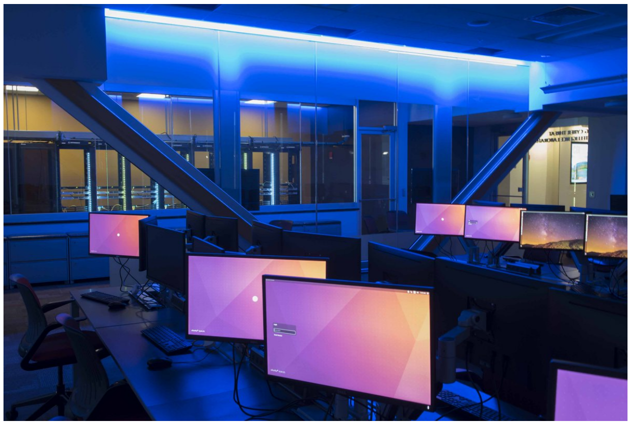
Welcome to
Advanced Cybersecurity!

CIT 485

Meets on Tuesdays and Thursdays 10:50-12:05 via Zoom.



Dr. James Walden

waldenj@nku.edu (859) 572-5571

http://faculty.cs.nku.edu/~waldenj

Table of Contents

1 SUMMARY

Advanced Cybersecurity builds on your prior knowledge of computer systems and cybersecurity to help you understand both how to hack and how to detect hacking activities. This class is organized around the cyber kill chain model, which describes the phases of a cyber attack from reconnaissance through exfiltration of data. Students will learn how attackers carry out attacks, so that they can learn how to detect and stop attacks at each step in the chain. While students run attacker tools to scan the network or launch exploits on one system, they will simultaneously be collecting data on those attacks using network monitoring tools on another system in order to understand what actual attacks look like on the network and in server logs. Class sessions will combine hands-on lab activities with short discussions and lectures.

1.1 Prerequisites

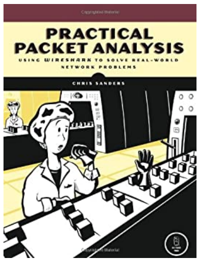
CIT 371 and either CIT 285 or CIT 480
Students should be familiar with cybersecurity terminology and concepts, such as access control, authentication, cryptography, and firewalls. You should be able to create, edit, and manage files using the Linux command shell. You should also know the OSI and TCP/IP network models and be familiar with using Wireshark to collect and analyze network packets.

1.2 Student Learning Outcomes

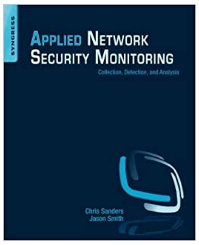
After successfully completing this course, you should be able to

1. Understand how to collect different types of network security data.
2. Analyze captured packets, network flows, logs, and IDS alerts to find indicators of compromise.
3. Identify the causes and impact of security incidents by following a well defined analysis process.
4. Compose a report that describes and supports analysis of a security incident with evidence.
5. Describe relevant cybersecurity laws and compliance requirements and their impact on IT and security operations.
6. Investigate and evaluate unfamiliar topics within cybersecurity.

1.3 Required Textbooks


PRACTICAL PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS

Practical Packet Analysis, 3rd Edition by Chris Sanders. No Starch Press. 2017.


SYNGRESS
APPLIED NETWORK SECURITY MONITORING
Collection, Detection, and Analysis
Chris Sanders
Jason Smith

Advanced Network Security Monitoring by Chris Sanders and Jason Smith. Syngress. 2013.

2 Course Topics

We will cover the following topics this semester. A detailed schedule of topics and what needs to be done for each class meeting with due dates can be found on the class web site.

1. Threats, Attacks, Vulnerabilities
2. Cyber Crime
3. Phishing
4. Network Data Collection
5. Passive Reconnaissance
6. Active Reconnaissance
7. Exploitation
8. Malware
9. Document Analysis
10. Incident Response
11. Layer 2 Analysis
12. Network Layer analysis
13. Denial of Service
14. Transport Layer analysis
15. Application Layer Analysis
16. Network Flow Analysis
17. Intrusion Detection
18. Log Analysis
19. Policy and Compliance
20. Legal Issues

3 What Can I Expect to Happen During Class?

In order to learn, you will need to be actively engaged with the course content. It's important to complete the readings and videos assigned before each class session, so that you will be prepared to work on hands-on lab activities during class. Class will be broken up into multiple segments, including lab activities, short lectures, and small group activities or discussions. Because we learn best when engaged with others, you will work with a partner or small group almost every class period. Most in-class activities will be keyboard based using virtual networks on NKU's vSphere system, but some will be pencil and paper based.

4 Technology Used in This Class

As a virtual class, class meetings will be held in Zoom meetings, with breakout rooms being used for small group activities and labs. Students will need a webcam and microphone to participate in class meetings. During class meetings, students can ask questions using Zoom's chat function. While I do not have regular office hours for online classes, I will schedule Zoom sessions to review course materials and provide additional help and I am available for one-on-one meetings by appointment.

Each student will have their own virtual lab environment, consisting of three virtual machines (VMs), labeled Seed, Attacker, and Server. Early labs will use only one VM, while later labs will use two or three VMs. Each VM has the same configuration based on Ubuntu Linux 16.04, with specific changes made so that course labs will work on them. The virtual lab environment is accessed through the NKU College of Informatics vSphere system.

vSphere is available through a web interface at https://coivcenter.hh.nku.edu. NKU's vSphere system can only be accessed while using NKU's Virtual Private Network (VPN). If you have already installed and configured the NKU VPN, you can use your current installation. If you have not installed NKU's VPN yet, go to https://vpn.nku.edu to download and install the VPN software.

5 Available Help and Support

I am available to help you with the class via e-mail, discussion forums, scheduled Zoom sessions, and appointments. I will respond to questions within one business day, unless an emergency arises. Please see the Communication Policy below for how to best get answers to your questions.

Cybersecurity content resources specific to this course can be found via the Resources page on the class web site, while cybersecurity resources for the university and local area can be found on the web site for NKU's http://cis.nku.edu/.

NKU's tutoring program and writing center are both available online at https://inside.nku.edu/plus/tutoring/online.html. Help and resources for NKU's learning management system are available from https://inside.nku.edu/cite/technologyresources/Canvas_student.html. The student technology guide, including support for student services, can be found at https://inside.nku.edu/it/student-tech-guide.html.

6 Grading

Your grade in this course will be based on the following classes of assessments, each of which counts for the specified percentage of your semester grade.

Assignments (30%) Assignments include a variety of activities, including conducting investigations of system and network data and researching security tools. There will be 3 assignments, each worth 10% of your semester grade. Each assignment will be expected to require about 8 hours to complete on average. Assignments are due on the date that they are posted on the schedule.

Research Project (30%) A semester-long research project on a cybersecurity topic of current interest. It includes multiple deliverables, which are described below in the Research Paper section.

Midterm Exam (20%) The take-home midterm examination will cover all material up until the class period during which it is given. It will consist of a combination of short answer and analysis questions, with the analysis questions involving applying the techniques learned during in-class labs and assignments. Students will have several days to complete the midterm exam.

Final Exam (20%) A comprehensive examination covering all of the material in the course given. The final exam will be a take-home exam in the same format as the midterm exam. It will be given during the last class meeting and will be due during finals week.

Your letter grade will be based on your percentage score from the sum of the assessment areas above as shown in the table below.

Grade	Percent	Grade	Percent
A	93-100	C+	77-80
A-	90-93	C	73-77
B+	87-90	C-	70-73
B	83-87	D+	67-70
B-	80-83	D	60-67
		F	0-60

Midterm grades will be provided to all students in 100 - 400 level courses, except in cases where the Department Chair and Dean have waived midterm grade reporting for pedagogical reasons. Midterm grades are only an estimate of performance as of the middle of the semester and are not an absolute predictor of final performance. Mid-term grades will be posted in myNKU by the deadline in the Academic Calendar.

7 Research Project

The research project is a semester long research project on a cybersecurity topic of current interest. The project has multiple deliverables, each of which will appear as its own assignment on Canvas. These deliverables are designed to ensure that you are on track to complete a high quality paper and presentation by the end of the semester. The five deliverables are:

1. Topic Proposal
2. Annotated Bibliography
3. Draft Paper
4. Final Presentation
5. Final Paper

The grade for the research project will be divided as follows: the topic proposal is worth 1%, the annotated bibliography 6%, the draft paper 5%, the presentation 6%, and the final paper 12% of the total semester grade. The research project as a whole is worth 30% of the semester grade.

8 Participation Policy

You are expected to be an active participant in class discussions and other in-class activities. To do this, you must prepare by completing the readings and other learning activities specified on the class schedule before coming to class. Class activities have been designed to help prepared students achieve the class learning outcomes. Missing class, not actively participating, and not being prepared will negatively affect your ability to learn course content.

9 Communication Policy

I'm here to help you learn, and I have a few communication guidelines to make the course run as smoothly as possible. Questions about course content or technology should be asked in the General Questions & Answers forum, so that other students can provide and benefit from posted answers. Personal matters should be discussed with me through e-mail.

When asking questions on a discussion forum or by e-mail, be sure to include:

- A subject that provides a summary of your question. Include the class number at the beginning of the subject for e-mail messages.
- A detailed description of the problem. Specify precisely on which assignment, virtual machine, user account, and software the problem occurred and provide a detailed list of steps needed to reproduce the problem. Include the full text of any error messages.
- The message should close with your full name.

I will answer forum questions within one business day unless a student has already provided a correct answers. I will respond to e-mail messages within one business day except in the event of an emergency.

Students should check the class web site and NKU e-mail accounts for university-wide and class-specific announcements 24 hours before each class period.

10 Late Work/Missed Exam Policy

All students are expected to complete learning tasks on schedule. It is important to stay on track with your assignments. This is an important skill in the workplace and will help you feel less stressed. Being able to meet deadlines and juggle many tasks are important career and life skills. Thus, you will need to complete all exams, labs, and assignments according to the class schedule. However, I recognize that personal circumstances may at times make it difficult or impossible to complete a learning task on schedule. If you have a personal situation that prevents you from completing a task on time, you will need to discuss this with me prior to the due date if possible, or as soon as it becomes possible, so that we can develop a plan. Extensions are at my discretion. If an extension is provided, it is important to know that the format or content of an assignment or exam may be modified.

11 Registrar Withdrawal Information

Students sometimes need to withdraw from a course for personal or academic reasons. If you do encounter difficulties with the course, please contact me prior to withdrawing. NKU's Fall 2020 Academic Calendar includes deadlines for withdrawing for a course.

12 Academic Integrity Policy

Academic integrity benefits everyone in our community. It not only helps you reach the real goal of this class–learning–but also allows for the university and degree program to be perceived positively by others, including your future colleagues and employers. When students are dishonest, they lose out on valuable learning that will help them perform well in their career. Academic dishonesty is any attempt by a student to gain academic advantage through dishonest means or to help another student in gaining an unfair advantage. Academic integrity is important whether the work is graded or ungraded, group or individual, written or oral.

The Student Honor Code is a commitment by students of Northern Kentucky University, through their matriculation or continued enrollment at the University, to adhere to the highest degree of ethical integrity in academic conduct. It is a commitment individually and collectively that the students of Northern Kentucky University will not lie, cheat, or plagiarize to gain an academic advantage over fellow students or avoid academic requirements.

Students, faculty, staff, and administrators at NKU strive to achieve the highest standards of scholarship and integrity. Any violation of the Student or Graduate Student Honor Codes is a potentially serious offense because it threatens the quality of scholarship and undermines the integrity of the community. All NKU faculty members are asked to report incidents of academic misconduct to the office of Student Conduct Rights and Advocacy. While academic in scope, a violation of the NKU Honor Code may be considered a violation of the NKU Code of Student Rights and Responsibilities and will follow the adjudication processes described therein.

Through the NKU Honor Code, students who are responsible for academic dishonesty may receive sanctions, including, but not limited to, a final grade of F, or removal from the course in which the violation occurs. Repeated violations of the NKU Honor Code, or when suspension or expulsion from NKU may be a possible outcome of the violation, the incident will be referred to the office of Student Conduct, Rights and Advocacy.

13 Credit Hour Policy

In accordance with federal policy, NKU defines a credit hour as the amount of work represented in the achievement of student learning outcomes (verified by evidence of student achievement) that reasonably approximates one hour (50 minutes) of classroom instruction and a minimum of two hours of out-of-class student work. For every course credit hour, a typical student should expect to spend at least three hours per week of concentrated attention on course-related work including, but not limited to, class meeting time, reading, reviewing, organizing notes, studying and completing assignments. At least an equivalent amount of time is expected for other academic activities such as online courses, laboratory work, internships, practica, studio work and other academic work leading to the award of credit hours.

Estimates of the time required for a typical student to complete course expectations are:

In-Class (2 day x 75 min x 15 weeks)	37.5 hours
Class Prep (105 min x 15 weeks)	26.25 hours
Assignments (8 hours x 3 assignments)	24 hours
Research Paper	40 hours
TOTAL	127.75 hours

14 NKU Policies

14.1 Accomodations Due to Disability

The University is committed to making reasonable efforts to assist individuals with disabilities in their efforts to avail themselves of services and programs offered by the University. To this end, Northern Kentucky University will provide reasonable accommodations for persons with documented qualifying disabilities. If you have a disability and feel you need accommodations in this course, you must present me a letter from the Office for Student Accessibility (OSA, SU 303) indicating the existence of a disability and the suggested accommodations. More information on OSA can be found at https://inside.nku.edu/osa.html.

14.2 Changes in the Syllabus

The syllabus is a projection of what the instructor anticipates for the course. The instructor has the right to modify the syllabus in order to adjust to changing circumstances.

14.3 Other Information

For information on university-wide policies governing students, please see the University Common Syllabus on your course Canvas site.