Advanced Hacking of Linux (and Embedded Systems) (ENPM809V)
Sections 0101 and CY01

Professor: Michael Wittner
Email: mwittner@umd.edu
**Office Hours – TBD (Likely Wednesday/Thursday
from 7:30-9:30pm)**
Term: Spring 2025
Credits: 3
Course Dates: From January 28, 2024 - May 20, 2024

Course Times: Tuesdays 7:00 pm - 9:40 PM and Online

Classroom: JMP 2116

CANVAS/ELMS Link: https://umd.instructure.com/courses/1360103

Discord link: https://discord.gg/ZSMAgyz4Xa

Course Description

This course provides an in-depth understanding of how to find flaws in Linux (both userspace and kernel space) and software within embedded devices (focusing on bare-metal software/firmware and hardware-focused techniques). Students will get an inside look at how modern operating systems and embedded devices protect their programs, flaws within the protection mechanisms, and how to exploit them. Although this is an offensive-focused course, mitigations to protect the programs will also be discussed.

Prerequisites

- Required Course: ENPM691

- Familiarity with Linux, x86_64 assembly language, and programming in C and Python.

- Recommended: ENPM695 and ENPM696

Learning Outcomes
After successfully completing this course you will be able to:

- Explain how vulnerabilities are found and how they are exploited
- Write secure code (code without vulnerabilities) and mitigate vulnerabilities that might be present on modern Linux and embedded systems.
- Differentiate between software in embedded systems and other modern computing systems, and explain the similarities and differences between securing both of them.

Required Technology

For a majority of the course, we will be working in a virtualized desktop environment in the pwn.college environment. This means that at a minimum you will need a computer with internet access. I strongly recommend that you also bring a laptop to class as this will help significantly with participating in hands-on coursework during class.

Course Structure

This course includes both on-campus and online sections.

For asynchronous online students, all lectures will be recorded and made available on ELMS-Canvas under "Panopto Recordings/Video Lectures" within 24 hours of the class time. Be sure to review the recorded lecture in a timely manner.

If online students wish to attend synchronously online, you can do so by logging into ELMS-Canvas at the time of the Section 0101 class [Tuesday/7:00 PM] and selecting "Video Conference" from the left side menu. This will open a Zoom link to the live classroom.

On-campus students are expected to attend in-person class sessions and be prepared to engage with the lecture and materials. If you have a conflict on a particular day, please reach out to me in advance to discuss. Online students, be sure to log into Canvas regularly and participate in discussions and activities. Regardless of the section you are enrolled in, participation is expected.

Please note that F1 students enrolled in the on-campus section are required to attend in person.

Communication Guidelines

Course Discord Server

We will be utilizing a Discord server throughout the semester. This will be used to communicate with the instructor, TA, and your peers about concepts taught in the course and in assignments. If you have questions regarding details about an assignment, please reach out to the instructor or TA directly. Do not ask a peer or put it in the public chat channel.

Here are a few examples of what to say/not to say to a peer or in a public chat channel,

- OKAY: How does the tcache poisoning vulnerability/exploit work?
- OKAY: Pwntools has a module called fmtstr that you can use to create format string-based exploits.
- OKAY: There is a buffer overflow in the homework where you need to do a ret2libc to get root and solve it!
- NOT OKAY: Here is the exact code for solving the buffer overflow homework

To join the Discord server, use this URL and create an account: https://discord.gg/ZSMAgyz4Xa. To help me know who you are, please update your profile to include your first name and last name.

Communicating with the Instructor and TAs

My goal is to be readily available to you throughout the semester. I can be reached by Discord for questions related to course material and assignments, and reachable by email at mwittner@umd.edu for administrivia. Please DO NOT email me with questions that are easily found in the syllabus or on ELMS-Canvas (e.g., When is this assignment

due? How much is it worth? etc.), but please DO reach out about personal, academic, and intellectual concerns/questions.

While I will do my best to respond to emails within 24 hours, you will more likely receive email responses from me Monday-Friday between 2:00pm and 8:00pm EST.

When constructing an email to me please put "**[ENPM809V]: Your Topic "** in the subject line. This will draw my attention to your email and enable me to respond to you more quickly.

Additionally, please review [These tips for 'How to email a Professor'](). By following these guidelines, you will be ensured to receive a timely and courteous response.

Finally, if you need to discuss issues not appropriate for the classroom, Discord, and/or an email, we can arrange to talk by phone, over Zoom, or in-person. Send me an email asking for a meeting and we can set something up.

Announcements
I will send IMPORTANT messages, announcements, and updates through both ELMS-Canvas and Discord. To ensure you receive this information in a timely fashion, make sure your email and announcement notifications (including changes in assignments and/or due dates) are enabled in ELMS-Canvas ([How to change notification settings in CANVAS]()).

Log into our ELMs-Canvas course site and/or Discord at least once every 24-hour period to check your inbox and the Announcements page.

Names/Pronouns and Self-Identifications
The University of Maryland recognizes the importance of a diverse student body, and we are committed to fostering inclusive and equitable classroom environments. I invite you, if you wish, to tell us how you want to be referred to in this class, both in terms of your name and your pronouns (he/him, she/her, they/them, etc.). Keep in mind that the pronouns someone uses are not necessarily indicative of their gender identity. Visit trans.umd.edu to learn more.

Additionally, it is your choice whether to disclose how you identify in terms of your gender, race, class, sexuality, religion, and dis/ability, among all aspects of your identity (e.g., should it come up in classroom conversation about our experiences and perspectives) and should be self-identified, not presumed or imposed. I will do my best to address and refer to all students accordingly, and I ask you to do the same for all of your fellow Terps.

Communicating with your Peers
With a diversity of perspectives and experience, we may find ourselves in disagreement and/or debate with one another. As such, it is important that we agree to conduct ourselves in a professional manner and that we work together to foster and preserve a virtual classroom environment in which we can respectfully discuss and deliberate controversial questions. I encourage you to confidently exercise your right to free speech—bearing in mind, of course, that you will be expected to craft and defend arguments that support your position. Keep in mind, that free speech has its limit and this course is NOT the space for hate speech, harassment, and derogatory language. I will make every reasonable attempt to create an atmosphere in which each student feels comfortable voicing their argument without fear of being personally attacked, mocked, demeaned, or devalued.

Any behavior (including harassment, sexual harassment, and racially and/or culturally derogatory language) that threatens this atmosphere will not be tolerated. Please alert me immediately if you feel threatened, dismissed, or silenced at any point during our semester together and/or if your engagement in discussion has been in some way hindered by the learning environment..

Netiquette Policy

Netiquette is the social code of online classes. Students share a responsibility for the course's learning environment. Creating a cohesive online learning community requires learners to support and assist each other. To craft an open and interactive online learning environment, communication has to be conducted in a professional and courteous manner at all times, guided by common sense, collegiality and basic rules of etiquette.

Grading

Grade Breakdown

Assignment	Percentage %
Assignments (Classwork and Homework)	80%
Final Project	20%
Total	100%

Course Assignments

Classwork Assignments
- In class work to help you understand a concept.
- These will be done during the course of the class. It is up to my discretion if it is graded.
- If it is graded, a submission of the code to Github Classroom and flag submission to pwn.college may be required.

Homework Assignments
- Small assignments to help you practice concepts learned. Generally this will be done on the infrastructure.
- Students are expected to submit code on Github Classroom or Canvas that is commented explaining what they have done.
- Students are expected to submit a short writeup with a set of questions they need to answer.
- No word limit or minimum. Write enough to explain what you did.

Final Project
- Individual assignment that is a cumulative (may switch to Group at my discretion).
- You will be given 3-5 problems similar to that of a homework assignment.
- Students need to submit code that is commented on for **each problem**.
- There **may** be a presentation aspect to this assignment
- No word limit or minimum. Write enough to explain what you did

Grading Assignments

All assignments will be graded according to a predetermined set of criteria (i.e., rubric) which will be communicated to students before the assignment is submitted.

To progress satisfactorily in this class, students need to receive timely feedback. To that end, it is my intention to grade all assignments within **two weeks(s)** of their due date. If an assignment is taking longer than expected to grade, students will be informed of when they can expect to see their grade.

Grade Computation

All assessment scores will be posted on ELMS/Canvas page. If you would like to review any of your grades (including the exams), or have questions about how something was scored, please email the TA or instructor who graded the assignment (and CC the instructor). If you would like to discuss in person or over Zoom, please email to schedule a time for us to meet and discuss.

It is expected that you will submit work by the deadline listed in the syllabus and/or on ELMS-Canvas. Late work will be penalized according to the late work policy described in the **Course Policies and Procedures** section below.

Grade Disputes: All grading concerns must be sent to the instructor via e-mail within 2 weeks of the grade being posted. If the instructor elects to review your assignment it will be for an exhaustive re-grade and your score for the assignment may go up or down depending on what the re-grade determines.

Final letter grades are assigned based on the percentage of total assessment points earned. To be fair to everyone I have to establish clear standards and apply them consistently, so please understand that being close to a cutoff is not the same as making the cut (89.99 ≠ 90.00). It would be unethical to make exceptions for some and not others.

Final Grade Cutoffs				
A+ = 100 – 96	**B+** = 89.99 – 86	**C+** = 79.99 – 76	**D+** = 69.99 – 66	**F** = 59.99 – 0
A = 95.99 – 90.01	**B** = 85.99 – 80.01	**C** = 75.99 – 70.01	**D** = 65.99 – 60.01	
A- = 90	**B-** = 80	**C-** = 70	**D-** = 60	

- **Extra Credit:** I generally do not offer extra credit. Do the work and you'll be fine.
- **Curve:** There will be no curve for the class. Do the work and you'll be fine.
- **Rounding**: I do not round grades up/down. Do the work and you'll be fine.
- **All assignments must be submitted via Github Classrooms. A link to the specific assignment on Github Classroom will be available on ELMS (as an assignment). Anything not submitted on Github Classroom (or ELMS if directed by the instructor) will not be accepted.**
- **Majority of the assignments will require to obtain a flag from pwn.college. All flag submissions must be submitted via pwn.college. No flag submission on pwn.college = no credit for that portion of the assignment.**
- **Assignments are not completed until they are submitted in ELMS.**

- **The only timestamp that matters is the one in ELMS.**
- **Check that you have submitted the correct assignment after you have uploaded it.**

Questions/Troubleshooting Matrix

Support Item	Support Contact
Class administrative issues	1. Review the syllabus 2. Review the week 1 slides 3. Contact the professor
Technical questions	1. Google 2. Contact the TA 3. Contact the Professor
ELMS/Canvas issues	IT Support- https://itsupport.umd.edu/
Issues with lecture video capture/playback	DETS - dets-support@umd.edu

Course Schedule

Week	Subject	Learning Objectives	Assignments
1	**Introduction to the Course, Tooling, and Shellcoding**	- Course Overview - Course Setup (pwn.college) - Debugging - Reverse Engineering Tools - Pwntools - Dynamic Analysis Tools - Shellcoding	Basic submission to Github Classroom **Assigned**
2	**ELF Files, x86_64 Assembly, Introduction to Return Oriented Programming (ROP) & Stack Mitigations**	- ELF & Linking - Library and System Calls - X86_64 Assembly Fundamentals - Review of Buffer Overflows - Introduction to ROP Programming	Buffer Overflow Homework **Assigned**
3	**ROP Chain & ret2libc**	- Fundamentals of ROP Chain Exploits - Tools for finding ROP	Basic Submission to Github Classroom **Due**

		- Gadgets - Ret2libc exploit	
3	**Heap Based Exploits**	- What is heap and the dangers - Basics of Heap exploitation - Heap Protection Mechanisms - TCache poisoning - Metadata Corruption	Buffer Overflow Homework **Due** Ret2libc and Bin poisoning homework **assigned**
4	**Linux File System and Race Conditions**	- What is a race condition - Overview of Linux File System - Exploitation of Race Conditions - Thread-Based Race Conditions - Memory-Based Race Conditions	
5	**Linux Processes and Sandboxing**	- What are System Calls - Linux System Calls - Chroot - Seccomp/BPF - Bypassing seccomp	Ret2libc and bin poisoning homework **due** Race condition and sandboxing homework **assigned**
6	**Injection**	- LD_PRELOAD - Process Memory Manipulation - ELF Poisoning - PTrace - Using injection to bypass sandboxing	
7	**Linux User Mode Hijacking**	- Hooking - Pointer Replacement - Callback registration	Race condition and sandboxing homework **due** Injection and entry stub trampoline homework **assigned** Reading given for Kernel Internals
8	**No Class Spring Break**		

8	**Linux Kernel Hacking Part 1**	- Kernel Modules and Character Devices - Basic Privilege Escalation	Injection and Entry Stub Homework **Due** Privilege Escalation Homework **Assigned**
10	**Linux Kernel Hacking Part 2**	- Shellcoding in the Kernel - Controlling I/O - Escaping seccomp via the kernel	
11	**Linux Kernel Hacking Part 3**	- Stack based attacks in the kernel - KASLR	Kernel Stack Overflow Homework **Assigned** Privilege Escalation Homework **Due**
12	**Linux Kernel Hacking Part 4**	- Learning Kernel Heap - Caches - Memory Cache Attacks	
13	**Linux Kernel Hacking Part 5**	- Practicing Exploiting the Heap - Exploiting Heap Caches	Final Project **Assigned** Kernel Heap Attacks homework **Assigned** Kernel Stack Overflow Homework **Due**
14	**Linux Kernel Hijacking**	- Living off of the land - Keyloggers - eBPF	
15	**Flex week/Vulnerability Research (if there is time)**	- Principals of Vulnerability Research - Fuzzing - Symbolic execution	Kernel Heap Attacks **Due**
16	**Finals Week**		**Final Project Due**

Note: This is a tentative schedule, and subject to change as necessary – monitor ELMS-Canvas for current deadlines. In the unlikely event of a prolonged university closing, or an extended absence from the university, adjustments to the course schedule, deadlines, and assignments will be made based on the duration of the closing and the specific dates missed.

Course Policies and Procedures

The University of Maryland's conduct policy indicates that course syllabi should refer to a webpage of course-related policies and procedures. For a complete list of graduate course related policies, visit the [Graduate School website](#). Below are course-specific policies and procedures which explain how these Graduate School policies will be implemented in this class.

Office Hours
Office hours during the times listed at the top of this syllabus. It is expected that the students contact the TA or professor at least three hours (or 10pm if the sessions starts before 10am) to let them know that they are coming. Otherwise office hours will be canceled for that day. If the day/time does not work, contact the TAs and professor to schedule a different time. Check the announcements if office hours changed for the week.

Satisfactory Performance
The Graduate School expects students to take full responsibility for their academic work and academic progress. The student, to progress satisfactorily, must meet all the academic requirements of this course. Additionally, each student is expected to complete all readings and any preparatory work before each class session, come to class prepared to make substantive contributions to the learning experience, and to proactively communicate with the instructor when challenges or issues arise.

Questions about Assignments
Please ask all questions you may have about an assignment 24 hours before the assignment is due. Any questions asked after that time may not be answered in time for you to make changes to your work.

Late Work Policy
Assignments should be completed by the due date and time listed with the assignment, on the syllabus, and/or in the course calendar. If you are unable to complete an assignment by the stated due date, it is your responsibility to contact your instructor to discuss an extension, at least 24 hours BEFORE the assignment is due. Extensions are not guaranteed, but may be granted at the instructor's discretion.

Late assignments will have 10% of the points deducted for every day the assignment is late. Assignments submitted over one week late will not be accepted or graded. If there are extenuating circumstances for you to submit work late please contact the instructor as soon as possible along with proof of your extenuating circumstance (preferably before the assignment is due.)

Religious Observance
It is the student's responsibility to inform the instructor of any intended absences for religious observances in advance. Notice should be provided as soon as possible but no later than the end of the schedule adjustment period.

Academic Integrity
For this course, some of your assignments will be collected via Turnitin on ELMS/Canvas. I have chosen to use this tool because it can help you improve your scholarly writing and help me verify the integrity of student work. For information about Turnitin, how it works, and the feedback reports you may have access to, visit Turnitin Originality Checker for Students

The University's Code of Academic Integrity is designed to ensure that the principles of academic honesty and integrity are upheld. In accordance with this code, the University of Maryland does not tolerate academic dishonesty. Please ensure that you fully understand this code and its implications because all acts of academic dishonesty will be dealt with in accordance with the provisions of this code. All students are expected to adhere to this Code. It is your responsibility to read it and know what it says, so you can start your professional life on the right

path. **As future professionals, your commitment to high ethical standards and honesty begins with your time at the University of Maryland.**

It is important to note that course assistance websites, such as CourseHero, or AI generated content are not permitted sources, unless the instructor explicitly gives permission. Material taken or copied from these sites can be deemed unauthorized material and a violation of academic integrity. These sites offer information that might be inaccurate or biased and most importantly, relying on restricted sources will hamper your learning process, particularly the critical thinking steps necessary for college-level assignments.

Additionally, students may naturally choose to use online forums for course-wide discussions (e.g., Group lists or chats) to discuss concepts in the course. However**, collaboration on graded assignments is strictly prohibited unless otherwise stated**. Examples of prohibited collaboration include: asking classmates for answers on quizzes or exams, asking for access codes to clicker polls, etc. Please visit the **Office of Graduate Studies' full list of campus-wide policies** and reach out if you have questions.

If you ever feel pressured to comply with someone else's academic integrity violation, please reach out to me straight away. Also, *if you are ever unclear* about acceptable levels of collaboration, *please ask*!

To help you avoid unintentional violations, *the following table* lists levels of collaboration that are acceptable for each graded exercise. Each assignment will contain more specific information regarding acceptable levels of collaboration. Please note: **if you use AI to solve the assignments, please mention how you used it in your submission.** This information will help us improve the course for future sections.

	OPEN NOTES	USE BOOK	LEARN ONLINE	GATHER CONTENT With AI	ASK FRIENDS	WORK IN GROUPS
In-Class Practice/Assignments	✔	✔	✔	✔	✔	✔
Homework Assignments	✔	✔	✔	✔ - With Restrictions	✔ - With restrictions	---
Final Project	✔	✔	✔	✔ - With Restrictions	✔ - With restrictions	TBD

Restrictions on Gathering Content with AI and Asking Friends for Help:
The best way to learn this subject matter is by learning from others. It is an extremely difficult subject to master alone and requires lots of practice. In the real world, you will have others and AI to help you explain parts that may be confusing. While I am allowed to discuss with others in the class, there are restrictions to what you can do.

1) You cannot use AI to generate your answer. It is a great tool for grammar/spelling, and explaining concepts. **If I catch that anyone uses AI to generate a response or reword a previous response/someone else's response, I will refer you to academic integrity immediately.**

2) Although you can ask friends to help you understand the content of the course/homework (and it is encouraged), you need to submit your own work. The reason for this is that if you copy code from another classmate, you are not learning the subject matter. Submit your own work. **If I catch any sense of plagiarism, I will refer you to academic integrity immediately.**

3) This doesn't replace the instructor/TA. Come to office hours.

Course Evaluation

Please submit a course evaluation through Student Feedback on Course Experiences in order to help faculty and administrators improve teaching and learning at Maryland. All information submitted to Course Experiences is confidential. Campus will notify you when Student Feedback on Course Experiences is open for you to complete your evaluations at the end of the semester. Please go directly to the **Student Feedback on Course Experiences** to complete your evaluations. By completing all of your evaluations each semester, you will have the privilege of accessing through Testudo the evaluation reports for the thousands of courses for which 70% or more students submitted their evaluations.

Copyright Notice

Course materials are copyrighted and may not be reproduced for anything other than personal use without written permission.

Tips for Succeeding in this Course

1. **Participate.** I invite you to engage deeply, ask questions, and talk about the course content with your classmates. You can learn a great deal from discussing ideas and perspectives with your peers and professor. Participation can also help you articulate your thoughts and develop critical thinking skills.

2. **Manage your time.** Students are often very busy, and I understand that you have obligations outside of this class. However, students do best when they plan adequate time that is devoted to course work. Block your schedule and set aside plenty of time to complete assignments including extra time to handle any technology related problems.

3. **Login regularly.** I recommend that you log in to ELMS-Canvas several times a week to view announcements, discussion posts and replies to your posts. You may need to log in multiple times a day when group submissions are due.

4. **Do not fall behind.** This class moves at a quick pace and each week builds on the previous content. If you feel you are starting to fall behind, check in with the instructor as soon as possible so we can troubleshoot together. It will be hard to keep up with the course content if you fall behind in the pre-work or post-work.

5. **Use ELMS-Canvas notification settings.** Pro tip! Canvas ELMS-Canvas can ensure you receive timely notifications in your email or via text. Be sure to enable announcements to be sent instantly or daily.

6. **Ask for help if needed.** If you need help with ELMS-Canvas or other technology, IT Support. If you are struggling with a course concept, reach out to me and your classmates for support.

Student Resources and Services

Taking personal responsibility for your learning means acknowledging when your performance does not match your goals and doing something about it. I hope you will come talk to me so that I can help you find the right approach to

success in this course, and I encourage you to visit the [Counseling Center's Academic Resources](#) to learn more about the wide range of resources available to you. Below are some additional resources and services commonly used by graduate students. For a more comprehensive list, please visit the Graduate School's [Campus Resources Page](#).

Accessibility and Disability Services

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is also committed to the principle that no qualified individual with a disability shall, on the basis of disability, be excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The [Accessibility & Disability Service (ADS)](#) provides reasonable accommodations to qualified individuals to provide equal access to services, programs and activities. ADS cannot assist retroactively, so it is generally best to request accommodations several weeks before the semester begins or as soon as a disability becomes known. Any student who needs accommodations should contact me as soon as possible so that I have sufficient time to make arrangements.

For assistance in obtaining an accommodation, contact Accessibility and Disability Service at 301-314-7682, or email them at adsfrontdesk@umd.edu. Information about [sharing your accommodations with instructors, note taking assistance](#) and more is available from the [Counseling Center](#).

Writing Center

Everyone can use some help sharpening their communication skills (and improving their grade) by visiting [The Graduate School's Writing Center](#) and schedule an appointment with them. Additionally, international graduate students may want to take advantage of the Graduate School's free [English Editing for International Graduate Students (EEIGS) program](#).

Health Services

The University offers a variety of physical and mental health services to students. If you are feeling ill or need non-emergency medical attention, please visit the [University Health Center](#).

If you feel it would be helpful to have someone to talk to, visit [UMD's Counseling Center](#) or [one of the many other mental health resources on campus](#).

Notice of Mandatory Reporting

Notice of mandatory reporting of sexual assault, sexual harassment, interpersonal violence, and stalking: As a faculty member, I am designated as a "Responsible University Employee," and I must report all disclosures of sexual assault, sexual harassment, interpersonal violence, and stalking to UMD's Title IX Coordinator per University Policy on Sexual Harassment and Other Sexual Misconduct.

If you wish to speak with someone confidentially, please contact one of UMD's confidential resources, such as [CARE to Stop Violence](#) (located on the Ground Floor of the Health Center) at 301-741-3442 or the [Counseling Center](#) (located at the Shoemaker Building) at 301-314-7651.

You may also seek assistance or supportive measures from UMD's Title IX Coordinator, Angela Nastase, by calling 301-405-1142, or emailing titleIXcoordinator@umd.edu.

To view further information on the above, please visit the [Office of Civil Rights and Sexual Misconduct's](#) website at [ocrsm.umd.edu](#).

Basic Needs Security
If you have difficulty affording groceries or accessing sufficient food to eat every day, or lack a safe and stable place to live, please visit [UMD's Division of Student Affairs website](#) for information about resources the campus offers you and let me know if I can help in any way.

Veteran Resources
UMD provides some additional supports to our student veterans. You can access those resources at the office of [Veteran Student life](#) and the [Counseling Center](#). Veterans and active duty military personnel with special circumstances (e.g., upcoming deployments, drill requirements, disabilities) are welcome and encouraged to communicate these, in advance if possible, to the instructor.