EAST TEXAS A&M
UNIVERSITY

CSCI 421.61E
Intrusion Detection and Prevention

COURSE SYLLABUS: Spring 2026

INSTRUCTOR INFORMATION

Instructor: Amy Hays M.S., Computer Science
Office Location: RELLIS ACB2 210
https://tamuc.zoom.us/j/92711096337?pwd=cS9UZllXb2xIc2V1dGtoNnArcDZ5UT09
Office Hours: Tuesdays and Thursdays, 12 to 2:30 PM
Other times by appointment only via email
University Email Address: amy.hays@etamu.edu
Preferred Form of Communication: For all emails, make sure the email the subject line reads: “CSCI 421.61E~~”.
Communication Response Time: 48 hours

COURSE INFORMATION

Lecture: Meets 1/12/2026 through 5/5/2025, Finals week (4/30 – 5/5)
Tuesdays and Thursdays, 2:50 p.m. - 4:05 p.m.
Campus: RELLIS Campus Building: ACB2 Room: 217

Class Textbook:

- (Required) Black Hat Bash, Nick Aleks & Dolev Farhi, No Starch Press, 2024, https://learning.oreilly.com/library/view/black-hat-bash/9781098182434/
- (Required) Cybersecurity Ops with bash, Paul Troncone & Carl Albing, O'Reilly Media, Inc., 2019, https://learning.oreilly.com/library/view/cybersecurity-ops-with/9781492041306/
- (Required) Practical Packet Analysis, 3rd Edition, Chris Sanders, No Starch Press, 2017, https://learning.oreilly.com/library/view/practical-packet-analysis/9781492020356/

The *syllabus/schedule are subject to change.*

Recommended Textbook(s), References, & Resources:

- Acing the CCNA Exam, Volume 1 Fundamentals and Protocols and Acing the CCNA Exam, Volume 2 Advanced Networking and Security, Jeremy McDowell, 2024. https://learning.oreilly.com/library/view/-/9781633437678/ and https://learning.oreilly.com/library/view/-/9781633435780/
- Computer Networking: A Top-Down Approach, 8th edition, James Kurose and Keith Ross, ISBN: 9780136681557 or eBook ISBN: 9780135928615, Pearson, 2021.
- An Introduction to Computer Networks. https://open.umn.edu/opentextbooks/textbooks/353
- Cisco network academy: https://www.netacad.com/

The professor will make other supplementary information for the course available online. These include class notes, assignments, PowerPoint slides, class announcements, the course syllabus, test dates, etc. The professor will announce in class when such information becomes available electronically. It is the student's responsibility to follow these announcements.

Course Description

This course provides a look at intrusion detection, methodologies, and tools, and the approaches to handling intrusions when they occur; includes a study of proper computer and network protection procedures to assist in the identification in tracking of intruders.

Student Learning Outcomes

Upon completion of this course, students will be able to:

- Apply a scientific methodology to analyze anomalies, correlate evidence from disparate sources, and identify intruder activity.
- Differentiate between intrusion detection methodologies (signature, anomaly, heuristic) and system architectures (NIDS, HIDS, EDR).
- Analyze network packet captures to identify reconnaissance, exploitation, and post-exploitation traffic using network analysis tools.
- Employ NIDS and HIDS to detect, analyze, and mitigate network and host-based threats.
- Evaluate the trade-offs between detection accuracy, false positives, and system performance when tuning security tools.
- Explain common network and host-based IDS evasion techniques and their corresponding countermeasures.
- Describe the phases of the Incident Response lifecycle and the role of IDS/IPS within it.
- Evaluate the role of AI/ML in modern intrusion detection, contrasting its anomaly-based approach with traditional signatures for detecting novel threats.

COURSE REQUIREMENTS

Minimal Technical Skills Needed

Prerequisites: CSCI 310 (Min Grade C) and CSCI 430 (Min Grade C) and CSCI 434 (Min Grade C)

Instructional Methods

During this course, we will using traditional and active learning methods, and work together using:
• In-class lectures: using slides, supplementary materials, and hands-on exercises. The syllabus/schedule are subject to change.
• Assignments and labs that will be released via the D2L Learning Management Systems (LMS).
• Individual / group projects.

Student Responsibilities or Tips for Success in the Course

It is the students' responsibility to keep up with the schedule. Makeup work (exams, quizzes, discussions, or assignments) will only be permitted in cases of emergency with proper documentation, or prior rescheduling. To reschedule contact me before the due date with a valid reason and suggested make-up dates will be given.

Please feel free to contact me and come to office hours to ask questions and get clarifications or assistance.

GRADING

Final grades in this course will be based on the following scale:

A = 90%-100%
B = 80%-89%
C = 70%-79%
D = 60%-69%
F = 59% or Below

Assessments

Basis for Evaluation:

Assignments & labs	20%
Attendance & Participation	10%
Quizzes	20%

The *syllabus/schedule are subject to change.*

Midterms	25%
Final Exam	25%

TECHNOLOGY REQUIREMENTS

LMS

All course sections offered by East Texas A&M University have a corresponding course shell in the myLeo Online Learning Management System (LMS). Below are technical requirements

LMS Requirements:
https://community.brightspace.com/s/article/Brightspace-Platform-Requirements

LMS Browser Support:
https://documentation.brightspace.com/EN/brightspace/requirements/all/browser_support.htm

Zoom Video Conferencing Tool
https://inside.tamuc.edu/campuslife/CampusServices/CITESupportCenter/Zoom_Account.aspx?source=universalmenu

ACCESS AND NAVIGATION

You will need your campus-wide ID (CWID) and password to log into the course. If you do not know your CWID or have forgotten your password, contact the Center for IT Excellence (CITE) at 903.468.6000 or helpdesk@tamuc.edu**.**

Note: Personal computer and internet connection problems do not excuse the requirement to complete all course work in a timely and satisfactory manner. Each student needs to have a backup method to deal with these inevitable problems. These methods might include the availability of a backup PC at home or work, the temporary use of a computer at a friend's home, the local library, office service companies, Starbucks, a ETAMU campus open computer lab, etc.

COMMUNICATION AND SUPPORT

If you have any questions or are having difficulties with the course material, please contact your Instructor.

Technical Support

If you are having technical difficulty with any part of Brightspace, please contact Brightspace Technical Support at 1-877-325-7778. Other support options can be found here:

https://community.brightspace.com/support/s/contactsupport

COURSE AND UNIVERSITY PROCEDURES/POLICIES

Course Specific Procedures/Policies

Late Policies

Credit will be given for ONLY those exams, quizzes, and assignments turned in no later than the deadline as announced by the instructor of this class unless prior arrangement has been made with the instructor.

Late assignments can gain partial credit upon the following policy. As per University requirements, assignments submitted within 7 days after the deadline can receive up to 20% deduction, assignments submitted between 8-14 days after the deadline can receive up to 50% deduction.

- **No assignments will be accepted two weeks after the assigned due date.**
- **No assignment will be accepted after the term end day.**
- Exceptions to this policy will only be made in extraordinary circumstances. Please let me know your circumstances.

Syllabus Change Policy

The syllabus is a guide. Circumstances and events, such as student progress, may make it necessary for the instructor to modify the syllabus during the semester. Any changes made to the syllabus will be announced in advance.

University Specific Procedures

Student Conduct

All students enrolled at the University shall follow the tenets of common decency and acceptable behavior conducive to a positive learning environment. The Code of Student Conduct is described in detail in the Student Guidebook.
http://www.tamuc.edu/Admissions/oneStopShop/undergraduateAdmissions/studentGuidebook.aspx

Students should also consult the Rules of Netiquette for more information regarding how to interact with students in an online forum:
https://www.britannica.com/topic/netiquette

ETAMU Attendance

For more information about the attendance policy please visit the Attendance webpage and Procedure 13.99.99.R0.01.
http://www.tamuc.edu/admissions/registrar/generalInformation/attendance.aspx

The *syllabus/schedule are subject to change.*

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/academic/13.99.99.R0.01.pdf

Academic Integrity

Students at East Texas A&M University are expected to maintain high standards of integrity and honesty in all of their scholastic work. For more details and the definition of academic dishonesty see the following procedures:

Undergraduate Academic Dishonesty 13.99.99.R0.03
Undergraduate Student Academic Dishonesty Form

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/documents/13.99.99.R0.03UndergraduateStudentAcademicDishonestyForm.pdf

Graduate Student Academic Dishonesty Form

http://www.tamuc.edu/academics/graduateschool/faculty/GraduateStudentAcademicDishonestyFormold.pdf

http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/13students/undergraduates/13.99.99.R0.03UndergraduateAcademicDishonesty.pdf

Students with Disabilities-- ADA Statement

The Americans with Disabilities Act (ADA) is a federal anti-discrimination statute that provides comprehensive civil rights protection for persons with disabilities. Among other things, this legislation requires that all students with disabilities be guaranteed a learning environment that provides for reasonable accommodation of their disabilities. If you have a disability requiring an accommodation, please contact:

Office of Student Disability Resources and Services
East Texas A&M University
Velma K. Waters Library Rm 162
Phone (903) 886-5150 or (903) 886-5835
Fax (903) 468-8148
Email: studentdisabilityservices@tamuc.edu
Website: Office of Student Disability Resources and Services
http://www.tamuc.edu/campusLife/campusServices/studentDisabilityResourcesAndServices/

Nondiscrimination Notice

East Texas A&M University will comply in the classroom, and in online courses, with all federal and state laws prohibiting discrimination and related retaliation on the basis of race, color, religion, sex, national origin, disability, age, genetic information or veteran status. Further, an environment free from discrimination on the basis of sexual orientation, gender identity, or gender expression will be maintained.

Campus Concealed Carry Statement

Texas Senate Bill - 11 (Government Code 411.2031, et al.) authorizes the carrying of a concealed handgun in East Texas A&M University buildings only by persons who have been issued and are in possession of a Texas License to Carry a Handgun. Qualified law enforcement officers or those who are otherwise authorized to carry a concealed handgun in the State of Texas are also permitted to do so. Pursuant to Penal Code (PC) 46.035 and East Texas A&M Rule 34.06.02.R1, license holders may not carry a concealed handgun in restricted locations.

For a list of locations, please refer to the Carrying Concealed Handguns On Campus document and/or consult your event organizer.

Web url:
http://www.tamuc.edu/aboutUs/policiesProceduresStandardsStatements/rulesProcedures/34SafetyOfEmployeesAndStudents/34.06.02.R1.pdf

Pursuant to PC 46.035, the open carrying of handguns is prohibited on all East Texas A&M campuses. Report violations to the University Police Department at 903-886-5868 or 9-1-1.

East Texas A&M Supports Students' Mental Health

The Counseling Center at East Texas A&M, located in the Halladay Building, Room 203, offers counseling services, educational programming, and connection to community resources for students. Students have 24/7 access to the Counseling Center's crisis assessment services by calling 903-886-5145. For more information regarding Counseling Center events and confidential services, please visit www.tamuc.edu/counsel

AI use policy [Draft 2, May 25, 2023]

East Texas A&M University acknowledges that there are legitimate uses of Artificial Intelligence, ChatBots, or other software that has the capacity to generate text, or suggest replacements for text beyond individual words, as determined by the instructor of the course.

Any use of such software must be documented. Any undocumented use of such software constitutes an instance of academic dishonesty (plagiarism).

The *syllabus/schedule are subject to change.*

Individual instructors may disallow entirely the use of such software for individual assignments or for the entire course. Students should be aware of such requirements and follow their instructors ’guidelines. If no instructions are provided the student should assume that the use of such software is disallowed.

In any case, students are fully responsible for the content of any assignment they submit, regardless of whether they used an AI, in any way. This specifically includes cases in which the AI plagiarized another text or misrepresented sources.

13.99.99.R0.03 Undergraduate Academic Dishonesty

13.99.99.R0.10 Graduate Student Academic Dishonesty

COURSE OUTLINE / CALENDAR

Textbook Key:
(PPA) Practical Packet Analysis
(BHB) Black Hat Bash
(CSOB) Cybersecurity Ops with Bash

WEEK OF	CONTENT	Readings
Jan 12	Course Introduction - The Cuckoo's Egg	
Jan 19	Shebang #! – bash	BHB – Ch 1 - 2 CSOB – Ch 1- 2 **1/19 – MLK Day**
Jan 26	grep, awk, & sed	BHB – Ch 2 CSOB – Ch 3
Feb 2	Packet analysis	PPA – Ch 1-2 Wireshark.org
Feb 9	IDS Models	Handout - McGraw
Feb 16	Network (NIDS)	Handout - McGraw
Feb 23	Host-based intrusion detection (HIDS)	Handout - McGraw
Mar 2	Advanced Detection	BHB Ch. 6 & 7; PPA Ch. 9 & 12 **Midterm**
Mar 9	**Spring Break**	
Mar 16	Detecting post-exploitation	BHB Ch. 8, 9, 10.
Mar 23	Intrusion Prevention System (IPS) & deception	CSOB Ch 9, 14

Mar 30	IDS Evasion & Countermeasures	BHB Ch. 12;
		CSOB Ch. 14;
		PPA Ch. 12.
		4/3 – Reading Day

Apr 6	Incident response (IR) fundamentals	TBD
Apr 13	Digital forensics in IR	TBD
Apr 20	Advanced Threats and Operations	Instructor-provided papers; NIST SP 800-61
Apr 27	Modern challenges & the future of detection	**4/28 – Last Day of Class**
Apr 30 – May 5	Final Exam **Due 5/4 at 11:59 pm**	

Note: The right to modify the presentation order of materials is reserved. Course progress will be based on feedback and suggestions from students. We would cover the course materials, so if we slow in some topics, we must accelerate elsewhere.

HAVE A HAPPY AND SUCCESSFUL SESSION

The *syllabus/schedule are subject to change.*