CSUS, College of Engineering and Computer Science

Department of Computer Science
CSC 154 – Computer System Attacks and Countermeasures

Instructor: Jun Dai, Assistant Professor in Department of Computer Science

Office: RVR 5060

Phone: (916)-278-5163

Email: emails through Canvas (preferred) or jun.dai@csus.edu
(**Please include "CSC 154" at the beginning of the subject line**)

Office Hours: Tuesdays (1:45-3:15pm) and
Thursdays (1:45-3:15pm)

Homepage: http://athena.ecs.csus.edu/~daij/

Textbook: William Stallings, Lawrie Brown, Computer Security: Principles and Practice, 3/E (Book 1, optional)

McClure, Scambray & Kurtz, Hacking Exposed (Network Security Secrets & Solutions), Osborne McGraw Hill, 6th Edition, 2009 (Book 2, optional)

Wenliang Du, Computer Security: A Hands-on Approach, CreateSpace (Book 3, optional)

As a plus to the textbooks, course slides, notes, assignments and other artifacts will be available to you through Canvas. In addition, some classic and emerging research outcomes or industry reports will be introduced and assigned to you for reading, study and discussion.

Catalog Description:

Introduction to network and computer security with a focus on how intruders gain access to systems, how they escalate privileges, and what steps can be taken to secure a system against such attacks. Topics include: Perimeter defenses, intrusion detection systems, social engineering, distributed denial of service attacks, buffer overflows, race conditions, trojans, and viruses. Prerequisite: CSC 138 or CPE 138. Graded: Graded Student. Units: 3.00

Course Policies:

Tentative Grading Policy:

Labs	30%
Group Project	15%
Quiz-exams	25% (middle) + 30% (final)

Grading Breakdown (%):

A = 93-100
A- = 90-92
B+ = 87-89
B = 83-86
B- = 80-82
C+ = 77-79
C = 73-76
C- = 70-72
D+ = 67-69
D = 63-66
D- = 60-62
F = 59 or below

Students are required to keep backup (machine-readable) copies of all submitted work, and also to keep all returned (graded) work, until after final grades are posted.

All the assignments will be graded with 100 as highest. The final scores will then be the weighted score, and rounded up to match the above scale. Please note that final score is not negotiable. Also, the highest grade in the university system is A. You will need a passing grade for all course exams to pass the whole class.

For labs and projects, as long as your answer involves certain commands or operations in specific software, screenshots are also needed to demonstrate your result. All the activities are independent work unless specified otherwise, therefore expected to be completed independently rather than relying on others' help. Assistance from instructors are mainly to clarify common problems/mistakes/misconceptions, but not to provide direct solutions to assignments. Debugging and diagnosis are also part of the requirements for activities.

Please do not run experiments towards your working settings, including your working host and production network. Virtual environment is encouraged.

The lab report, project report and oral presentation are supposed to illustrate or explain **what you did** (commands or configurations) and **what you got** (screenshots and analysis). They will all be evaluated based on the following grading criteria.

Correctness	25%
Completeness	25%
Clearness	25%
Quality of English writing	25%

Individual Work

Most parts in this course should be accomplished **independently**!

For example, we will independently work on a series of labs during the whole semester. The lab environment and instructions will be introduced later by the instructor in specific documents, including guidelines and due dates (**Please make sure you get this important information in class or via Canvas**). All the students need to work on the labs one by one. At the same time, they need to maintain/organize a **lab report** to document their inputs (like screenshots of commands issued) and outputs (like screenshots of exploit success) during all the labs. **Please disconnect your computer from any network when you perform the labs**. The following gives a list of requirements **for each lab** included in the lab report:

Introduction to the tool/platform/software or the vulnerability (if any)
Screenshots of commands issued to navigate the tool going through the guideline or to exploit the vulnerability (if any)
Screenshots of tool outputs/exploit results
Any existing or possible solution to mitigate the vulnerability (if any)

Group Work

For group work, the whole class needs to be divided into several 4-person/5-person groups. So, please first introduce yourself to your potential partners and find each other. The grouping has to be done and all the groups need to let the instructor know their members before the end of the first week (Friday 11:59pm). The group members will share the same score for group work.

After the groups are formed, each group will be assigned to perform the following tasks:

- **Group Project**: Each group will be responsible for the investigation or exploration on **the task assigned by instructor via the "group project assignment"**. Each group has a whole semester to work on this. The groups are free to take any strategy and format to deal with the task, as long as it meets the instructor's expectation. That is, this group project is an **OPEN-mind** assignment. All you do in this project will all enable you towards credits!

  The deliverables need to include a **mid-term report** (due date: week 7's Friday 11:59pm), a **final manual** (due date: the last week's Friday 11:59pm) and a **presentation/demo** (due date: class presentation time).

Submission Rules:
Each submission needs to be in an **electronic version** (through Canvas only). Electronic version submitted in ways other than Canvas, such as by email, will NOT be graded and will get a **ZERO**. Double check the correctness and the format (**see below**) of files before your submission. Email attachments with a new version with an explanation such as "I forgot to include some parts in my submission, please do grading based on this attachment" or "please grade this attachment because I accidentally attached a wrong file format in my Canvas submission" will **NOT** be accepted.

The hard copy will be returned to you for feedback. Any file needs be named according to one of the following formats (depending on the submission type). **Please do NOT use txt format**. **PDF/Word** format is preferable. Please also write your class **section number** in document.

> CSC154_sec#_lab#_name,
> CSC154_sec#_project_mid-term_group#, CSC154_sec#_project_final_group#,
> CSC154_sec#_project_PPT_ group#.

For example, if group1 is submitting PPT for their group project, the file name of the submission should be CSC154_project_PPT_group1. **On the first page of each submitted document, please always list all the group members' names**. Only one copy of the documents is needed for each group, hence only one member of the group needs to submit the documents on behalf of the whole group. Please note: if the attachment is not according to proper format as stated above, it will not be accepted.

Due Date and Late Submission:
Please see above due dates specified in instruction documents at Canvas from the instructor.
The mid-term exam will be performed respectively at the second class of week 8.

Late submission will be penalized by the following rules:

- within 24 hours: **20% off** the assignment grade;
- within 24-48 hours: **50% off** the assignment grade;
- after 48 hours: **100% off** the assignment grade.

Laptop and Cell Phone Regulation:
Laptop and cell phone can be used if necessary, but NO game, NO noise and NOT in the quizs/exams! In any case, you are not allowed to disturb others in the classroom.

Legal Policy:
Every student agrees with the following "Legal Policy" by enrolling into this course.

> “Computer and Network Security course mission is to educate, introduce, and demonstrate hacking tools for penetration testing and education purposes only. I will not use the newly acquired skills for illegal or malicious attacks and I will not use such tools in an attempt to compromise any computer system, and to indemnify California State University, Sacramento and College of Engineering and Computer Science with respect to the use or misuse of these tools, regardless of intent.”

Other Course Policies:

- Information in this syllabus is subject to change with notice.
- Attendance to class and frequent check of email is expected. **Class roll will be checked randomly at least 10 times** after first week of classes. **If you miss more than 3 (i.e., >3) classes, you will be automatically excluded from the possible curving on the final scores.** You are responsible for materials presented and announcements made in class or by email. This could include changes to the syllabus, exam dates, etc.
- Make-up exams will only be given under extreme circumstances. The instructor reserves the right to reject make-up requests. There will be no make-up for unannounced quizzes (if any) under any circumstances.
- Be aware of the institution policy on drops and incomplete.

University or Department Policies:

Prerequisite Proof (if the course has specific prerequisites listed above):

The Department of Computer Science has a policy that each instructor needs to verify the student transcript and ascertain that the student has the prerequisites. You can log on to My Sac State go to “Student Center” and select “Unofficial Transcripts” to print. You also can select and print “Transfer Credit Report” if you have transferred from another institution. You must submit your transcript for verification. Any student who has completed one or more prerequisites at another school must provide similar verification to the instructor. Any student who has not submitted their transcript for verification by the end of the second week will be dropped from the class.

Repeat Policy:

The department has a policy specifying that students may not repeat a computer science course more than once. Any student who wishes to repeat a course more than once (that is, take a course for a third time) must submit a petition requesting the permission to do so. Student records will be reviewed to determine whether a student is taking this course for three or more times. Any such student must return an approved petition to the instructor within the first two weeks of class. Any student who does not submit an approved petition will be dropped from the class. Petitions are available in the department office (RVR 3018) and require the signature of both the instructor and the department chair.

Drop Policy

If you plan to drop this course, please make sure you understand the following information.

- **There is no such thing as an “automatic drop”.** The instructor can drop you from the course, but this does not happen automatically. If you plan to drop the course, make sure to use MySacState.
- After the 2nd week, you cannot drop the course through MySacState. At this point, you must provide written verification of a compelling reason. Both the instructor and the Department Chair must approve.

- After the 4th week, you must fill out a “Petition to Drop after Deadline” form and collect all the necessary signatures. This must be turned into Admission and Records in Lassen Hall.

Students with Disabilities

If you have a disability and require accommodations, you need to provide disability documentation to SSWD (Services to Students with Disabilities), Lassen Hall 1008, (916) 278-6955. Please discuss your accommodation needs with me after class or in lab early in the semester.

Ethics/Academic Honesty

Any work submitted is a contractual obligation that the work is the student’s and for which he/she could be quizzed in detail. Discussion among students in assignments and projects is part of the educational process and is encouraged. No discussion among students is allowed in any exams/quizzes. However, each student must make an effort to do his/her own work in all assignments and exams. No type of plagiarism will be tolerated (the corresponding assignment grade will immediately be ZERO). In that case each student should indicate the part of the work, which was their major responsibility in their final joint submission. Nevertheless, I emphasize any work submitted is a contractual obligation that the work is the student’s and for which he/she could be quizzed in detail. *The minimum* penalty for even a *single incident* of cheating brought to the attention of the instructor in this course is automatic failure of the course; additional more severe penalties may also be applied. Note that *cheating is grounds for dismissal from the University*.

Please refer to the Computer Science Dept. document entitled “Policy on Academic Integrity” (available online via the Computer Science department, www.ecs.csus.edu/csc home page) and to the University Policy Manual section on Academic Honesty (all available online via the instructor’s home page. Please visit http://www.csus.edu/admbus/umanual/UMA00150.htm) for additional information. IT IS THE RESPONSIBILITY OF EACH STUDENT TO BE FAMILIAR WITH, AND TO COMPLY WITH, THE POLICIES STATED IN THESE DOCUMENTS. *In addition, unless otherwise stated, the use of the following devices during exams/quizzes is prohibited: cell phones, pagers, laptops, and PDAs.*

CSC 154 - TENTATIVE SCHEDULE SUBJECT TO CHANGE

Week		**Topic**	**Reading Materials**
1	Introduction	introduction to network security (survey and the big pictures)	
2-3	Attacker’s Perspective	introduction to network attacks, network vulnerabilities and penetration (demo), security ethics	Book 1 Chapter 1 Book 2 Part 1, Part 2, Part 3.10
4-5		internet malware: worms, buffer overflow (demo)	Book 1 Chapter 6, 10 Book 2 Part 4.11
6-7	Defender’s Perspective	firewall: packet filtering, proxying, iptables (demo)	Book 1 Chapter 9 Book 2 Part 3.9
8		intrusion detection system (IDS), intrusion prevention system (IPS), honeypot, honeynet, honeyfarm	Book 1 Chapter 8, 9

9		authentication, Kerberos	Book 1 Chapter 23
10		network security protocols: VPN, IPSec, SSL, HTTPS, Tor and anonymity	Book 1 Chapter 22
11		access control: basics and models, setuid, chroot	Book 1 Chapter 4
12		security administration: security awareness, security configuration (system and network hardening), security management, security ethics	Book 1 Part 3
13		production network security: web, database (demo), email, mobile security (demo), setup and management	Book 1 Part 3 Book 2 Part 3.7, Part 4.12, 4.13
14		programming security: robust programming (example), cybersecurity first principles	Book 1 Chapter 1, 11
15	Group Project	group project presentations/demos	

IMPORTANT DATES:

Sep 2, 2019	Labor Day (Holiday, Campus Closed)
Nov 11, 2019	Veteran's Day (Holiday, Campus Closed)
Nov 28-29, 2019	Thanksgiving Holiday (Holiday, Campus Closed)
Dec 6, 2019	Last Day of Instruction
Dec 9-13, 2019	Finals Week
Final Exam	TBD by College Official Final Exam Schedules