CS 647: Counter-Hacking Techniques

New Jersey Institute of Technology

Ying Wu College of Computing

Department of Computer Science

Instructor Contact Information

Instructor: Michael Martin
Email: mjm222@njit.edu
Course website: https://canvas.njit.edu/
Online Office Hours:

Wednesdays	17:30 – 18:30
Thursdays	17:30 – 18:30

Statement of Purpose

This course covers advanced techniques that can be used for offensive or defensive goals in networks, computer systems, and applications. The course follows a "learning by doing" teaching approach through extensive use of virtual machines with vulnerable operating systems and applications. Topics covered include system memory organizations, CPU registers, assembly language fundamentals, GDB debugger, fuzzing-based security testing development of local and remote Linux and Windows exploits, shellcode development, stealthy attacks, bypassing memory protection techniques, network and wireless hacking techniques, and ethical and legal implications of cyber-attacks.

The general topics covered are:

- Basic Computer Architecture
- Programming in x86 Assembly
- Buffer Overflow Exploits and Protections
- Format String Exploits
- Network-based Attacks
- Code Hardening
- Ethical Hacking
- Cybersecurity Ethics
- Malware Analysis and Reverse Engineering
- Hardware Side Channel Attack (Spectre & Meltdown)

Prerequisites

One of the following courses or approval from the instructor:

- CS 645
- CS 646
- CS 696
- ECE 638

Recommended Topics:

- A basic understanding of computer architecture.
- Prior experience working with assembly language will be helpful (x86 specifically) but is not required.
- Some prior experience with the C programming language or the ability to self-learn.
- Some prior experience using a Linux Operating system and with basic Linux commands.
- An understanding of basic cryptographic principles such as hashing and public key infrastructure.

Required Materials

This course **does not require any text**; however, it will reference information and material from the following sources:

- "Hacking: The Art of Exploitation" 2nd Edition, *by Jon Erickson*,
  ISBN-13: 978-1593271442
  ISBN-10: 1593271441
- "Introduction to Computer Security", *by M. Goodrich and R. Tamassia*,
  Addison Wesley, 2010,
  ISBN: 0321512944
- "Computer Systems: A Programmer's Perspective" 3rd Edition, *by Randal Bryant and David O'Hallaron*
  ISBN-13: 978-0134092669
  ISBN-10: 013409266X
- "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" 1st Edition, *by Michael Sikorski and Andrew Honig*
  ISBN-13: 978-1593272906
  ISBN-10: 1593272901

To participate in the course, students must either own or be able to use a computer with virtualization capabilities. It is suggested that the computer has at least 50-60GB of available storage space and a minimum of 4GB of memory to allocate to the guest virtual machine. While many operating systems can be used, Windows 10 or 11 is recommended. If a student's computer cannot support the course's virtual machine, they can use Amazon Web Services instead. As long as the student is careful about managing their Amazon EC2 instance uptime, the costs for the semester are expected to be low.

A webcam is required to take the proctored exams via Respondus Lockdown Browser and Respondus Monitor.

Course Learning Outcomes

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

- Describe cybersecurity and privacy mechanisms, standards, and state-of-the-art capabilities.
- Describe potential cyber-attacks and the actors that might perform them.
- Apply cyber defense methods to prepare a system to repel attacks.
- Perform security review of applications and systems.
- Create exploits to vulnerabilities identified on Linux or Windows systems.
- Design and implement system, network, and infrastructure-level solutions to ensure the security and privacy of communications and data against specific security threats.
- Describe the trade-offs between security, usability, and performance.
- Use standard security terminology to communicate effectively with other cybersecurity professionals.
- Analyze ethical considerations in cybersecurity, such as potential harm, red flags, common challenges, contributions to the public good, and affected stakeholders.

Course Structure and Components

Announcements

Each week, typically when a new Module is released, a "Housekeeping" announcement that contains crucial information will be posted. This part of the course is by design, and students must read these announcements carefully. **Please be on the lookout for these and other ad hoc announcements and read them carefully; it is essential!**

Lectures

Lecture slides, supplemental materials, and lecture recordings are available weekly through Canvas modules. The lectures aggregate material from personal experience and training and the text references mentioned in the Required Materials section.

The lecture recordings are mostly broken down into short videos with descriptive titles. This should make it easier for students to go through at their own pace and reference back to specific lecture sections.

Students will find that most lectures include hands-on challenges administered with virtual machines. Attempting the challenges is not optional but a structured part of the course. Many of the topics presented are low-level, semi-advanced, requiring hands-on practice. The lectures follow a learn-by-doing approach where the students are given a concept/technique and then challenged to implement it themselves in a controlled environment. The video following the challenge will include a walk-through solution to explain it in detail.

Weekly Assignments

Students will conduct cyber vulnerability assessments for assigned programs each week. These assessments aim to foster critical thinking and encourage collaboration among students. The assessments require the students to identify vulnerabilities, create exploits, and communicate mitigation strategies to a hypothetical client. While the assignments are closely tied to lecture material, they will also require students to apply learned techniques to novel scenarios. Depending on the student's technical background and experience, they may need additional research. All assessment materials are in a virtual machine designed specifically for this course.

For the assessments, students will work in randomly assigned groups on Canvas, which the instructor may change throughout the semester. After completing the assessment and developing a working exploit, each group member must demonstrate the implementation of

that exploit on their instance of the course virtual machine. To prove success, each student on the team must submit their flag on Canvas within one week of the assessment being assigned.

The teams will be given an extra week to work together on a report that conforms to the Writing Guide of the course. The Writing Guide, which includes details on writing style and other report necessities, is readily available on Canvas. The reports should be composed on a Google Doc assigned through Canvas's Collaboration menu. The instructor will have access to the document and may examine the version history to assess each student's input. Students who do not contribute sufficiently to the team may receive lower grades. To better understand their grades, a rubric is available for the reports. For both submissions, students must include a text-based version of the challenges' flag files and a screenshot that showcases the output of the flag file printed to the terminal.

Projects

Two assignments are given more time to work on and carry slightly more weight. The first project requires students to showcase their ability to write a functioning program in x86 assembly language. For the second project, students must demonstrate their creativity by crafting an attack that exploits a buffer overflow vulnerability, allowing them to execute arbitrary code on a machine. The exploit must be able to bypass several modern buffer overflow defenses. Additionally, students must write a detailed technical report outlining their methods and procedures.

Exams

The midterm and final exams are closed-book exams. Many problems are open-ended questions that probe the student’s knowledge of core concepts taught throughout the course. These exams will be held online with Respondus LockDown Browser. There are two options for proctoring that students can choose between. They can take the exam in person with the instructor (recommended) or remotely. Students who take the exam remotely must do so through Respondus Monitor and will need a webcam to be proctored. For more information, please see the "Online Exams and Proctoring" page at the top of Module 0x0 in Canvas.

Students who take the exams on campus do not need a webcam and will only use Respondus LockDown Browser. This is the recommended mode to take the exam. A time and location will be announced, and students can email the instructor that they will be attending in person.

Schedule of Assignments

Important Dates

Spring 2024 Academic Calendar

January	15	Monday	Martin Luther King, Jr. Day
January	16	Tuesday	First Day of Classes
January	20	Saturday	Saturday Classes Begin
January	22	Monday	Last Day to Add/Drop a Class
January	22	Monday	Last Day for 100% Refund, Full or Partial Withdrawal
January	23	Tuesday	W Grades Posted for Course Withdrawals
January	29	Monday	Last Day for 90% Refund, Full or Partial Withdrawal, No Refund for Partial Withdrawal after this date
February	12	Monday	Last Day for 50% Refund, Full Withdrawal
March	4	Monday	Last Day for 25% Refund, Full Withdrawal
March	10	Sunday	Spring Recess Begins - No Classes Scheduled - University Open
March	16	Saturday	Spring Recess Ends
March	29	Friday	Good Friday - No Classes Scheduled - University Closed

March	31	Sunday	Easter Sunday - No Classes Scheduled - University Closed
April	1	Monday	Last Day to Withdraw
April	30	Tuesday	Friday Classes Meet
April	30	Tuesday	Last Day of Classes
May	1	Wednesday	Reading Day 1
May	2	Thursday	Reading Day 2
May	3	Friday	Final Exams Begin
May	9	Thursday	Final Exams End
May	11	Saturday	Final Grades Due
May	-	TBA	Commencement

Weekly Outline

Module	Topics and Assignments	Assignments Due *At 11:59PM on Sunday at the end of each module.*
0x0	**Course Introduction** *Assigned:* • *Pippin Assessment* • *Syllabus Acknowledgment* • *Introduction Video*	☐ Pippin Assessment Flags ☐ Syllabus Acknowledgment ☐ Introduction Video
0x1	**Basic Computer Architecture** *Project 1 Assigned*	☐ Pippin Assessment Report ☐ Pippin Assessment Peer Evaluation
0x2	**x86 Assembly Part 1** **x86 Assembly Part 2**	
0x3	*Work on Project 1*	☐ Project 1 Due ☐ Project 1 Peer Evaluation
0x4	**Exploitation** **Buffer Overflows Part 1** *Merry Assessment Assigned*	☐ Merry Assessment Flag
0x5	**Buffer Overflows Part 2**	☐ Merry Assessment Report ☐ Merry Assessment Peer Evaluation
0x6	Midterm Exam ***The exact time, date, and location will be announced on Canvas.*** *Sam Assessment Assigned*	☐ Sam Assessment Flags

0x7	**Buffer Overflows Part 3** *Project 2 Assigned*	☐ Sam Assessment Report ☐ Sam Assessment Peer Evaluation
0x8	**Buffer Overflows Part 4** **Format String Vulnerabilities** Continue work on Project 2	
0x9	Introduction to Cybersecurity Ethics Continue work on Project 2	☐ Cybersecurity Ethics Discussion Posts are due by Friday at 23:59 ☐ Responses to Peers are due by Sunday at 23:59
0xa	Network-Based Attacks and Code Hardening *Frodo Assessment Assigned*	☐ Project 2 Report ☐ Project 2 Peer Evaluation
0xb	Introduction to Ethical Hacking	☐ Frodo Assessment Flag
0xc	Malware Analysis and Reverse Engineering	☐ Frodo Assessment Report ☐ Frodo Assessment Peer Evaluation
0xd	Hardware Side Channel Attack Lab (Spectre & Meltdown)	
0xe	Final Exam ***Time and location TBD by Registrar***	

Grading

Letter Grade	Significance	Calculation
A	Excellent	90% and above
B+	Good	85% - 89%
B	Acceptable	80% - 84%
C+	Marginal Performance	75% - 79%
C	Minimum Performance	65% - 74%
F	Failure	Below 65%

Grading based on assignments:

- Vulnerability Assessments (*two parts each*): 16%
  - Pippin Assessment
  - Merry Assessment
  - Sam Assessment
  - Frodo Assessment
- Cybersecurity Ethics Discussion Post 4%
- Legolas Assessment (Project 2) 10%
- Programming Project (Project 1) 10%
- Midterm Exam 30%
- Final Exam 30%

To earn full points on the vulnerability assessments, students must:

- Craft a working exploit to obtain the flag file.
- Each student must submit their flag for the first part of the assignment.
- Collaborate with the team to complete the report that conforms to the course writing guide on Google Docs and contribute to the overall effort.
- Upon the instructor's request, demonstrate the exploit in Webex.

Assignments have 8 hours after the due date for which they can still be submitted with a 50% deduction in score. Do not wait until just before the deadline to submit. After the eight hours pass, assignments will no longer be accepted without prior approval.

Peer Evaluations

In this course, peer evaluations play a pivotal role in assessing teamwork skills during vulnerability assessments and projects. You will engage in self-reflection and evaluate your peers while considering aspects like listening, communication, collaboration, idea development, and overall contribution. Your thoughtful feedback will contribute to a collaborative learning environment and accountability for the team.

While the peer evaluations will not count toward your final grade, they are mandatory for receiving credit on your vulnerability report and projects. Please ensure timely submission to facilitate the assessment process.

Submissions of all assignments MUST be on Canvas for accountability. Submissions will not be accepted through email or any other form.

Responsiveness and Availability

Under normal conditions, emails will be responded to within 24 hours. Students should send another email if there is no response within 48 hours. Assignments will be graded within two weeks of their due date.

IMPORTANT: Start the subject line of all emails with **CS647:** <Your subject here>
This will allow course-related emails to be filtered for prompt responses.

Students are encouraged to ask for help and attend office hours. Every student on the course comes from various backgrounds and experiences. Asking questions is excellent and can benefit the entire class. Students should ask questions via email and pay attention to announcements where common questions will be posted.

Students are encouraged to seek help whenever they need it. Every student comes from a different background and has unique experiences. Asking questions is an excellent way to enhance the learning experience. Those who need extra help must reach out to the instructor early in the modules. They should do so via email. Additionally, responses to common questions may be posted on the announcements page, so please watch for any updates.

Feedback

Feedback for the course assignments will be delivered using the comments feature in Canvas. Any details that require further discussion will take place over email, in an online chat, or over the phone.

Academic Integrity

The below statement also goes for copying code. Students will have individual assignments and group assignments. Source code and exploit information must not be shared outside assigned groups. Information on vulnerability assessments is not to be shared. Students should make sure to read NJIT's academic integrity policy in full here.

Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree to which students are working. As a member of the NJIT community, it is every student's responsibility to protect their educational investment by knowing and following the academic code of integrity policy, which is found here.

Please note that my professional obligation and responsibility is to report any academic misconduct to the Dean of Students Office. *Any student found in violation of the code by cheating, plagiarizing, or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university.*

There will be no warnings or second chances about cheating. It is every student's responsibility to understand specifically what constitutes academic dishonesty. Ignorance is not an excuse or a defense. It is also each student's responsibility to understand the rules for properly citing the work of others in the submission of classwork. Improper citation with a simple "copy/paste" from online sources may be grounds for failure of the assignment and/or the course. If students have any questions about the Code of Academic Integrity, they should contact the Dean of Students Office at dos@njit.edu.

Student Support

Canvas Accessibility Statement

Please note: For an accessible version of the course PowerPoint slides, open the files with Microsoft Office 365.

Canvas Orientation

For students who are unfamiliar with Canvas, this is a link to self-paced student orientation.

Resources for NJIT Online Students

Use the following link to visit NJIT Online Students Resources.

Office of Accessibility Resources and Services

The OARS office goal is to enhance the educational experience for students with disabilities at NJIT. OARS is committed to promoting accessibility, inclusivity and awareness as a resource to all members of NJIT.
If students need accommodation due to a disability, they should contact the Office of Accessibility Resources and Services at OARS@NJIT.EDU or visit Kupfrian Hall 201 to discuss their specific needs. A Letter of Accommodation Eligibility from the office authorizing student accommodations is required.