**University of Oklahoma**
**College of Engineering**

# Computer Science 5970-001: Cyber Attacks & Defenses

**Spring 2025**

| | |
|---|---|
| **Instructor:** | Anindya Maiti, am@ou.edu, DEH 210G |
| **Teaching Assistant** | Scott Seidenberger, seidenberger@ou.edu |
| **Office Hours:** | Thursdays 2:00-5:00PM<br>DEH 210G/245 |
| **Class Times:** | January 13 - May 2, 2025<br>TR 9 - 10:15 am |
| **Class Location:** | Carson Engr Ctr 0438 |
| **Credit Hours:** | 3.0 |
| **Course Prerequisite:** | CS3823 or CS4413; or permission of instructor. |

## Course Description

This course will provide hands-on training in the (ethical) use of the various software tools that are available in a hacker's arsenal to execute the different stages of an attack kill-chain which includes passive and active reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities (such as, maintaining persistent access and data exfiltration). This course will focus on open-source tools and libraries available on the popular Kali Linux platform for conducting information gathering and network discovery, vulnerability discovery and analysis, web application analysis, password cracking, wireless attacks, network sniffing and spoofing, software exploits and reverse engineering, social engineering, forensics and deploying backdoors/trapdoors.

## Measurable Student Learning Outcomes

After passing this course, students will be able to:

1. Evaluate and perform in-depth analysis of security vulnerabilities in deployed software systems, computing infrastructures, and networked environments.
2. Utilize advanced software tools and methodologies to detect, analyze, and exploit security vulnerabilities in operational software, computing systems, and network configurations.

## Suggested Textbooks

1. Mastering Kali Linux for Advanced Penetration Testing, Third Edition, Vijay Kumar Velu

and Robert Beggs, 2019, Packt Publishing Ltd. (ISBN: 978-1-78934-056-3).
2. The Hacker Playbook 3: Practical Guide to Penetration Testing, Red Team Edition, Peter Kim, 2018, Secure Planet LLC. (ISBN: 978-1-98090-175-4).

**Resources Provided by the Instructor**

As part of this course, each student will receive access to their own/individual Kali Linux Virtual Machine (or VM), hosted on the instructor's server, for the whole semester. This VM will run a recent version of Kali Linux OS, along with all the supporting libraries and tools required to complete the course labs and exercises, and will be accessible through any remote desktop application (e.g., *Remote Desktop Connection* app on Windows and macOS, and *rdesktop* on Linux). Students will have "root" or superuser access to their individual VMs to enable proper functioning of certain tools that require such access and to support potential environmental changes and/or software additions and modifications. Students are expressly forbidden to share their individual VM passwords with other students, and should change their initial passwords after first log in. In addition to a VM, all students will also have access to a common Cyber Range or virtual network hosting a set of vulnerable VMs. This Cyber Range, hosted on the instructor's server, will be the (only) target network for all the lab exercises and Capture-The-Flag (CTF) competitions in this course. In summary, students will not require anything, except a computer with a remote desktop application to participate in the course's lab exercises and competitions. If a student does not have continuous access to a computer with a remote desktop application, please contact the instructor as soon as possible. Students could choose to install and use a personal copy of Kali Linux on their own computers, however, no support will be provided by the instructor for such personal installations. All VMs, and the associated data, will be deleted at the end of the semester and there is no plan to maintain any backups. Students requiring access to their scripts/code after the course must make appropriate plans to back up their code before the end of the semester.

**Code-of-Conduct and Usage Rules**

Students should note that the instructor-provided Kali VM tools and resources should be only used to compromise and analyze the VMs on the instructor provided Cyber Range. Students are expressly forbidden to use the provided Kali VM to compromise/analyze any other system, server or network resource, including other OU or Computer Science (CS) systems and servers. Students should note that it is illegal and unlawful to search for vulnerable systems and servers on the Internet and attempt to try the exploits you learn in class on them. If students get involved in such activities, they should expect legal action against them. All activities/communications on, and originating from, the Kali Linux VMs and the Cyber Range are logged and will be shared with the appropriate authorities in case of misuse. Students are also expressly forbidden to use the provided Kali VM (or any other instructor provided resource) for their own profit, for example, by participating in authorized bug bounty programs of any nature. Please remember, if you ever feel like what you are doing is wrong, it probably is! Before indulging in any hacking/pen-testing activity which is beyond the scope of this course, please seek sound legal advice. By continuing to register and participate in this course, you are agreeing to abide by these

code-of-conduct rules and your agreement will be considered binding.

**Course Announcements and Updates**

All course related announcements and content will be posted on the course webpage on Canvas (http://canvas.ou.edu). *All course related assignment submissions should be done using the course's Canvas page only.* Course related grades will be posted only on Canvas. Students are expected to, and are responsible for, regularly monitoring the course page on Canvas. Students should also make sure that they receive emails and announcements sent by the instructor through Canvas. The instructor reserves the right to make reasonable changes in the syllabus as the course progresses. The latest syllabus will be posted on Canvas and students will be notified of any changes to syllabus through Canvas announcements and emails.

**Attendance and Participation**

This course will follow a face-to-face or in-person model of instruction. Attendance is not mandatory, however it is highly recommended for students to satisfactorily achieve their learning goals.

**Tentative Schedule***

| Week | Topics | Notes |
|---|---|---|
| 1 | Discussion of course syllabus, and introduction to Benevolent Hacking, Penetration Testing and the Attack Kill-Chain | |
| 2 | Getting familiar with the Kali Linux platform | Lab 1 |
| 3 | Open Source Intelligence (OS-INT) and Passive Reconnaissance | |
| 4 | Active Reconnaissance and Vulnerability Assessment | Lab 2 |
| 5 | Advanced Social Engineering | |
| 6 | Attacks on Wireless Access Points and Networks | Lab 3 |
| 7 | Web-based and Client-side Exploitations | |
| 8 | Web-based and Client-side Exploitations | Lab 4 |
| 9 | Bypassing Security Controls and Anti-Virus Software | |
| 10 | Metasploit Framework – Windows Exploits | Lab 5 |
| 11 | Metasploit Framework – Linux Exploits | |
| 12 | Post-exploitation Lateral Movement | Lab 6 |
| 13 | Vertical Movement and Privilege Escalation | |
| 14 | Backdoors and Persistence | Lab 7 |
| 15 | Future Topics, Security Certifications, and Capture-the-Flag (CTF) Preparation | |
| 16 | Capture-the-Flag (CTF) | In-Class |

*The schedule and due dates of the various assignments are tentative and subject to change. Please refer to the course page on Canvas for the most up-to-date information.

**In-class Security Labs**

The course consists of a total of 7 *in-class security lab assignments*. These labs will focus on the usage of software tools and libraries (available on Kali Linux) and some programming/coding tasks to conduct passive and active reconnaissance, vulnerability assessment, exploitation, and post-exploitation activities (such as, maintaining persistent access and data exfiltration) on the various VMs in the course's Cyber Range. By means of these labs, students will not only be exposed to the various tools on Kali (and how to use them to carry out system hacking and pen-testing tasks), but will also give them an insight on potential system weaknesses and how to protect against these threats. All lab assignments are expected to be completed individually and are due on Canvas by the deadline. **No late assignment submissions beyond the official deadline will be accepted (and graded) and will automatically receive zero points, unless there is a STRONG well-documented reason for missing multiple labs.** Some acceptable reasons include, but are not limited to, medical emergencies, emergency in family, jury duty, military service and religious event. Please inform the instructor of your emergency or reason of absence/failure-to-submit, along with the appropriate documentation, as early as possible. The instructor will make the final call on whether to grant the leave of absence and allow for the late submission. **Students must bring their laptop and charger to class for completing the in-class lab assignments.**

**Important Academic Dates**

For the Spring 2025 semester, classes begin on Jan 13, 2025. OU academic calendar for Spring 2025 semester can be found at: www.ou.edu/registrar/academic-records/academic-calendars/spring-2025.html

**Grading Policy**

Your letter grade will be based on the following components (Total out of 100%):
In-class Security Labs (after dropping lowest) – 70%
Capture-the-Flag (CTF) – 30%

Individual course assignments will be accompanied with a detailed grading guideline. The final letter grade for the course will be assigned based on the following distribution:

| Percentage obtained | Letter grade |
|---|---|
| >= 90 | A |
| >= 80 and < 90 | B |
| >= 70 and < 80 | C |
| >= 60 and < 70 | D |
| < 60 | F |

# University Policies

### Copyright Syllabus Statement for In-Person or Online Courses

Sessions of this course may be recorded or live-streamed. These recordings are the intellectual property of the individual faculty member and may not be shared or reproduced without the explicit, written consent of the faculty member. In addition, privacy rights of others such as students, guest lecturers, and providers of copyrighted material displayed in the recording may be of concern. Students may not share any course recordings with individuals not enrolled in the class or upload them to any other online environment.

### Mental Health Support Services

Support is available for any student experiencing mental health issues that are impacting their academic success. Students can either been seen at the University Counseling Center (UCC) located on the second floor of Goddard Health Center or receive 24/7/365 crisis support from a licensed mental health provider through TELUS Health. To schedule an appointment or receive more information about mental health resources at OU please call the UCC at 405-325-2911 or visit University Counseling Center. The UCC is located at 620 Elm Ave., Room 201, Norman, OK 73019.

### Title IX Resources and Reporting Requirement

The University of Oklahoma faculty are committed to creating a safe learning environment for all members of our community, free from gender and sex-based discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking, in accordance with Title IX. There are resources available to those impacted, including: speaking with someone confidentially about your options, medical attention, counseling, reporting, academic support, and safety plans. If you have (or someone you know has) experienced any form of sex or gender-based discrimination or violence and wish to speak with someone confidentially, please contact OU Advocates (available 24/7 at 405-615-0013) or University Counseling Center (M-F 8 a.m. to 5 p.m. at 405-325-2911).

Because the University of Oklahoma is committed to the safety of you and other students, and because of our Title IX obligations, I, as well as other faculty, Graduate Assistants, and Teaching Assistants, are mandatory reporters. This means that we are obligated to report gender-based violence that has been disclosed to us to the Institutional Equity Office. This means that we are obligated to report gender-based violence that has been disclosed to us to the Institutional Equity Office. This includes disclosures that occur in: class discussion, writing assignments, discussion boards, emails and during Student/Office Hours. You may also choose to report directly to the Institutional Equity Office. After a report is filed, the Title IX Coordinator will reach out to provide resources, support, and information and the reported information will remain private. For more information regarding the University's Title IX Grievance procedures, reporting, or support measures, please visit Institutional Equity Office at 405-325-3546.

## Reasonable Accommodation Policy

The University of Oklahoma (OU) is committed to the goal of achieving equal educational opportunity and full educational participation for students with disabilities. If you have already established reasonable accommodations with the Accessibility and Disability Resource Center (ADRC), please submit your semester accommodation request through the ADRC as soon as possible and contact me privately, so that we have adequate time to arrange your approved academic accommodations.

If you have not yet established services through ADRC, but have a documented disability and require accommodations, please complete ADRC's pre-registration form to begin the registration process. ADRC facilitates the interactive process that establishes reasonable accommodations for students at OU. For more information on ADRC registration procedures, please review their Register with the ADRC web page. You may also contact them at (405)325-3852 or adrc@ou.edu, or visit www.ou.edu/adrc for more information.

Note: disabilities may include, but are not limited to, mental health, chronic health, physical, vision, hearing, learning and attention disabilities, pregnancy-related. ADRC can also support students experiencing temporary medical conditions.

## Religious Observance

It is the policy of the University to excuse the absences of students that result from religious observances and to reschedule examinations and additional required classwork that may fall on religious holidays, without penalty. [See Faculty Handbook 3.15.2]

## Adjustments for Pregnancy/Childbirth Related Issues

Should you need modifications or adjustments to your course requirements because of documented pregnancy-related or childbirth-related issues, please contact the Accessibility and Disability Resource Center at 405/325-3852 and/or the Institutional Equity Office at 405/325-3546 as soon as possible. Also, see the Institutional Equity Office FAQ on Pregnant and Parenting Students' Rights for answers to commonly asked questions.

## Final Exam Preparation Period

Pre-finals week will be defined as the seven calendar days before the first day of finals. Faculty may cover new course material throughout this week. For specific provisions of the policy please refer to OU's Final Exam Preparation Period policy.

## Emergency Protocol

During an emergency, there are official university procedures that will maximize your safety.

**Severe Weather:** If you receive an OU Alert to seek refuge or hear a tornado siren that signals severe weather.

1. Look for severe weather refuge location maps located inside most OU buildings near the entrances.

2. Seek refuge inside a building. Do not leave one building to seek shelter in another building that you deem safer. If outside, get into the nearest building.
3. Go to the building's severe weather refuge location. If you do not know where that is, go to the lowest level possible and seek refuge in an innermost room. Avoid outside doors and windows.
4. Get in, Get Down, Cover Up
5. Wait for official notice to resume normal activities.

Additional Weather Safety Information is available through the Department of Campus Safety.

**The University of Oklahoma Active Threat Guidance**

The University of Oklahoma embraces a Run, Hide, Fight strategy for active threats on campus. This strategy is well known, widely accepted, and proven to save lives. To receive emergency campus alerts, be sure to update your contact information and preferences in the account settings section at one.ou.edu.

**RUN**: Running away from the threat is usually the best option. If it is safe to run, run as far away from the threat as possible. Call 911 when you are in a safe location and let them know from which OU campus you're calling from and location of active threat.

**HIDE:** If running is not practical, the next best option is to hide. Lock and barricade all doors; turn of all lights; turn down your phone's volume; search for improvised weapons; hide behind solid objects and walls; and hide yourself completely and stay quiet. Remain in place until law enforcement arrives. Be patient and remain hidden.

**FIGHT:** If you are unable to run or hide, the last best option is to fight. Have one or more improvised weapons with you and be prepared to attack. Attack them when they are least expecting it and hit them where it hurts most: the face (specifically eyes, nose, and ears), the throat, the diaphragm (solar plexus), and the groin.

Please save OUPD's contact information in your phone.

**NORMAN** campus: For non-emergencies call (405) 325-1717. For emergencies call (405) 325-1911 or dial 911.

**TULSA** campus: For non-emergencies call (918) 660-3900. For emergencies call (918) 660-3333 or dial 911.

**Fire Alarm/General Emergency**

If you receive an OU Alert that there is danger inside or near the building, or the fire alarm inside the building activates:

1. LEAVE the building. Do not use the elevators.
2. KNOW at least two building exits
3. ASSIST those that may need help
4. PROCEED to the emergency assembly area

5. ONCE safely outside, NOTIFY first responders of anyone that may still be inside building due to mobility issues.
6. WAIT for official notice before attempting to re-enter the building.

OU Fire Safety on Campus