CIT 485–Advanced Cybersecurity

Fall 2018 (MW 2:00-3:15 in GH 224)

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

1 Instructor Information

Name	James Walden
E-mail	*waldenj@nku.edu*
Office	GH 526
Phone	(859) 572-5571

Office Hours

MW	1:00-2:00pm
M	3:15-4:30pm
M	9:00-10:00pm
W	3:15-4:00pm
also	by appt

2 Summary

Students will learn the fundamentals of cyber defense and cyber operations, with a focus on network forensics and incident response. The class will also include web application security and discussions of the legal and ethical issues around cybersecurity. The class will focus on hands-on activities and investigations. Students should be familiar with fundamental security concepts as well as network protocols and the Linux command line.

Prerequisites: CIT 371; CIT 285 or CIT 480

Textbooks:

- Chris Sanders. *Practical Packet Analysis, 3rd Edition*. No Starch Press. 2017.
- Chris Sanders and Jason Smith. *Advanced Network Security Monitoring*. Syngress. 2013.

3 Student Learning Outcomes

By the end of the course, a successful student should be able to

1. Describe common security threats and attacks, including malware.
2. Understand how to collect different types of network security data.
3. Analyze captured packets, network flows, and IDS alerts to find indicators of compromise.
4. Identify causes and impact of security incidents by following a well defined analysis process.
5. Compose a report that describes and supports analysis of a security incident with evidence.
6. Explain web application technologies and the security issues associated with them.
7. Describe relevant cybersecurity laws and compliance requirements and their impact on IT and security operations.

4 COURSE TOPICS

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

5 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 (40%)	Most assignments will focus on analyzing network security data to identify and investigate security incidents. Each student will have their own virtual network to use for this type of analysis. Assignments will be graded based on a combination of the accuracy of conclusions made, the documentation of the process through which the conclusions were reached, and the quality of writing. 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.
Class Participation (10%)	All students are expected to have completed the assignment due during the current class period and be ready to discuss the problems they encountered and the solutions they produced.
Midterm Exam (25%)	The midterm examination will cover all material up until the class period during which it is given. It will consist of a set of short answer and essay questions, most of which will be similar to the questions assigned as class preparation exercises. You will have a 75-minute period during class to complete the exam. The date is on the class schedule web page.
Final Exam (25%)	A comprehensive examination covering all of the material in the course given during finals week in a two hour period. The format will be the same as that of the midterm exam. The date is on the class schedule web page and can also be found on the NKU final exam schedule.

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

In accordance with university policy, mid-term grades will be available online through MyNKU and are

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

issued to all undergraduate students. These grades are not part of your permanent record and will be replaced when final grades are submitted. Remember: mid-term grades do not guarantee a good or bad class grade; they reflect the current level of performance and can be altered by the quality of subsequent work.

6 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 (1 day x 60 min x 15 weeks)	15 hours
Weekly assignments (8 hours x 10 weeks)	80 hours
Final Project	40 hours
TOTAL	135 hours

7 RESOURCES AND REFERENCES

Information security resources specific to this course can be found via the Resources link on the class web site, while information security resources for the university and local area can be found at the Center for Information Security page, http://cis.nku.edu/.

8 TECHNOLOGY REQUIREMENTS

Students will need to use NKU's vSphere environment for most assignments.

9 NON-ATTENDANCE POLICY

NKU students are expected to attend the first scheduled class session of each course for which they are enrolled. If a student does not attend the first day of class, the instructor may drop the student for non-attendance.

Students who know they will be absent must contact their instructor(s) prior to the first class meeting to explain their absence and request to remain enrolled in the course.

10 HONOR CODE

This 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.

Additional information is available at: https://inside.nku.edu/scra.html#policies.

11 STUDENTS WITH DISABILITIES

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 a letter to me from the Disability Programs and Services Office (SU 303), indicating the existence of a disability and the suggested accommodations.More information can be found at http://disability.nku.edu.