CYBR380 : OFFENSIVE INFORMATION WARFARE

College of Graduate and Continuing Studies, Norwich University

Print This Page

Course Description

Welcome to CYBR 380 Offensive Information Warfare. This course is designed to build on the concepts learned in Introduction to Information Warfare to develop a more technical understanding of how computer based attacks work and what techniques are employed by cybersecurity professionals to defend their information systems. In the next 8 weeks we will begin with an introduction to policy and conclude with a comprehensive penetration test of a closed network.

3 Credits

Seminar Description

This course is an introduction to Offensive Information Warfare and the technical means used to execute and defend against attacks. This course will examine the laws and regulations governing Information Warfare and provide hands-on experience in a closed network environment with executing and observing common computer based attacks. Using the NSA Center of Academic Excellence learning objectives and outcomes, students will learn how Offensive Information Warfare is executed at the technical level and the defensive measures cybersecurity professionals use to prevent them. At completion of this course, students will understand and have applied the following principles from the National Security Agency and Department of Homeland Security Information Assurance/Cyber Defense Knowledge Units:

- Cyber Defense
- Cyber Threats
- IA Fundamentals
- Policy, Legal, Ethics, and Compliance
- Network Defense
- Networking Technology and Protocols

PREREQUISITES:

CYBR370 or Permission of Instructor

Course Outcomes and Objectives

The broad objective of this three credit course is to develop an understanding of the laws and policies governing Offensive Information Warfare and provide a technical understanding of computer based attacks through hands-on implementation of exploits in a closed network environment.

Course Outcomes:

1. Understand the laws, policies, and regulations that govern Offensive Information Warfare both globally and as it applies to the Department of Defense.
2. Analyze how computer based attacks work by implementing exploits and observing network and target host activity.

3. Use open source penetration testing tools to perform the seven stages of a cyberspace attack.
4. Employ defense and deception techniques and observe how they allow cybersecurity professionals to deter or defeat cyberspace attacks.
5. Describe potential system attacks and the actors that might employ them
6. Identify malicious actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, and aversion to risk

Learning Objectives:

- Explain the different viewpoints and definitions of Information Warfare
- Describe the spectrum of nation and non-nation state adversaries in Information Warfare
- Discuss how the United States develops Rules of Engagement for its forces conducting Information Warfare
- Indicate how to characterize cyber adversaries by intent and capability
- Summarize how services use TCP ports for communication
- Illustrate how Network Address Translation and Firewalls operate
- Explain the Linux Kernel architecture
- Explain Windows Security Policies
- Identify spoofing methods to obscure source information
- Apply methods used to find open firewall ports using TCP ACK scans
- Distinguish between UDP and ICMP scanning techniques
- Define IDS and IPS evasion techniques
- Search vulnerability databases for exploits
- Explain how brute force password cracking works
- Recall the differences between, viruses, Trojans and rootkits
- Indicate how antivirus systems prevent against application level tools
- Demonstrate how Windows and Linux systems record host event logs
- Demonstrate network tunnels to encrypt communications
- Demonstrate the ability to research a given cyber attack problem and develop a well thought written response citing sources as examples of their conclusions.

Weekly Outline

Week	Topic	Readings	Assignments
Week 01	Introduction to Offensive Information Warfare	Assigned Articles	Discussion, Lab Introduction (ungraded)
Week 02	Networking Fundamentals	Chapters 1-2	Discussion, Lab One
Week 03	Linux and Windows Foundations	Chapters 3-4	Discussion, Lab Two
Week 04	Reconnaissance and Scanning	Chapters 5-6	Discussion, Lab Three
Week 05	Gaining Access	Chapters 7-8	Discussion, Lab Four
Week 06	Maintaining Access	Chapters 10	Discussion, Lab Five
Week 07	Covering Tracks	Chapters 11	Discussion, Lab Six

Week 08	Anatomy of an Attack	Chapters 12	Discussion, FINAL EXAM (Essays)

Required Textbooks

The textbook pages and other readings are all listed in the Weekly Overview under Required Readings.

The textbook for **CYBR380** is:

- **Skoudis, E. & Liston, T. (2006). *Counter hack reloaded: A step-by-step guide to computer attacks and effective defenses*. Pearson Education, Prentice Hall.**

Access to all Required Readings is through links listed in each weeks outline.

Grading Criteria

You will be provided a weekly commentary/lecture and have required readings.

Each week, you will have a variety of discussion forums, written papers, and quizzes to complete and each assignment will be graded based on the category it falls into. Participation in these topics/groups will be evaluated as well.

Grading for the weekly discussions will be based on quality of your posts (initial and response posts). Remember, discussion questions are designed to foster intellectual conversation regarding the subject. Discussion post responses that lack intellectual merit are not acceptable and have no place in this course (i.e. Good job!, Great post!, I agree…..). Grading for the weekly labs will be based upon the percentage of correctly completed tasks. Quizzes and exams are graded in the traditional sense.

As a student in this course, you have a number of responsibilities that will affect the level of learning you achieve. These responsibilities include: 1) working actively to create a challenging and useful learning experience for yourself, your discussion group and the class as a whole; 2) encouraging and supporting the learning of each member of the class in all activities; 3) preparing and participating fully in discussions as well as group and/or class activities; and 4) completing all assigned work on time or making prior arrangements if an absence of late submission is unavailable.

All written academic work must be submitted by the deadline specified in the assignment and late submissions must be telephonically discussed with the instructor. Written work must be formatted in accordance with the *Publication Manual of the American Psychological Association* (6th Edition) and will be graded in accordance with the APA Guidelines for Written Work as detailed in the Norwich University rubric.

Discussion Groups

In this course, you will be assigned to a small discussion group (if class size permits). Each week your group will discuss at least one question; all questions will be graded. You are expected to contribute *a minimum of at least three posts* to each question every week. The quality of your posts and those of your fellow students will create a lively discussion and ensure that a high level of learning takes place.

Your **first** post should be substantive (approximately 150-250 words) and it should be made by **Tuesday** (the earlier you make your initial posts, the more your classmates, and you, will have to work with). Your deadline for first post is Wednesday night after which time you will loose points for the week. It should answer the question using your own experience, if appropriate, and, very importantly, it should refer to the readings of that week, using correct APA citations. You should all conduct additional readings and research beyond the readings and resources provided for each week in order to completely answer the discussion question.

Your **second** two posts should be responses to posts made by your fellow group members. This is a minimum requirement as you are expected to respond to more posts in order to have a lively discussion. Responses such as, “Good point,” or, “I agree,” are not sufficient. Your response posts should be substantive –ask questions, point out additional thoughts, spur deeper insights and thoughts, etc. Posts should build on the course content and add momentum to our collective learning. Disagreement and critical feedback are part of an academic classroom, as is respect for the diversity of opinion. Above all, respect for each other as learners is paramount. Challenging, disrespectful, abusive, or profane language will not be tolerated in any form.

For more information about what is expected in regard to discussion postings, please review the Weekly Discussion Rubric and Discussion Guidelines in the Resource area of this classroom.

Assignments

Written Paper

Week 01 includes a small written paper that asks you to examine a question about offensive warfare.

Weekly Labs

Week 01 begins with an ungraded diagnostic lab to make sure you can access the lab environment and guide you on how to write up your weekly lab reports.

In weeks 02-07 your labs will contain questions based on operating in a Windows or Linux (ADHD) environment. You will use the environment to execute the commands in each question and answer based on expected output. Try to use the environment to answer questions and not resources outside the course such as internet forums. The labs are built to measure your understanding of executing an offensive technique in the ADHD environment and answers may be specific to this course.

If you are stuck on a lab question you can always reach out to the instructor for help. If you can clearly explain what you have done and why you think the tools aren’t working properly, your instructor may be able to provide a hint to get you back on track. Labs are individual efforts and you may not receive help from anyone in or outside of this class.

Discussions

Each week’s discussions consist of questions where you will be required to post one original response and reply to two of your fellow student’s posts. An original post must take a position for or against the weekly question and cite at least two sources. Replies must argue for or against the original post. Pay attention to these discussion questions because they will prepare you to write the final project which will be in the form of a penetration test report.

Clarity, completeness, and evidence of academic rigor are requirements for all posts and replies. I do not have a minimum length requirement, but original posts should be complete in that you argue a point in a methodical fashion using logic to justify your position and sources to back up your claims. Posts should be clear, concise, and well written using proper grammar and spelling. You are not limited to one original post and two replies, and are encouraged to use the weekly discussions to engage your fellow students if something is not clear.

If you are using an outside source that is not the class text or lecture material, provide a citation using APA format and a link if one exists. Above all, be respectful in your posts.

Final Exam (Essay's)

In your final week you are required to write 5 essay responses, one for each phase of a cyber attack. Each essay will be a minimum of 300 words and each will cite at least 3 sources. Students are required to format their essays and their citations using the APA sytle guide.

Students will be given a group of questions to choose from, and in answering those questions you will need to fully explain how an adversary seeks to successfully execute that phase and how a cybersecurity professional could deter or defeat an attack. For full credit, use screenshots and examples from the ADHD environment to demonstrate your point.

Late Work

It is important that writing assignments and discussion posts be completed on time. Extensions of deadlines will be given only for serious extenuating circumstances. In the absence of such extensions, assignments may be downgraded for lateness at the discretion of the instructor.

Extra Credit Submissions

Extra credit submissions and the length of such submissions require advanced approval by your instructor. Instructors are not required to use the grading rubric, or provide rubric scores. Instructors do not have to provide the same level of formal feedback on extra credit submissions as they do on essay assignment, but should provide whatever level of useful feedback is appropriate.

The **maximum** grade based on word-count is 0.005 credit/word, or 5 points per 1,000 words. Thus a student who agrees to submit a 2,000-word essay on a specific topic approved in advance may have **up to** 10 points added to the "Extra Credit" column in the grade book. These points are added to the total points accumulated.

Extra credit assignments cannot be used as a substitute for missed research papers. The way to obtain credit for missed research papers is to request permission to submit the paper late.

Submission Deadlines

Discussions officially close on Saturday of each week at 11:55 PM Eastern time. Posts submitted after that time will not be graded.

Exams are due on their assigned dates at 11:55 PM Eastern time.

Lab documents and papers and the written Paper are due on their assigned dates at 11:55 PM Eastern time.

Grades

Grades will be based the quality and accuracy of problem set solutions, the final programming project, and contributions to the online discussions.

Graded Activity	# Required	% of Grade
Weekly Labs	6	60 %
Discussions & Participation	8	16 %
Written Paper Assignment	1	4 %
Final Exam (Essay's)	1	20 %

Letter grades for the course will be based on the following grading scale:

Letter Grade	Percentage	Grade Point
A	93-100%	4.0

A -	90-92.9%	3.7
B +	87-89.9%	3.3
B	83-86.9%	3.0
B -	80-82.9%	2.7
C +	77-79.9%	2.3
C	75-76.9%	2.0
C -	73-74.9%	1.7
D +	70-72.9%	1.3
D	67-69.9%	1.0
D-	63-66.9%	0.7
F	0-62.9%	0.0

For complete information on the Grading Policy for Bachelor Degree students, please refer to the CGCS Online Catalog (Sub-Section of Catalog on "Grades.")

Academic Honesty and the Norwich University Honor Code

A student must submit work that represents the student's own original analysis and writing. Copying another's work is not appropriate. If the student relies on the research or writing of others, the student must cite those sources. Words or ideas that require citations include, but are not limited to all hardcopy or electronic publications, whether copyrighted or not, and all verbal or visual communication when the content of such communication clearly originates from an identifiable source. While students are encouraged to seek editing feedback, extensive revisions of one's work by another person is considered a lack of academic honesty, as it is representing another student's work as one's own.

For more information see:

Academic Dishonesty
Academic Integrity
Norwich University Honor Code

Copyright Notice

The content of this seminar contains material used in compliance with the U.S. Copyright Law, including the TEACH Act and principles of "fair use." Materials may not be downloaded, saved, revised, copied, printed or distributed without permission other than as specified to complete seminar assignments. Use of these materials is limited to class members for the duration of the seminar only.

Section 504 of the Rehabilitation Act of 1973/ADA

Please consult Appendix H: University Policy - Section 504 of the Rehabilitation Act of 1973/Americans with Disabilities Act (ADA) for instructions on obtaining an accommodation.

Disclaimer: Please note the specifics of this Course Syllabus are subject to change. Students are responsible for abiding by any such changes. Your instructor will notify you of any changes.