ECE529 - Introduction to Technical Cybersecurity

Instructor: Dr. Chris Lamb
Email: cclamb@unm.edu
Location: UNM Learn
Department Info: ECE Building Room 125, (505) 277-2436

Credits: 3
Time: Self-paced

Course Description

This course will cover introductory material around technical cybersecurity. Along these lines, we will cover host based attacks (stack exploitation, disassembly and analysis) and defenses, host and network based attacks, and web application vulnerabilities and scanning. This will be a fast moving course in which we introduce students to these topics to prime them for further, more in-depth later study. Most of the tools we use will be free, though some will require student expenditure. The focus will be on application exploitation and defense; we will not explore kernel analysis in the scope of this course in any detail, though the skills learned in this course will provide a strong foundation for kernel analysis as well.

Course Goals

This course is intended to be the first of a future series of technical cybersecurity courses that address both defensive and offensive cybersecurity, analysis, and development. It will focus on embedded devices and the Internet of Things. This course will provide students with a unique perspective on how to protect systems via an in-depth understanding of how attacks work, how malicious engineers analyze programs in order to develop attacks, how technical defenses against attacks work, and how attackers try to prevent program analysis via countermeasure development.

Course Objectives / Learning Outcomes

All the below objectives apply to host- and network-based analysis and exploitation:

1. *Explain the history of cybersecurity and hacking*
2. *Identify the key events socially and technically that lead us to where we are today*
3. *Explain the different types of cyber campaigns*
4. *Be able to defensively and offensively analyze a system*
5. *Be able to design and execute and defend against a malware campaign against a target*

Textbooks / Supplies

We will not use a dedicated text, but will rather refer to case studies, white papers, and a variety of publications. You will need to be able to find additional references on your own as needed (e.g. programming texts, technical standards, and so on). An O'Reilly Safari account (or similar) would certainly help with ongoing references as we will be addressing material from a range of texts.

Course Requirements

We will have lectures covering the technical topics as well as quizzes and programming assignments. This will give you exposure to cyber-security technologies and concepts. We will make heavy use of virtualization, so students will need a high-powered computer system and virtualization software (VMWare Workstation or Fusion, or VirtualBox).

Expectations for Participation

The course will require on the order of 10 hours per week, give or take 5 hours depending on the module. Students will need to know or learn how to navigate UNM learn as well. We expect you'll keep us informed of any problems you might experience, address technical problems immediately, and observe appropriate netiquette at all times. Student-to-student and student-to-instructor interaction will be via learn using the discussion feature, primarily. We also have web conference rooms set up for ad-hoc meetings or discussions at any time for class participants. I expect each of you to actively be engaged in discussions, and to reply to questions from me or other students. I will be posting question threads in the discussion groups that I would like you to think about and respond to. When you respond, reply to either my question or a reply from another student. I expect you to answer post at least twice, once to me, and once to another student. I encourage you to work together on assignments as well, but ensure that you turn in your own work. Sharing ideas and solutions to individual problems is fine! Sharing your program or report for an assignment is not.

Grading

Grades will be based on exams, quizzes, homeworks and project work based on the following scale:

A+	(97-100)
A	(93-96)
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	(0-59)

The course will have an assignment at the end of each module except for module 8

All written reports should be submitted as a PDF via learn following the specific formatting guidelines. Homework assignments will also be submitted via learn, usually as a single archive file. We will grade assignments within a week of submission. We will provide feedback via course messages in learn.

Late Work

I'll accept late work, and will give you opportunities to submit graded assignments for higher grades. Please submit your initial attempt by the indicated times, in working condition. All the work in this class is cumulative; if you fall behind, it will be very hard for you to catch up, so ensure you keep up.

Accommodation Statement
Accessibility Services (Mesa Vista Hall 2021, 277-3506) provides academic support to students who have disabilities. If you think you need alternative accessible formats for undertaking and completing coursework, you should contact this service right away to assure your needs are met in a timely manner. If you need local assistance in contacting Accessibility Services, see the Bachelor and Graduate Programs office.

Schedule of Activities
This is an eight week course.

Week 1: Cybersecurity: A History
Week 2: Architecture & Analysis
Week 3: Reconnaissance & Vulnerability Identification
Week 4: Penetration & Delivery
Week 5: Binary Analysis
Week 6: Attacking the Stack
Week 7: Ret2libc & ROP
Week 8: Lab Week

Technical Skills
We will be using Linux and virualization extensively. Students are expected to be familiar with Linux, be familiar with C programming and make, and understand essentially how computers work.

Technical Requirements
You'll need a relatively powerful computer for this course and virtualization software (like Virtualbox or VMWare). That computer will either need to run Linux or be able to run a Linux virtual machine. You'll need access to a high speed internet connection to watch videos as well. You'll need to be able to run Firefox, and you may be required to install Java or Flash plugins.

For UNM Learn Technical Support call (505) 277-0857 or use the *Create a Support Ticket* link in Learn.

Web Conferencing/Discussions
We may use web conferencing/Discussions at times in the course. If we do, you'll need video and audio capabilities, including a microphone. A USB headset with these capabilities may be helpful, as well as access to high-speed internet. For Web Conference technical help call (505) 277-0857.

Tracking Course Activity
UNM Learn automatically records all students' activities including your first and last access to the course, the pages you have accessed, the number of discussion messages you have read and sent, web conferencing, discussion text, and posted discussion topics. This data can be accessed by the instructor to evaluate class participation and to identify students having difficulty.

Instructor Response Time
I usually check our email daily, so my response time (unless otherwise noted) can be measured in hours in most cases. If you don't hear back from me, please resend your message, I may have misplaced it (especially given the volume of email I receive). As a rule of thumb, you should expect a response at most within 48 hours, or the following Monday if over a weekend; generally, you'll hear back much more quickly.

I travel extensively, but I do respond to emails when on travel, and will inform you of any interruptions you might expect (e.g. when in transit, or in countries with poor internet access).

Procedures for Completing Coursework
It's important that you turn in work on time so I can assess the work and give you feedback. I will provide private feedback via email or learn messaging after assignments or quizzes. That said, I understand that life happens and I will be as flexible as I can when it does. When things do come up, please let me know as soon as possible. Quizzes are all online, and you will submit homework assignments online as well.

Assignments
Assignments for the course include C programs and exploits and analysis reports. Specific details are included within the course material and within Learn.

Netiquette

In following with the UNM Student Handbook, all students will show respect to their fellow students and instructor when interacting in this course. Take Netiquette suggestions seriously. Flaming is considered a serious violation and will be dealt with promptly. Postings that do not reflect respect will be taken down immediately.

http://online.unm.edu/help/learn/students/pdf/discussion-netiquette.pdf

UNM Policies

Title IX: Gender Discrimination. In an effort to meet obligations under Title IX, UNM faculty, Teaching Assistants, and Graduate Assistants are considered "responsible employees" by the Department of Education (see pg. 15 http://www2.ed.gov/about/offices/list/ocr/docs/qa-201404-title-ix.pdf). This designation requires that any report of gender discrimination which includes sexual harassment, sexual misconduct

and sexual violence made to a faculty member, TA, or GA must be reported to the Title IX Coordinator at the Office of Equal Opportunity (oeo.unm.edu).

For more information on the campus policy regarding sexual misconduct, see: https://policy.unm.edu/university-policies/2000/2740.html

Copyright Issues
All materials in this course fall under copyright laws and should not be downloaded, distributed, or used by students for any purpose outside this course.

Accessibility
The American 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 accommodations of their disabilities. If you have a disability requiring accommodation, please contact the UNM Accessibility Resource Center in 2021 Mesa Vista Hall at 277-3506 or http://arc.unm.edu/ . Information about your disability is confidential.

Blackboard's Accessibility statement: http://www.blackboard.com/accessibility.aspx

Academic Misconduct
You should be familiar with UNM's Policy on Academic Dishonesty and the Student Code of Conduct which outline academic misconduct defined as plagiarism, cheating, fabrication, or facilitating any such act.

Drop Policy:
This course falls under all UNM policies for last day to drop courses, etc. Please see http://www.unm.edu/studentinfo.html or the UNM Course Catalog for information on UNM services and policies. Please see the UNM academic calendar for course dates, the last day to drop courses without penalty, and for financial disenrollment dates.

UNM Resources
CAPS Tutoring Services: http://caps.unm.edu/programs/online-tutoring/

CAPS is a free-of-charge educational assistance program available to UNM students enrolled in classes. Online services include the Online Writing Lab, Chatting with or asking a question of a Tutor.

UNM Libraries: http://library.unm.edu

Student Health & Counseling (SHAC) Online Services:

http://online.unm.edu/help/learn/support/shac