graduate Assistant:** Jatin Narendrabhai Soni Email: jsoni5@calstatela.edu

**Description:** This course exposes students to various techniques related to defending networked servers and devices. Topics covered include port scanning, vulnerability testing, packet sniffing and analysis, intrusion detection systems, Denial-Of-Service attacks, firewalls, VPN, and AAA. 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 and configure intrusion detection systems, firewalls, and VPNs

**Course Structure:**

This course will be conducted in-class and/or online. Submission of assignments will be through Cal State LA learning management system Canvas at https://canvas.calstatela.edu/ .

**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 Oreilly Books online at https://libguides.calstatela.edu/az.php?a=o
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 7.95 https://nmap.org/download.html for Windows, Linux, & MacOS
Nessus 8.15 https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true for Win, Linux, MacOS
Cisco Packet Tracer 8.2.2 https://www.netacad.com/courses/packet-tracer for Windows, Ubuntu, & MacOS
Snort (http://www.snort.org)
**V**Mware Workstation Player 17 for Windows or Linux
https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html ,
VMware Workstation Pro 17.6 for Personal Use (Windows) [*Note: need to create user account*]

https://support.broadcom.com/group/ecx/productdownloads?subfamily=VMware+Workstation+Pro , or
Oracle VirtualBox 7.0.20 for Windows, Mac, or Linux http://virtualbox.org/
Kali Linux 2024 VM for VMware and VirtualBox https://www.kali.org/get-kali/#kali-virtual-machines
Ubuntu 24.04 desktop iso https://ubuntu.com/download/desktop
metaploitable2 Linux VM image https://sourceforge.net/projects/metasploitable/files/Metasploitable2/
Wireshark 4.2.6 https://www.wireshark.org/download.html for Windows and MacOS

**References:**

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

**Lab Assignments:** Students will gain practical experience through projects such as the following.

- 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

All student work should be submitted via Canvas https://calstatela.instructure.com . Homework submission format of Cisco Packet Tracer assignments should adhere to guidelines described at https://cs3.calstatela.edu/~egean/cs5781/Homework%20submissions%20format.pdf

Late submission of assignments may be penalized one point during first week assignment is past due. For each additional week past due date, submitted assignment may be penalized an additional point.

**Grading policy:** Overall grade will be comprised of the following components:

attendance (5%), participation (5%), 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 15%) register & participate in National Cyber League Competition
https://nationalcyberleague.org/competition
After registering for NCL, student should assign Edmund Gean as faculty coach
https://cyberskyline.com/events/ncl/coach/Y1HD-JNYK-QRRC
Participants shall adhere to NCL rules of conduct
https://cs3.calstatela.edu/~egean/cs5781/NCL%20Abridged%20Rules%20of%20Conduct.pdf
Rules of Conduct (nationalcyberleague.org)

(15%) pass Cisco CyberOps Associate Exam 200-201
https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/cyberops-associate.html
https://learning.oreilly.com/videos/cisco-cyberops-associate/9780137333455/
https://learning.oreilly.com/library/view/cisco-cyberops-associate/9780136807964/
http://www.pearsonvue.com/cisco/

# HELPFUL STUDENT RESOURCES

## *Technical Resources*

Information on Cal State LA technical support resources for students: Technical Support Resources

## *Student Support Resources*

Information on Cal State LA student support resources for students: Student Support Resources

## *Academic Support Resources*

Information on Cal State LA academic support resources for students: Academic Support Resources

## Center for Academic Success

The Center for Academic Success (CAS) supports all students throughout their educational journey. You are encouraged to visit a CAS tutor for STEM, social science, or writing tutoring early in the semester. The academic services CAS provides are inclusive, engaging, challenging, and impactful. CAS tutors offer a one-on-one opportunity to discuss your assignments and will provide you with tools to become an independent scholar. The appointments are 30 minutes long. Log on to the Student Success Collaborative portal to make an appointment online.

## *Canvas Student Support*

Information for students on how to be a successful online student and how to use Canvas:

- Canvas Student Guide

## *Glazer Family Dreamers Resource Center*

The Erika J. Glazer Family Dreamers Resource Center promotes the success of undocumented students and students from mixed-status families at Cal State LA through a variety of resources, services, and community engagement opportunities. Such programs and services are weekly immigration legal clinics, California Dream Act Application for Financial Aid Assistance, and professional and academic development workshops.

# UNIVERSITY POLICIES

## *Student Conduct*

Information on student rights and responsibilities, standards of conduct, etc., can be found by visiting the Cal State LA University Catalog Appendices.

## *Dropping and Adding*

Students are responsible for understanding the policies and procedures about add/drops, academic renewal, etc. Students should be aware of the current deadlines and penalties for adding and dropping classes by visiting the GET home page. (Registrar news and information)

## *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.

## *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 2024 v1.5)

| Week | Lecture | Lab Project |
|---|---|---|
| #1<br>Aug 21<br>& 26 | Chapters 1,2 (Counter Hack)<br>Introduction<br>Network Overview<br>Chapter 1,2,9 (CEH)<br>Intro<br>System Fundamentals<br>Sniffers | **Lab1:** 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 . 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. Homework submission format should adhere to guidelines at https://cs3.calstatela.edu/~egean/cs5781/Homework%20submissions%20format.pdf Hints can be found at https://www.youtube.com/watch?v=Tp10jMxdbWk |
| #2<br>Aug 28<br>&Sep 4<br><br>Holiday<br>Sep 2 | Chapters 3,6 (Counter Hack)<br>Unix Overview<br>Scanning (eg nmap, Nessus)<br>Chapter 4,5 (CEH)<br>Footprinting (reconnaisance)<br>Scanning(eg. Nmap ) | **Lab2: Port scanning & Packet Capture**<br>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.<br><br>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.<br><br>2. Which UDP port and service was open? If none, find and scan another target that has open UDP port(s). What nmap option flags did you use to accomplish the UDP port scan? Provide nmap (or Zenmap) output as evidence.<br><br>3. What is target's IP address and operating system? Provide supporting evidence from output of nmap (or Zenmap).<br><br>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<br>Sep 9<br>Sep 11 | Chapter 4 & 5 (Counter Hack)<br>Windows NT/2000 Overview<br>Reconnaissance<br>Chapter 3,6 (CEH)<br>Cryptography<br>Enumeration | **Lab3: Penetration and Vulnerability testing**<br>Install a network-based vulnerability scanner Nessus Essentials and activation code from https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true 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, high, or critical security risk). Include screenshot of report that lists the name(s) of these discovered vulnerabilities. Be sure to temporarily turn off any host-based firewall software if needed to get meaningful output. |

| | | |
|---|---|---|
| #4<br>Sep 16 & 18 | Chapters 5-7 (Malik)<br>Secure Switching<br>NAT<br>Firewalls | **Lab4: Firewall Lab Assignment**<br>http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Cisco%20ASA%20Firewall%20Lab%20Assignment.pdf |
| #5<br>Sep 23 & 25 | Chapters 8 (Malik)<br>Cisco ASA firewall | (NCL regular season registration 8/19-10/11) *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*<br>https://www.nationalcyberleague.org/fall-season<br>(NCL gymnasium opens August 19 – Dec 13, 2024) |
| #6<br>Sep 30 & Oct 2 | Chapter 7 (Counter Hack)<br>Gaining Access via application/OS attacks<br>Chapter 7,8 (CEH)<br>System Hacking<br>Malware | **Lab5: Security Challenge**<br>http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/security%20challenge.pdf |
| #7<br>Oct 7 & 9 | Chapters 10, & 13 (Malik)<br>VPN<br>IPSEC | **Lab6: IPSec VPN**<br>http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Cisco%20IPSec%20VPN%20Lab%20Assignment.pdf |
| #8<br>Oct 14 & 16 | Chapter 8 (Counter Hack)<br>Gaining access via network attacks<br>Chapter 10,18,19 (CEH)<br>Social Engineering<br>Cloud Technology<br>Physical Security | (NCL Practice game Oct 14 – Oct 20, 2024 mandatory for participants; submit score) |
| #9<br>Oct 21 & 23 | Chapters 9, 14, & 15 (Malik)<br>IOS firewall<br>Network Intrusion Detection<br>Cisco Secure IDS<br>Chapter 17 (CEH)<br>Evasion & IDS | (NCL regular season game weekend Oct 25- Oct 27, 2024 mandatory for participants; submit score)<br>**Lab7: Network intrusion detection system**<br>Install Snort (http://www.snort.org) onto your computer (or into Kali Linux or into **Ubuntu Desktop** via "apt-get install snort"). Download latest Snort rules if needed and modify configuration file /etc/snort/snort.conf . Simulate two different network attacks against your computer while running Snort . Submit screenshot of alert messages displayed for two different types of traffic detected by Snort IDS. In addition, submit printout of the two signature definitions Snort used from its "*.rules" signature definition files in folder /etc/snort/rules to generate the two alert messages. |
| #10<br>Oct 28 & | Chapters 16-18 (Malik)<br>AAA<br>TACACS+<br>RADIUS | Special Project signup<br>**Lab 8: AAA**<br>http://cs3.calstatela.edu/~egean/cs5781/lab- |

| | | |
|---|---|---|
| Oct 30 | Chapter 9 (Counter Hack)<br>Denial-of-Service attacks<br>Chapter 11,12 (CEH)<br>Denial of Service<br>Session Hijacking | assignments/Cisco%20AAA%20Lab%20Assignment.pdf |
| #11<br>Nov 4<br>& 6 | Chapter 10 (Counter Hack)<br>Maintaining Access<br>Chapter 13,14 (CEH)<br>Web Servers and Applications<br>SQL Injection | **Lab 9: Exploit code generation using Metasploit**<br>http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/Metasploit%20Lab%20Assignment.pdf |
| #12<br>Nov 11<br>Holiday<br>Nov 13 | Chapter 11 (Counter Hack)<br>Covering Tracks and Hiding<br>Chapter 15,16 (CEH)<br>Hacking WiFi and Bluetooth<br>Mobile Device Security | |
| #13<br>Nov 18<br>& 20 | **Special Project Presentations** | **Special Project Presentations** |
| #14<br>Nov 25<br>& 27 | Fall Recess (no class) | |
| #15<br>Dec 2<br>& 4 | **Special Project Presentations** | **Special Project Presentations** |
| #16<br>Dec 11 | **Final Exam (Wed Dec 11, 2024) 5pm – 7pm via Canvas** | |
| | | |