NORTHERN ARIZONA UNIVERSITY

School of Informatics, Computing, and Cyber Systems

CYB 310 **Malware Analysis** Syllabus

Term	Class No.	Section	Units	Days & Times	Room	Mode
SP2021	CYB310	ONLINE	3	N/A	N/A	Online

Enrollment Requirements

Pre-requisites: (CYB 136, MAT 226, and CS 205) with grades of C or better.

Course Website

http://bblearn.nau.edu

Instructor(s)

Dr. Alex Groce
Email: alex.groce@nau.edu
Office Hours: TBD

Catalog Text

Introduction to reverse engineering techniques for the identification, classification, and analysis of malware using disassembly, virtual machines, static analysis, and dynamic analysis.

Course Purpose

This course prepares students to understand and defend against malware using static and dynamic analysis techniques. Topics include disassembly, debugging, network analysis, anti-reverse-engineering, privilege escalation, and persistence. The course requires prior experience with software development and network security. This course provides a foundation in malware analysis, which motivates CYB 410 Secure Software and develops critical skills needed in CYB 486C Capstone. By developing the skills to understand and analyze extant malware, students also learn how software exploits can be discovered and can be guarded against in software engineering practice. This is a required course in the B.S. in Cybersecurity curriculum. This class also directly supports several program student outcomes through its subject matter, student learning, activities, and assessment (student outcomes 1, 2, and 6).

Course Student Learning Outcomes

Upon successful completion of this course, students will be able to demonstrate the following competencies:

- **LO1.** Describe major classes of malware and common malware propagation strategies;
- **LO2.** Select and apply static analysis techniques to malware using common disassembly and binary inspection tools;
- **LO3.** Select and apply dynamic analysis techniques to malware using virtual machines, debugging, break points, process monitoring, and network monitoring;
- **LO4.** Understand how to defend against malware behaviors such as credential stealing, privilege escalation, and persistence; and
- **LO5.** Draw inferences on the meaning of network data as a signature of malware activity.

Program Student Outcomes supported by this class

This course directly supports the following program student outcomes in the CYB program assessment and improvement plan:

- **SO1.** Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
- **SO2.** Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- **SO3.** Communicate effectively in a variety of professional contexts.
- **SO5.** Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline.
- **SO6.** Apply security principles and practices to maintain operations in the presence of risks and threats.

Assignments / Assessments of Course Student Learning Outcomes

Learning outcomes are assessed through a variety of means: A midterm and final exam assess student ability to describe and explain foundational concepts in malware analysis (LO1) and specific malware analysis techniques and concepts (LO2-LO5).

Individual and team homework assignments assess student ability to synthesize and analyze malware analysis concepts, methods, problem-solving.

Discussion forums will be a part of your participation grade. There will be a prompt each week, with a specific, rubric-driven requirement for participation. There will also be a separate general participation grade that is focused on participation in a professor-lead discussion that will introduce the week's content in an interactive (though asynchronous) fashion. The participation grade may also factor in (positively) personal interaction with the professor and other contributions.

Grading System

A weighted sum of assessment components is used to determine your final grade in the course:

- Discussion Boards: 10% (weekly prompts)
- Participation in "Class Time Thread": 10% for participation in the weekly content thread
- Midterm Exam: 15%
- Homework assignments (3): 45%
- Final Exam: 20%

Grades will be assigned using the weighted sum described above using this scale:
A $\geq$ 90%, **B** $\geq$ 80%, **C** $\geq$ 70%, **D** $\geq$ 60%, **F** $<$ 60%.

There is no "curve". Each student's grade is based on their own outcomes assessments and not affected by the grades of other students. Extra credit opportunities may present themselves throughout the semester and will be announced during class meetings. Mistakes in grading to happen, and students are encouraged to discuss such concerns with the instructor during office hours.

Readings and Materials

Students will be required to purchase a textbook for this class:

Practical Malware Analysis by Michael Sikorski and Andrew Honig. 2012. ISBN: 1-59327-290-1

Students will also need access to a computer with the following software tools:

- GCC suite
- IDA Pro
- OllyDbg
- WinDbg
- VMWare Fusion or Player (and a Windows VM)

Class Outline and Tentative Schedule

The course topics and a tentative schedule serve as an outline for the class:

	Dates	Topics	Reading	Assignment
Week 1	1/11-1/17	An introduction to malware analysis (part 1)	PMA ch 1-2	Forum 1
Week 2	1/18-1/24	An introduction to malware analysis (part 2)	PMA ch 3	Forum 2
Week 3	1/25-1/31	x86 Disassembly (part 1)	PMA ch 4	Forum 3 HW 1
Week 4	2/1-2/7	x86 Disassembly (part 2)	PMA ch 4	Forum 4
Week 5	2/8-2/14	Advanced static analysis (part 1)	PMA ch 5-7	Forum 5
Week 6	2/15-2/21	Advanced static analysis (part 2)	PMA ch 5-7	Forum 6
Week 7	2/22-2/28	Debugging techniques	PMA ch 8	Forum 7
Week 8	3/1-3/7	Midterm review and midterm exam		
Week 9	3/8-3/14	Advanced dynamic analysis (part 1)	PMA ch 9	Forum 9 HW 2
Week 10	3/15-3/21	Advanced dynamic analysis (part 2)	PMA ch 10	Forum 10
Week 11	3/22-3/28	Malware behavior	PMA ch 11-12	Forum 11
Week 12	3/29-4/4	Malware signatures	PMA ch 13-14	Forum 12
Week 13	4/5-4/11	Anti-disassembly and anti-debugging	PMA ch 15-16	Forum 13 HW 3
Week 14	4/12-4/18	Anti-VM, packers, and unpacking	PMA ch 17-18	Forum 14
Week 15	4/19-4/25	Special topics (shellcode, C++, 32 vs 64-bit)	PMA ch 19-21	Forum 15
Week 16	4/26-4/29	Final exam		

*No Forum 8

Due dates for quizzes and homework are posted on BBLearn. Please check BBLearn frequently for updates.

Course Policies

The following policies will apply to this course:

- Students who have not completed the prerequisite(s) for this course, or who do not participate in the first week of class may be administratively dropped from the course.
- The makeup and late work policies are as follows:
  - Quizzes: No make-ups or late submissions allowed.
  - Homework: No make-ups or late submissions allowed.
  - Exams: Make-up exams will be given only in the case of a documented emergency supported by appropriate documentation **and** with approval from the instructor. Make-up exams may be considerably different than the original exam. Make-up exams must be taken within 3 business days of the original exam. Exams are proctored with the ProctorU system.

- Cheating and plagiarism are strictly prohibited. All academic integrity violations are treated seriously. All work you submit for grading must be your own. You are encouraged to discuss the intellectual aspects of assignments with other class participants. However, each student is responsible for formulating solutions independently and in their own words. Academic integrity violations may result in penalties including, but not limited to, a zero on the assignment, a failing grade in the class, or expulsion from NAU.
- Grades will be entered in BBLearn but your final grade will be calculated in Excel using the grading system described above and then entered in LOUIE. Your final course grade will **not** necessarily appear in BBLearn. Please check LOUIE for your final grade.
- The Academic Success Centers offer free tutoring and academic support to improve your study skills and review course material in a number of engineering and math courses. You can schedule an appointment by visiting nau.edu/asc, calling the Academic Success Center at 928-523-7391 or swinging by Dubois Center room 140.
- Email to the instructor and teaching assistants must be respectful and professional. Specifically, all emails should:
    - Contain a salutation, (for example, “Dear Dr. Palmer”)
    - Contain a closing, (for example, “Best, Jane Doe”)
    - Use complete sentences and correct grammar including correct usage of lowercase and uppercase letters. Composing emails on a mobile device is **not** an excuse for poor writing.
    - The body of your message should also be respectful and explain the full context of the query.
    - The subject should be prefixed with “INF110” so that the message can be easily identified. The subject should also use lower case and upper case correctly.
    - Although email will typically be answered quickly, you should allow up to three (3) business days for a response.
    - If you have a question that would require a long response or you have a lot of questions, please come to office hours or schedule an appointment with the instructor.
- Visiting the instructor(s) during office hours is encouraged! I am happy to talk about the class, careers, research, and topics related (even loosely) to this course.

Appendix A. UNIVERSITY POLICY STATEMENTS

COVID-19 Requirements and Information

The following statements in red are specific to NAU's response to the COVID-19 situation. The requirements outlined below are mandatory until further notice. They are based upon current public health conditions and guidance and may change as circumstances warrant or new information becomes available. Additional information about the University's response to COVID-19 is available from the **Jacks are Back!** web page located at https://nau.edu/jacks-are-back/lumberjack-responsibilities.

FACE COVERING AND PHYSICAL DISTANCING REQUIREMENTS
Appropriate face masks or other suitable face coverings must be worn by all individuals when present in classrooms, laboratories, studios, and other dedicated educational spaces. To maximize the benefits of physical distancing as an important strategy to help reduce community transmission of the SARS-CoV-2 virus, instructors may implement mandatory student seating arrangements or specific seat assignments. Instructors may remove students who do not cooperate with these requirements from the instructional space in the absence of an approved accommodation arranged through Disability Resources. Failing to comply with these requirements will constitute a violation of the university's *Disruptive Behavior in an Instructional Setting* policy available at https://nau.edu/university-policy-library/disruptive-behavior.

USE NAUFLEX TO HELP MAINTAIN PHYSICAL DISTANCING
NAUFlex (available at https://nau.edu/nauflex/student) is designed to help all students to actively participate in their coursework during the required day and time of a course, even when they are not physically present in the classroom. This course design model allows students to be fully engaged with faculty and peers and receive the high-quality educational experience for which NAU is known.

CLASS SESSION RECORDINGS FOR STUDENTS AND FACULTY USE ONLY
Certain class sessions may be audio or video recorded to help reinforce live instruction during the COVID-19 pandemic. These recordings are for the sole use of the instructor and students enrolled in the course. Recordings will be stored in approved, accessible repositories. By enrolling, students agree to have their image and classroom statements recorded for this purpose, to respect the privacy of their fellow students, and university-owned intellectual property (including, but not limited to, all course materials) by not sharing recordings from their courses. Questions regarding restrictions on the use of classroom audio or video recordings may be addressed to the appropriate academic unit administrator.

Syllabus Policy Statements

ACADEMIC INTEGRITY

NAU expects every student to firmly adhere to a strong ethical code of academic integrity in all their scholarly pursuits. The primary attributes of academic integrity are honesty, trustworthiness, fairness, and responsibility. As a student, you are expected to submit original work while giving proper credit to other people's ideas or contributions. Acting with academic integrity means completing your assignments independently while truthfully acknowledging all sources of information, or collaboration with others when appropriate. When you submit your work, you are implicitly declaring that the work is your own. Academic integrity is expected not only during formal coursework, but in all your relationships or interactions that are connected to the educational enterprise. All forms of academic deceit such as plagiarism, cheating, collusion, falsification or fabrication of results or records, permitting your work to be submitted by another, or inappropriately recycling your own work from one class to another, constitute academic misconduct that may result in serious disciplinary consequences. All students and faculty members are responsible for reporting suspected instances of academic misconduct. All students are

encouraged to complete NAU's online academic integrity workshop available in the E-Learning Center and should review the full *Academic Integrity* policy available at https://policy.nau.edu/policy/policy.aspx?num=100601.

COURSE TIME COMMITMENT

Pursuant to Arizona Board of Regents guidance (ABOR Policy 2-224 – *Academic Credit*), for every unit of credit, a student should expect, on average, to do a minimum of three hours of work per week, including but not limited to class time, preparation, homework, and studying.

DISRUPTIVE BEHAVIOR

Membership in NAU's academic community entails a special obligation to maintain class environments that are conductive to learning, whether instruction is taking place in the classroom, a laboratory or clinical setting, during course-related fieldwork, or online. Students have the obligation to engage in the educational process in a manner that does not interfere with normal class activities or violate the rights of others. Instructors have the authority and responsibility to address disruptive behavior that interferes with student learning, which can include the involuntary withdrawal of a student from a course with a grade of "W". For additional information, see NAU's *Disruptive Behavior in an Instructional Setting* policy at https://nau.edu/university-policy-library/disruptive-behavior.

NONDISCRIMINATION AND ANTI-HARASSMENT

NAU prohibits discrimination and harassment based on sex, gender, gender identity, race, color, age, national origin, religion, sexual orientation, disability, or veteran status. Due to potentially unethical consequences, certain consensual amorous or sexual relationships between faculty and students are also prohibited. The Equity and Access Office (EAO) responds to complaints regarding discrimination and harassment that fall under NAU's *Safe Working and Learning Environment* (SWALE) policy. EAO also assists with religious accommodations. For additional information about SWALE or to file a complaint, contact EAO located in Old Main (building 10), Room 113, PO Box 4083, Flagstaff, AZ 86011, or by phone at 928-523-3312 (TTY: 928-523-1006), fax at 928-523-9977, email at equityandaccess@nau.edu, or via the EAO website at https://nau.edu/equity-and-access.

TITLE IX

Title IX is the primary federal law that prohibits discrimination on the basis of sex or gender in educational programs or activities. Sex discrimination for this purpose includes sexual harassment, sexual assault or relationship violence, and stalking (including cyber-stalking). Title IX requires that universities appoint a "Title IX Coordinator" to monitor the institution's compliance with this important civil rights law. NAU's Title IX Coordinator is Pamela Heinonen, Director of the Equity and Access Office located in Old Main (building 10), Room 113, PO Box 4083, Flagstaff, AZ 86011. The Title IX Coordinator is available to meet with any student to discuss any Title IX issue or concern. You may contact the Title IX Coordinator by phone at 928-523-3312 (TTY: 928-523-1006), by fax at 928-523-9977, or by email at pamela.heinonen@nau.edu. In furtherance of its Title IX obligations, NAU will promptly investigate and equitably resolve all reports of sex or gender-based discrimination, harassment, or sexual misconduct and will eliminate any hostile environment as defined by law. Additional important information about Title IX and related student resources, including how to request immediate help or confidential support following an act of sexual violence, is available at http://nau.edu/equity-and-access/title-ix.

ACCESSIBILITY

Professional disability specialists are available at Disability Resources to facilitate a range of academic support services and accommodations for students with disabilities. If you have a documented disability, you can request assistance by contacting Disability Resources at 928-523-8773 (voice), 928-523-6906 (TTY), 928-523-8747 (fax), or dr@nau.edu (e-mail). Once eligibility has been determined, students register with Disability Resources every semester to activate their approved accommodations. Although a student may request an accommodation at any time, it is best to initiate the application process at least four weeks before a student wishes to receive an accommodation. Students may begin the accommodation process by submitting a self-identification form online at https://nau.edu/disability-resources/student-eligibility-process or by contacting Disability Resources. The Director of

Disability Resources, Jamie Axelrod, serves as NAU's Americans with Disabilities Act Coordinator and Section 504 Compliance Officer. He can be reached at jamie.axelrod@nau.edu.

RESPONSIBLE CONDUCT OF RESEARCH

Students who engage in research at NAU must receive appropriate Responsible Conduct of Research (RCR) training. This instruction is designed to help ensure proper awareness and application of well-established professional norms and ethical principles related to the performance of all scientific research activities. More information regarding RCR training is available at https://nau.edu/research/compliance/research-integrity.

MISCONDUCT IN RESEARCH

As noted, NAU expects every student to firmly adhere to a strong code of academic integrity in all their scholarly pursuits. This includes avoiding fabrication, falsification, or plagiarism when conducting research or reporting research results. Engaging in research misconduct may result in serious disciplinary consequences. Students must also report any suspected or actual instances of research misconduct of which they become aware. Allegations of research misconduct should be reported to your instructor or the University's Research Integrity Officer, Dr. David Faguy, who can be reached at david.faguy@nau.edu or 928-523-6117. More information about misconduct in research is available at https://nau.edu/university-policy-library/misconduct-in-research.

SENSITIVE COURSE MATERIALS

University education aims to expand student understanding and awareness. Thus, it necessarily involves engagement with a wide range of information, ideas, and creative representations. In their college studies, students can expect to encounter and to critically appraise materials that may differ from and perhaps challenge familiar understandings, ideas, and beliefs. Students are encouraged to discuss these matters with faculty.

Last revised July, 2020