ECE595 - Advanced Technical Cybersecurity

Instructor:	Dr. Chris Lamb		
Email:	cclamb@unm.edu	**Credits:**	3
Location:	UNM Learn	**Time:**	Self-paced
Department Info:	ECE Building Room 125, (505) 277-2436		
Alternate Contact:	Erika Elwell, (505) 277-1434		

Course Description

This course will cover modern material around technical cybersecurity. Along these lines, we will cover host based attacks (stack exploitation, disassembly and analysis) and defenses, malware techniques and defenses, encryption, and modern binary attacks and defenses. This will be a fast moving course. 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 second of a series of technical cybersecurity courses that address both defensive and offensive cybersecurity, analysis, and development. 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

C.1. Build selected malware functions

C.2. Build advanced binary exploits

C.3. Analyze a system

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 and associated 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). VMWare Workstation can be purchased at

VMWare’s site (http://www.vmware.com). Linux images can be downloaded from Ubuntu (http://www.ubuntu.com). Windows licenses and images are available via the ECE department Azure partnership. Some of the videos require a larger display to accommodate the tools used.

Expectations for Participation

The course will require on the order of 15 hours per week for external work. I will grade submitted work within a week, typically. 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. I expect each of you to actively be engaged in discussions, and to reply to questions from me or other students. When you respond, reply to either my question or a reply from another student. I expect you to answer or post at least twice per discussion. 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 assignments 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	(70-76)
F	(0-69)

The course will have multiple assignments per modules, but the total number of points per module is 20. Some assignments will be worth 20 points, some 10, and some 5. Assignments can be resubmitted as many times as you would like.

All written reports should be submitted as a PDF via learn following the specific formatting guidelines (APA). 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 learn associated with the grade.

Late Work

I’ll accept late work, and will give you opportunities to submit graded assignments for higher grades. All work will be due at the end of the term. 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.

Schedule of Activities

This is an eight week course. We will address both offensive and defensive techniques.

Week 1:	Your Environment
Week 2 & 3:	Cryptology & Cybersecurity
Week 4 & 5:	ROP and Code Reuse
Week 6:	The Modern Heap and Heap Attacks
Week 7 & 8:	Malware Design, Development, and Defense

Prerequisites & Technical Skills

I expect you have taken Introduction to Technical Cybersecurity (ECE529), or you have equivalent experience. We will be using Linux and virtualization extensively. Students are expected to be familiar with Linux, be familiar with C programming and make, and understand essentially how computers work. Students will need to be at a strong level of proficiency in a computer language like Python, Perl, Lua, or Ruby. We will use disassemblers, decompilers, and binary debuggers.

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 will also need to run a windows virtual machine. You'll need access to a high speed internet connection to watch videos as well, and you will need a large screen for videos with live debugging examples as the screen size requirements for these tools are high. 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.

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. 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. You will submit homework assignments online.

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
Ubuntu's accessibility statement: https://help.ubuntu.com/community/Accessibility
VMWare accessibility statement: https://www.vmware.com/help/accessibility.html
GNU accessibility statement: https://www.gnu.org/accessibility/accessibility.en.html

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

Graduate Resource Center: https://ctl.unm.edu/graduate-students/index.html

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

Student Health & Counseling (SHAC) Online Services:
http://online.unm.edu/help/learn/support/shac