CS 479 - Reverse Engineering: Malware Analysis

Instructor Contact Information:

Instructor: Joshua Reynolds
Office:
Email: jr1@nmsu.edu
Office Hours: T/Th 2-3pm If you cannot attend these hours, send an email and we can schedule another time.

Course Summary: Reverse Engineering is a valuable skill to protect society from cyber threats, and is a lucrative skill for a cybersecurity analyst to have. This challenging course will prepare students to perform entry-level malware reverse engineering. Students will build a portfolio of reverse engineering projects they can share freely. Students will gain experience with reverse engineering techniques, tools, and concepts that will allow them to step into an entry level malware analyst position.

Learning Outcomes:

- Students will learn how malware behaves, spreads, and is controlled.
- Students will learn how to safely analyze malware in controlled environments.
- Students will learn how malware seeks to hide in systems.
- Students will learn to perform static analysis of binaries using simple tools
- Students will learn how malware obfuscates itself to avoid analysis, including using crypto packers, polymorphism, and sandbox detection
- Students will learn to perform decompilation and control-flow analysis of binaries using Ghidra
- Students will learn to dynamically analyze malware in a sandbox environment while observing network traffic, resource consumption, and system calls
- Students will learn to detect malware running with operating-system level permissions (rootkits)
- Students will learn memory forensics techniques to detect malware hidden within benign processes

Course Prerequisites:

There are no official prerequisites for this course. If you haven't taken CS 370 and CS 478, this class may take extra effort for you.

Textbook:

The textbook for this course is required for the readings and projects. If you are around somebody in the class often, you could probably get away with sharing a copy. No access code is required to access the assignment materials.

Learning Malware Analysis by Monnappa K. A. (Published June 2018) ISBN: 9781788392501

Optional Secondary Resource: Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig *Why might I want this secondary resource?* This book is well-known in the reverse engineering community. Having worked through its exercises will give you instant credibility with potential employers. The included assignments are high-quality, and specifically designed to show you each concept we are learning. It is not required to do well in the class.

Hardware Requirements:

This course will involve analyzing Windows 10 malware, which means you will need a machine capable of simultaneously virtualizing Windows 10 and a *nix OS.

We recommend the following specifications at minimum:

- 50+ GB HDD or (USB3.0+ external)
- 8GB+ RAM
- 1GHz+, x86-64 dual core or better processor supporting virtualization (not ARM)
- a USB 3.0+ port

You will need to be able to run a *nix OS on your hardware – this may mean dual booting if you usually run Windows (WSL will not be sufficient).

Course Workload:

Each week, the previous week's assignment will be due on Monday. By Tuesday's class you will have read that week's textbook chapter (20 pages). You will be required to attend class and participate on Tuesdays and Thursdays.

In class, we will send the first $\tilde{2}0$ minutes on lecture and questions. The remainder of the class will be a lab section where everyone will work on the week's assignment. Often, the instructor will prepare a demo or walk through the first steps of the project. Everyone will be responsible for producing their own lab write-up each week. But, working together and learning together is encouraged. You will be responsible to be able to perform the lab techniques yourself on the exams.

You will submit all of your lab write-ups in GitHub, and you will be allowed to have these public to show to potential recruiters your skills. The format of the reports will be markdown. The reports will describe what you discovered about the malware we analyze, and how other analysts could reproduce and confirm your findings.

Course Outline:

Module	Description	Class Dates
Module 0:	Ethics and Reverse Engineering Careers	1/18
Module 1:	Operational Security and Isolation	1/23, 1/25
Module 2:	Assembly, Program Memory Layout, Calling Conventions	1/30, 2/1
Module 3:	Basic Static Analysis	2/6, 2/8
Module 4:	Disassembly and Decompilation in IDA and Ghidra	2/13, 2/15
Module 5:	Beginner Crackmes	2/20, 2/22
Module 6:	Defeating Ransomware	2/27, 2/29
Midterm Week	Review Tuesday, Exam Thursday 3/7 during class time	3/5, **3/7**
–	Spring Break	
Module 7:	Advanced Crackmes	3/19, 3/21
Module 8:	Process Injection and Malware Static Analysis	3/26, 3/28
Module 9:	Dynamic Analysis	4/2, 4/4
Module 10:	Malware Behavior	4/9, 4/11
Module 11:	Crypters and Packers	4/16, 4/18
Module 12:	Control Flow Integrity Attacks and Defenses	4/23, 4/25
Module 13:	64-bit Control Flow Hijacking	4/30, 5/2
Final Exam	Thursday 1-3PM in classroom	**5/9**

Important Dates:

Drop Deadline ..... February 3
Withdraw Deadline ..... March 21
Midterm Exam Practicum ..... March 7
Final Exam Practicum ..... May 9

Grade Policy: Grading in this course will be based on three components: Participation, Projects, and Practical Exams. Participation is worth 10% of the final grade. Students are expected to attend class. Any absence more than 2 class periods will result in a 1% deduction from the 10% total. Projects are worth 60% of the final grade. Weekly projects will be submitted throughout the semester. Exams are worth 30% of the final grade. Exams may include interactive sessions with the instructor evaluating students understanding of course topics and ability to use taught skills.

Deadline Policy Feel free to turn in assignments early. Late assignments have a 10% penalty if they are less than 1 day late, a 50% penalty on the second day, and are not accepted later. We have this penalty so you can move on from past assignments and keep up with the current ones. If an emergency arises, take care of yourself or whoever needs you first, then send a message to course staff when you are able. Remember, even a poor grade is numerically more advantageous than a zero so always submit whatever you have!

Attendance Expectation Lectures will include learning activities as well as information you will be responsible for at exam time to demonstrate your knowledge of reverse engineering. Participation will be recorded during each lecture. It is anticipated that all good-faith efforts to participate will

earn full credit. You have the freedom to miss up to 2 classes without penalty. Any further absences will require documentation.

Collaboration Working together to understand how the malware samples work is encouraged. However, everyone must submit their own reports which include instructions on how another analyst could reproduce your results. In exams, be prepared to individually demonstrate that you have learned to use the tools from the assignments.

Etiquette Communications in class, with instructors, and online are expected to be professional and polite.

Generative AI Policy Using generative AI, with attribuiton, is allowed in this course. It won't be able to do the work you need to do for the projects, but it can help you create more professional reports – especially if technical writing in Engish is not your strength. This being the case, there is no reason your reports should be poorly written. Watch out, however, that the AI doesn't insert made-up facts into your work. Understanding of the projects will be tested in exams.

Additional Information and University Policies Please visit https://provost.nmsu.edu/faculty-and-staff-resources/syllabus/policies for university policies and student services, including Discrimination and Disability Accommodation, academic misconduct, student services, final exam schedule, grading policies and more.