CIT 481–Cybersecurity Capstone

Fall 2017 (M 6:15-7:30 in GH 312)

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

Instructor Information

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

Office Hours

M	7:30-8:30pm
W	2:00-3:00pm
TR	10:00-10:40am
also	by appt

Summary

Description	:	Students will learn the fundamentals of cyber operations and incident response, with a focus on network security monitoring. The focus of the class is on hands-on assignments and a final incident handling project. The class meets once per week in person for students to discuss assignments and their projects. Students should be familiar with fundamental security concepts as well as network protocols and the Linux command line.
Prerequisites	:	CIT 480: Securing Computer Systems; STA 205, 212, or 250

Student Learning Outcomes

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

1. Understand how to collect different types of network security data.
2. Analyze captured packets, network flows, and IDS alerts to find indicators of compromise.
3. Identify causes and impact of security incidents by following a well defined analysis process.
4. Write a security incident report.

Course Topics

1. Incident Response
2. Network Data Collection
3. Network Layer analysis
4. Transport Layer analysis
5. Application Layer Analysis
6. Network Flow Analysis
7. The Analysis Process
8. Signature Analysis
9. Indicators of Compromise
10. Reputation
11. Anomaly Based Detection
12. Honeypots

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 (50%)	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.
Final Project (40%)	The final project is an in-depth analysis of a security incident using all of the analysis techniques and tools covered in the course. Students will have several weeks to perform the analysis, write the incident report, and develop a presentation base don the report. Students will make a presentation based on their project during the final exam period.

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

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	F	0-70
B-	80-83		

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

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

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/.

TECHNOLOGY REQUIREMENTS

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

STUDENTS WITH DISABILITIES

Students with disabilities who require accomodations (Academic adjustments, auxiliary aids or services) for this course must register with the Disability Services Office. Please contact the Disability Service Office immediately in the University Center, Suite 320 or visit the website at http://disability.nku.edu/ for more information. Verification of your disability is required in the Disability Services Office for you to receive reasonable academic accomodations.

HONOR CODE

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.

The purpose of the Honor Code is to establish standards of academic conduct for students at Northern Kentucky University and to provide a procedure that offers basic assurances of fundamental fairness to any person accused of violations of these rules. Each Northern Kentucky University student is bound by the provisions of the Honor Code and is presumed to be familiar with all of its provisions. Students also should aspire to conduct themselves in a manner that is consistent with the highest degree of ethical integrity in all matters, whether covered in the Honor Code or not. The success of this commitment begins in the diligence with which students uphold the letter and the spirit of the Honor Code. Students may view the complete honor code at http://deanofstudents.nku.edu/policies/student-rights.html#policies.

STUDENT EVALUATIONS

Northern Kentucky University takes Instructor and Course Evaluations very seriously as an important means of gathering information for the enhancement of learning opportunities for its students. It is an important responsibility of NKU students as citizens of the University to participate in the instructor and course evaluation process. During the two weeks prior to the end of each semester's classes, you will be asked to reflect upon what you have learned in this course, the extent to which you have invested the necessary effort to maximize your learning, and the role your instructor has played in the learning process. It is very important that you complete the online evaluations with thoughtfully written comments.

Student evaluations of courses and instructors are regarded as strictly confidential. They are not available to the instructor until after final grades are submitted, and extensive precautions are taken to prevent your comments from being identified as coming from you. Students who complete an evaluation for a particular course (or opt out of doing so in the evaluation) will be rewarded for their participation by having access to their course grade as soon as that grade is submitted by the instructor. On the other hand, any student who does not complete the course evaluation (or opt out of doing so in the evaluation) should expect to incur a two week delay in access to his or her course grade beyond the university's official date for grade availability. To complete online evaluations go to http://eval.nku.edu/. Click on "student login" and use the same username and password as used on campus.

In addition, you should be aware that:

- Evaluations can effect change in courses. Evaluations without comments are less valuable and less credible than those filled out thoughtfully. Comments that are expressed well are more effective than those that are not.
- Positive feedback is just as important as criticism. Moreover, negative evaluations without any explanation and specifics are not especially useful.
- Once grades are submitted, all evaluations are read not only by the instructor, but also by the instructors department chairperson.
- Evaluations not only provide feedback to your instructor, but also provide information to the department chair for use in performance evaluations. This information affects reappointments, promotions, salaries, and teaching assignments.