USC Viterbi
School of Engineering

Running as TAC 499 for Fall 2025
Subject to Change – For Schedule of Classes

TAC 458: Defending and Investigating Compromised Networks

Units: 4
Fall 2025
Wednesday 5:00 – 8:20PM
Location: OHE 542

Instructor: Pierson Clair
Office: [TBD]
Office Hours: [TBD]
Contact Info: pclair@usc.edu

Learning Assistant: [TBD]
Contact Info: [TBD]

USC Digital Forensics Open Lab Hours: [TBD]

Catalogue Description

Build, secure, harden, compromise, and investigate enterprise network infrastructure; red, purple, blue team capabilities; gain access, follow, and eject the attackers.

Course Description

- This course is designed as an advanced course and the capstone combining network security architecture and incident response investigations. The course assumes that students have satisfied at least two of the following recommended prerequisites ITP/TAC 325 (Ethical Hacking), ITP/TAC 357 (Enterprise Networks), ITP/TAC 370 (Cybersecurity Management), ITP/TAC 375 (Digital Forensics), and/or have received instructor approval. Students will bring different skills, backgrounds, experiences, and capabilities to this course and work in groups to conduct lab assignments.
- The goal of the Cyber Security and Digital Forensics programs at USC is to develop the critical thinking, analytical reasoning, and technical writing skills that are necessary to effectively work in a junior level digital forensic or cyber security analyst role. This is accomplished through utilizing industry standard tools and techniques to conduct labs based upon real-world investigations.
- You'll apply knowledge you've learned in ITP/TAC 125 and other ITP/TAC classes to logically solve puzzles. You are expected to manage your time properly taking into account that assignments are staggered but may be due at the same time. This class contains broad instructions and is built to help you bridge from an academic setting to a business environment.
- Students will form groups based on experience to create the Information Technology and Information Security department for a fictional company. They will implement a wide range of security controls to harden their environment and leverage penetration testing capabilities to attempt to gain access into their infrastructure and environment. The course conclusion will include conducting a cyber risk assessment to identify known and acknowledged risks, identify further hardening steps, and develop a future security road map for the fictional company.

Learning Objectives

By the end of this course, students will be able to:

- Implement technical controls to thwart threat actor initial access intrusion methodologies.
- Implement secure network architecture and system hardening techniques.
- Author policies that demonstrate understanding of the relationship between Information Technology, Information Security, Incident Response, and Digital Forensics along with Governance, Risk, and Compliance.
- Implement industry standard best practices utilizing industry standard tools for hardening, validation, and incident response related to modern on-premise enterprise networks.
- Install, configure, compromise, and defend operating systems commonly found in on-premise enterprise infrastructure.
- Conduct cyber risk assessments to validate implementation of technical controls.
- Recommend security hardening configurations, methodologies, and approaches while understanding the various risks stemming from the balance of operational, compliance, and security requirements.

Prerequisite(s): ITP/TAC 125 and instructor approval (approval based upon completion of recommended preparation)

Recommended Preparation: Have successfully completed, at minimum, two of the following, or Instructor Approval:

- ITP/TAC 325 (Ethical Hacking)
- ITP/TAC 357 (Enterprise Networks)
- ITP/TAC 370 (Cybersecurity Management)
- ITP/TAC 375 (Digital Forensics)

Required Textbook

Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats (Donaldson, et al. 2015) [ISBN: 978-1430260820]

Course Notes

Course is letter graded, with materials available on Brightspace (Brightspace.usc.edu). Assignments will be submitted to the course Brightspace. Labs will be conducted in the security lab (OHE 542) during assigned class time, during open lab hours, or on your own time outside the classroom.

Technological Proficiency and Hardware/Software Required

Students will need a computer and access to the internet. Students will demonstrate advanced technical knowledge of computers and networks and research capabilities that have been refined in the preparatory classes.

Required Readings and Supplementary Materials

All course materials will be posted on Brightspace.

Description of Assignments and How They Will Be Assessed

The assignments will be a combination of in-class and out-of-class exercises. They will typically involve some form of procedural work, with some reflection on the work performed including researching processes and procedures performed. All exercises will be graded on a point scale. There will be a midterm project and a final project, as noted in the schedule and Grading breakdown

Assignment Submission Policy

The Assignments will be posted on Brightspace. Each Assignment will include instructions, a due date, and a link for electronic submission. Assignments must be submitted using this link. Do not email your assignments to the instructor, Learning Assistants, or graders. TurnItIn may be utilized for some assignments.

Unless otherwise noted, all Assignment assignments are due before the next class. The final project presentation will be during the USC Finals period on the day and time specified by the university.

Group Nature of this Course

Every student will be assigned to a group of three and no more than four students to form the Information Technology/Information Security ("IT/IS") Department for their fictional entity. These groups will start week three and will remain assigned for the remainder of the semester. All labs including hands-on configuring exercises starting week three will be conducted in your IT/IS dept group. The infrastructure policies (due as listed in the syllabus) and the final project (due on the day of the scheduled final exam) will be conducted in the same groups. Groups will be built from students with varying skills derived from the preparatory courses. It is expected that each group member will participate equally and assignments will take into account individual group member effort as reported by other group members with each submission.

Final Project

In the same group that has been your team all semester, starting at week eight conduct a Cyber Risk Assessment of the infrastructure that your team has built through lab exercises. You will map your infrastructure technical controls and policies to an appropriate and accepted cyber security risk management framework (example: NIST CSF) which will dictate the structure of your assessment. The risk assessment document should not exceed 20 pages and the presentation should be 20 minutes allowing 5-10 minutes for questions. On the day indicated in the USC Final Exam Schedule for our class, you will present the findings from your risk assessment in a mock Board of Directors presentation. Concurrently, you will submit your risk assessment and provide full network topology documentation. There will be status check-ins every other week in class. The grading will be half to the written report and half to the presentation. Grading criteria will be based upon technical accuracy, appropriate and reasonable controls, and generally accepted risks with suitable recommendations.

Grading Breakdown

Lab Assignments (14)	60%
Infrastructure Policies	10%
Final Project – Infrastructure Risk Assessment	20%
Weekly News Posting & Discussion	10%
Total	100%

Grading Policies

The lab assistants, graders, and instructors will do their best to return assignments graded to students within two weeks of submission. Certain assignments that are longer in length, including exams, case reports, and final projects, may require more time.

The grading breakdown is posted above. There is no curve, and grades are based on performance in the class. While we understand the importance of grades and maintaining a high GPA, we cannot hand out high marks without justified performance in the class. Do not rely upon an expectation of a guaranteed minimum final grade in this class regardless of its impact on your overall GPA, financial situation, familial situation, or the fate of the galaxy.

The instructor is the ultimate authority over any grade for any assignment, exam or class.

University policy states that no extra credit may be afforded to individual students without the same opportunity made available to everyone in the class. Should there be extra credit in the class, it will be made available to the entire class. Do not ask the instructor for additional extra credit.

Grades will be posted on Brightspace and it is your responsibility to ensure that the grades online are accurate and to follow your progress in the class.

Assignment Policies

The labs will be posted on Brightspace under the "Assignments" or "Labs" section. Each lab will include instructions, a due date, and a link for electronic submission. Labs must be submitted using this link. Do not email your assignments to the instructor, lab assistants, or graders. TurnItIn may be utilized for some assignments, and you must make sure that you have fully submitted the assignment (usually a two-step process).

Unless otherwise noted, all assignments are due at the beginning of class on the date noted in the syllabus, unless otherwise modified by Brightspace announcement and/or email from the instructor. Do not expect a timely response from the lab assistants, graders, or instructors if emailed after normal business hours particularly on the date the assignment is due.

If you join the class after the semester has started, you will have one week from the date of enrollment to complete all assignments due before you joined the class unless a written extension is granted from the instructor, typically via email.

It is your responsibility to submit your assignments on or before the due date and verify it has been successfully submitted. Assignments turned in up to 24 hours late will have 25% of the total points deducted from the graded score. Assignments turned in between 24 and 48 hours late will have 50% of the total points deducted from the graded score. After two days, submissions will not be accepted and you will receive no credit for the assignment.

The lab assistants and graders are not authorized to grant an extension on any assignment. Any extensions must be requested of the instructor in writing and confirmed in writing. If you ask for an extension on the day the assignment is due, without expressing an emergency such as being kidnapped and taken to Mexico, it will probably not be granted.

The instructor and lab assistants reserve the right to not answer certain questions about the lab assignments. This is normally due to the nature of the question being directly related to the learning objectives of the lab. You are encouraged to use online resources to further your understanding of the material to successfully answer questions related to the lab assignment (in other words, use your research skills).

Contacting the Instructor, Lab Assistants or Graders

When emailing the lab assistants, graders or instructor, please be sure to include your full name, student ID, class name and number, and class section (day and time) in the email.

Emails sent to the instructor, lab assistants, or graders will endeavor to be responded to within two business days. Do not email anyone with the expectation of an immediate response within the hour. Please do not complain when we have not responded to your email ten minutes before the assignment deadline.

Questions regarding individual clarification or regrade must be made through email to both the grader and the instructor. When requesting a regrade, the instructor has the prerogative to alter a grade higher or lower based upon a review of the entire assignment. Be absolutely certain before requesting a regrade of any assignment or exam – if you are going to roll the dice, be certain of your gamble.

The instructor will post their regular office hours on Brightspace. You may request a meeting with the instructor outside of normal office hours. Should you go to the instructor's office outside of normal office hours or outside of a scheduled meeting, do not expect the instructor to be able to meet with you.

Attendance Policy

You are expected to be in class, on time, and distraction free. As this class meets once a week and as it is lecture and lab any student who misses more than two classes is in danger of failing the course. Please see the instructor immediately if you have missed two or more class meetings.

This is a lab-based class. Certain class sections will be lecture, lab, or a combination of lecture and lab. Attendance is vital to success in the class, and punctuality is vital to success in your professional careers. The lab assistants will be

taking attendance for every class meeting. If you anticipate missing a class due to an event, please email the lab assistants and instructor prior to the start of class. If you are sick, we want you to get better and not infect your fellow classmates – please email the lab assistants and instructor. Should you miss a class with a lab assignment, contact the lab assistants to determine available times to come to the lab and finish your assignment.

If you are not in class, it is not the LA nor the instructor's responsibility to teach you the material that you missed. Attendance is mandatory for guest lectures. Guest lectures will be announced in class. The Professionalism/Participation grade is a combination grade based upon class participation, overall quality of work, and other factors that are important in the forensic investigation line of work.

Writing Skills

A significant portion of the cyber security and digital forensics curriculum involves communicating what was discovered by writing professional quality reports. These reports are held to standards that are expected by professionals in industry who are writing reports for clients, attorneys, judges and juries. It is expected that the reports will be written with correct spelling, grammar and language nuances of the American English language. A component of each report grade will be based on writing style, grammar and word choice. These reports must be accessible to technical and non-technical readers alike. Please take care to properly communicate your lab and assignment findings.

If you are not a native English speaker and writer, it is recommended that you visit the USC American Language Institute (http://ali.usc.edu/) for resources to assist you in this course and your professional careers. Writing assistance is also available from the Dornsife Writing Center (https://dornsife.usc.edu/writingcenter/). You do not need to be a Dornsife student to take advantage of the services from the Writing Center. Additional writing assistance is also available from the Viterbi Writing Center in the form of Writing Consultations (http://viterbi.usc.edu/students/undergrad/varc/writing-consultations.htm). In accordance with University standards, plagiarism of any type will not be tolerated.

Weekly News Assignment

To promote class discussion, each student will be required to submit an article for class discussion starting week two. Articles shall be posted with a hyperlink to the article and a one-paragraph summary to the Brightspace discussion page.

News stories should directly pertain to material covered in this class.

- Post a link to the proper week on the blog at least one hour before class.
- Please submit a story that is no more than one week old.
- Please take care not to duplicate stories that have been submitted that week.
- If the story is behind a pay-wall or subscription-wall or requires a login, please submit a PDF copy along with the link.
- Be prepared to give a short two-minute summary of the article and any surrounding background details to start the discussion.
- Press releases including anything from prweb.com are not valid news content
- Make sure you validate the veracity of your news story
- Each proper posting contributes to your news assignment & discussion grade
- If you are in need of news sources, please visit http://feedly.com/pclair

Academic Integrity

Unless otherwise noted, this course will follow the expectations for academic integrity as stated in the USC Student Handbook. The general USC guidelines on Academic Integrity and Course Content Distribution are provided in the subsequent "Statement on Academic Conduct and Support Systems" section.

For this class, you are expected to submit work that demonstrates, as assigned, your individual or group mastery of the course concepts. In-class presentations will require group work, and you will be expected to work cooperatively on your presentation delivery

If found responsible for an academic violation, students may be assigned university outcomes, such as suspension or expulsion from the university, and grade penalties, such as an "F" grade on the assignment, exam, and/or in the course.

Please ask the instructor if you are unsure about what constitutes unauthorized assistance on an exam or assignment, or what information requires citation and/or attribution.

Class Recordings and Course Content Distribution: You may not record this class without the express permission of the instructor and all other students in the class. Distribution of any notes, recordings, exams, or other materials from a university class or lectures — other than for individual or class group study — is prohibited without the express permission of the instructor; violations will be considered an intentional act to facilitate or enable academic dishonesty and reported to the university.

Policy on Generative AI

Since creating, analytical, and critical thinking skills are part of the learning outcomes of this course, all assignments should be prepared by the student working individually or as allowed by the instructor in groups. Students may not have another person or entity complete any substantive portion of the assignment. Developing strong competencies in these areas will prepare you for a competitive workplace. Therefore, using AI-generated tools is prohibited in this course, will be identified as plagiarism, and will be reported to the Office of Academic Integrity.

Generative AI including ChatGPT:

ChatGPT and similar programs and platforms represent great promise for the field of information technology, cybersecurity, and just about every other part of our world. Our policy on ChatGPT is as follows: you may use ChatGPT or similar programs for your assignments for this class, but treat them as a research *tool* and not a primary or secondary *source*. This means 1) cite your original source(s), and they can't be ChatGPT or similar tools directly, 2) treat everything those tools tell you to do or information they provide with a strong grain (pound?) of salt, and 3) *never* copy and paste or treat their output as a source or knowledgebase of ultimate authority. We want to emphasize the concept of using them as *tools* since they may guide you to the right answers; however, they can't and don't always do this correctly, and you may not know when they're telling the truth or making something up. If we suspect or determine that your assignments are being produced by AI-based tools or otherwise violate the guidelines above, your submissions will be treated as violations of the university's academic integrity policy and handled as such.

Course Evaluations

There will be a course evaluation that occurs at the end of the semester. It is an important review of your experience in the class, and will ensure that any concerns are noted, as well as knowing what you enjoyed about the class, into the overall improvement of the course.

Additional University policies follow the course schedule.

TAC 458 - Course Schedule

Subject to Change Throughout the Semester

Week	Topic	Reading (to be done in preparation for class the week posted)	Lab*
1	Introduction to Building Defensible Networks, Cyber Breach Response Tabletop	none	Breach Biography - Choose a major public breach, no duplicates, present next class based on public reporting: How and when did the Threat Actor (TA) get in? What did they do while they were in? Did they take anything? Were they ejected? Were any regulatory sanctions applied? What was the follow-on legal activity?
2	Learning from Breaches - What Went wrong? MITRE ATT&CK and Early Stages of the Cyber Kill Chain: How attackers gain access, initial infection vectors, lateral movement	Chapter 1 - Defining the Cyber Security Challenge Chapter 2 - Meeting the Cyber Security Challenge	Annual Data Breach Report Trends - in a group of 2 choose a major breach report (DBIR, Mandiant, Kroll, Crowdstrike, Baker Hostetler, MWE, IC3, etc) - review the last 3 years and report on trends, present next class
3	Inventory and Control of Enterprise Assets, Software Assets	Chapter 3 - Enterprise Cybersecurity Architecture	Create Fictional Company & Build Hypervisor/Virtualized Environment
4	Review of Enterprise Networks & Infrastructure, Protocols, Devices, Software, Functionality	Chapter 4 - Implementing Enterprise Cybersecurity Chapter 5 - Operating Enterprise Cybersecurity	Create Router/Firewall VM in Hypervisor, Connect to Internet
5	Continuous Vulnerability Management, Patch Management	Chapter 8 - Building an Effective Defense	Enable Remote Access including VPN and Wireguard/Tailscale
6	Enterprise Data Recovery, Backup, Archival, Retention, Enterprise Data Protection including Encryption at Scale	none	Create 2x Windows VMs and 1 Linux VM for each Group Member
7	Secure Configuration of Enterprise Assets and Software	none	Harden one Windows and 1 Linux with DISA STIG's

Week	Topic	Reading (to be done in preparation for class the week posted)	Lab*
8	Enterprise Account Management & Access Control Management	none	Build Active Directory (AD) Domain Controllers (DC), Create the AD Domain, join Computers to domain
	Infrastructure Policies: Build the Business Continuity/Disaster Recovery and Incident Response Plan for your environment (due Sunday 11:59pm on Brightspace Week 8)		
9	Enterprise Network Infrastructure Management	none	Implement STIG at DC level, Credential & Account Hardening
10	Enterprise Email and Web Browser Protections	Chapter 11 - Assessing Enterprise Cybersecurity	Build IIS Web Server & Build LAMP Stack for Wordpress website
11	Enterprise Malware Defenses	Chapter 12 - Measuring a Cybersecurity Program	Build e-mail server with SSO authentication
12	Enterprise Network Monitoring and Defense, Audit Log Management	Chapter 13 - Mapping Against Cyber Security Frameworks	Implement a SIEM & Log Aggregator, Vulnerability scan the environment
13	Managing & Identifying First Party & Third Party Risk in an Evolving Threat Landscape	Chapter 14 - Managing an Enterprise Cybersecurity Program	Segment the environment, Implement WAF
14	Enterprise Incident Response Management	Chapter 9 - Responding to Incidents Chapter 10 - Managing a Cybersecurity Crisis	Sensor the environment (EDR), monitor the environment
15	Enterprise Penetration Testing		Red Team the environment: Mimikatz, PowerShell Empire, attempt to gain Domain Administrator
Final	Submit final project risk assessment and provide full network documentation and present the findings	Refer to the final exam schedule in the USC *Schedule of Classes* at classes.usc.edu.	

* Labs starting week 3 will be conducted in your IT/IS dept group of 4. Labs will be assigned the week listed, due one week later before class

Academic Integrity

The University of Southern California is foremost a learning community committed to fostering successful scholars and researchers dedicated to the pursuit of knowledge and the transmission of ideas. Academic misconduct — which includes any act of dishonesty in the production or submission of academic work (either in draft or final form) — is in contrast to the university's mission to educate students through a broad array of academic, professional, and extracurricular programs.

This course will follow the expectations for academic integrity as stated in the USC Student Handbook. All students are expected to submit assignments that are their own original work and prepared specifically for this course and section in this academic term. You may not submit work written by others or "recycle" work prepared for other courses without obtaining written permission from the instructor(s). Students suspected of engaging in academic misconduct will be reported to the Office of Academic Integrity.

Other violations of academic misconduct include, but are not limited to, cheating, plagiarism, fabrication (e.g., falsifying data), knowingly assisting others in acts of academic dishonesty, and any act that gains or is intended to gain an unfair academic advantage.

Academic dishonesty has a far-reaching impact and is considered a serious offense against the university. Violations will result in a grade penalty, such as a failing grade on the assignment or in the course, and disciplinary action from the university itself, such as suspension or even expulsion.

For more information about academic integrity see the student handbook or the Office of Academic Integrity's website, and university policies on Research and Scholarship Misconduct.

Please ask your instructor if you are unsure what constitutes unauthorized assistance on an exam or assignment or what information requires citation and/or attribution.

Course Content Distribution and Synchronous Session Recordings Policies

USC has policies that prohibit recording and distribution of any synchronous and asynchronous course content outside of the learning environment.

Recording a university class without the express permission of the instructor and announcement to the class, or unless conducted pursuant to an Office of Student Accessibility Services (OSAS) accommodation. Recording can inhibit free discussion in the future, and thus infringe on the academic freedom of other students as well as the instructor. (Living our Unifying Values: The USC Student Handbook, page 13).

Distribution or use of notes, recordings, exams, or other intellectual property, based on university classes or lectures without the express permission of the instructor for purposes other than individual or group study. This includes but is not limited to providing materials for distribution by services publishing course materials. This restriction on unauthorized use also applies to all information, which had been distributed to students or in any way had been displayed for use in relation to the class, whether obtained in class, via email, on the internet, or via any other media. Distributing course material without the instructor's permission will be presumed to be an intentional act to facilitate or enable academic dishonestly and is strictly prohibited. (Living our Unifying Values: The USC Student Handbook, page 13).

Statement on University Academic and Support Systems

Students and Disability Accommodations:
USC welcomes students with disabilities into all of the University's educational programs. The Office of Student Accessibility Services (OSAS) is responsible for the determination of appropriate accommodations for students who encounter disability-related barriers. Once a student has completed the OSAS process (registration, initial appointment, and submitted documentation) and accommodations are determined to be reasonable and appropriate, a Letter of Accommodation (LOA) will be available to generate for each course. The LOA must be given to each course instructor by the student and followed up with a discussion. This should be done as early in the semester as possible as accommodations are not retroactive. More information can be found at osas.usc.edu. You may contact OSAS at (213) 740-0776 or via email at osasfrontdesk@usc.edu.

Student Financial Aid and Satisfactory Academic Progress:
To be eligible for certain kinds of financial aid, students are required to maintain Satisfactory Academic Progress (SAP) toward their degree objectives. Visit the Financial Aid Office webpage for undergraduate- and graduate-level SAP eligibility requirements and the appeals process.

Support Systems:
Counseling and Mental Health - (213) 740-9355 – 24/7 on call
Free and confidential mental health treatment for students, including short-term psychotherapy, group counseling, stress fitness workshops, and crisis intervention.

988 Suicide and Crisis Lifeline - 988 for both calls and text messages – 24/7 on call
The 988 Suicide and Crisis Lifeline (formerly known as the National Suicide Prevention Lifeline) provides free and confidential emotional support to people in suicidal crisis or emotional distress 24 hours a day, 7 days a week, across the United States. The Lifeline consists of a national network of over 200 local crisis centers, combining custom local care and resources with national standards and best practices. The new, shorter phone number makes it easier for people to remember and access mental health crisis services (though the previous 1 (800) 273-8255 number will continue to function indefinitely) and represents a continued commitment to those in crisis.

Relationship and Sexual Violence Prevention Services (RSVP) - (213) 740-9355(WELL) – 24/7 on call
Free and confidential therapy services, workshops, and training for situations related to gender- and power-based harm (including sexual assault, intimate partner violence, and stalking).

Office for Equity, Equal Opportunity, and Title IX (EEO-TIX) - (213) 740-5086
Information about how to get help or help someone affected by harassment or discrimination, rights of protected classes, reporting options, and additional resources for students, faculty, staff, visitors, and applicants.

Reporting Incidents of Bias or Harassment - (213) 740-2500
Avenue to report incidents of bias, hate crimes, and microaggressions to the Office for Equity, Equal Opportunity, and Title for appropriate investigation, supportive measures, and response.

The Office of Student Accessibility Services (OSAS) - (213) 740-0776
OSAS ensures equal access for students with disabilities through providing academic accommodations and auxiliary aids in accordance with federal laws and university policy.

USC Campus Support and Intervention - (213) 740-0411
Assists students and families in resolving complex personal, financial, and academic issues adversely affecting their success as a student.

Diversity, Equity and Inclusion - (213) 740-2101
Information on events, programs and training, the Provost's Diversity and Inclusion Council, Diversity Liaisons for each academic school, chronology, participation, and various resources for students.

USC Emergency - UPC: (213) 740-4321, HSC: (323) 442-1000 – 24/7 on call
Emergency assistance and avenue to report a crime. Latest updates regarding safety, including ways in which instruction will be continued if an officially declared emergency makes travel to campus infeasible.

USC Department of Public Safety - UPC: (213) 740-6000, HSC: (323) 442-1200 – 24/7 on call
Non-emergency assistance or information.

Office of the Ombuds - (213) 821-9556 (UPC) / (323-442-0382 (HSC)
A safe and confidential place to share your USC-related issues with a University Ombuds who will work with you to explore options or paths to manage your concern.

Occupational Therapy Faculty Practice - (323) 442-2850 or otfp@med.usc.edu
Confidential Lifestyle Redesign services for USC students to support health-promoting habits and routines that enhance quality of life and academic performance.