

IS406 – CDX Preparation – Spring 2010 - Syllabus

General Course Information

Instructor: Dr. Peter Stephenson, CISSP, CISM, FICAF

Office: Dewey 205

Office Hours: As posted

Phone: University extension 2007, Mobile 802-498-4923

E-mail: pstephen@norwich.edu

AIM: NUCISO

Web site: <http://www2.norwich.edu/pstephen>

Classroom: Cyber Weapons Range War Room

Class Times: W 18:00 – 20:30

Prerequisites: Approval of Instructor

Textbooks: Chained Exploits Whitaker, Andrew, Keatron Evans, Jack B. Voth pub Addison Wesley ISBN0-321-49881-X; Counter Hack Reloaded – 2nd Edition Skoudis, Ed, Tom Liston pub Prentice Hall ISBN 0-13-148104-5

Course Objectives

This course introduces students to the techniques and tools required for network attack and defend. By the time the course is completed students will have been exposed to network attack and penetration, attack modeling, intrusion detection and network defense.

Course Description

This laboratory-based course is designed to make the students knowledgeable of the fundamentals underlying the defense of complicated computing systems and networks through a detailed understanding of network attacks, monitoring and measurement tools and techniques and attack modeling. Students will form two teams – red (attack) and blue (defend) – and will practice network defense and exploitation after which the teams will reverse. Students will learn how to model networks and attacks, simulate the behavior of the network under attack, simulate the results of adding countermeasures to the network, and determining the impact of adding new applications to the network.

Learning Objectives

1. *Terminology.* The student will be able to explain the meaning of terms used to describe common techniques and concepts in network-centric warfare and network attacks and defense.
2. *Advanced Network Protection Concepts.* The student will be able to demonstrate advanced techniques for designing and implementing network protection.

3. *Network Attack Concepts*. The student will be able to use penetration testing tools to develop cyber attacks.
4. *Behavioral and Organizational Issues*. The student will be able to identify and suggest appropriate responses to such “people-based” attack techniques as social engineering.
5. *Social and Ethical Issues*. The student will understand the major social and ethical issues involved in the processes of network-centric warfare.

Specific topic coverage includes:

- Network communications review
- IPV6 introduction
- Penetration testing tools and techniques
- Defensive tools and techniques
- Network-centric warfare concepts
- Attack modeling using attack trees
- Network modeling and simulation with Colored Petri Nets
- Network monitoring tools and techniques
- Attack analysis

Grading and Evaluation Criteria

Your understanding and ability to explain terminology, advanced network protection and attack concepts, behavioral and organizational issues, and social and ethical issues will be measured in the quantity and quality of your answers to our discussions in class, our lab sessions and our red team/blue team exercises.

Grading

Your grade will be determined as follows:

- Lab exercises (4) – 40% (10 points each)
- Analysis projects (2) – 30% (15 points each)
- Final Exam – 30%

Class Requirements

Class Meetings

You are required to attend all class meetings. If you miss a meeting, it is *your responsibility* to obtain notes from a fellow student. Because of the compressed nature of this course and its limited meetings it is critically important that the student attend all class meetings.

Class Participation

The University requires regular attendance by students. Class attendance is useful to the student as a means of acquiring knowledge and clarification, and it is a prerequisite for class participation. Class

participation is the active engagement in questions and answers, partaking in analysis of business situations, and contribution of comments in class sessions.

Keep all of your work until the end of the course. Errors may occur or I or NUoodle may lose your assignment. YOU are responsible for being able to resubmit any paper, quiz or assignment that shows as a zero in the NUoodle grade book.

NUoodle

Because I am occasionally off campus during our class meetings, some of your assignments will be carried out on NUoodle. NUoodle also is the only place where I will communicate with you on-line so it is your responsibility to stay connected to the information there. When I am off campus during a class period we will conduct our classroom discussions there in a forum I will set up for that purpose. Also, your assignments will be posted every week on our NUoodle site.

Academic Dishonesty.

Academic integrity is the pursuit of scholarly activity free from fraud and deception and is an educational requirement of this institution. Plagiarism, presenting others' work as your own, cheating, telling the professor that you "need" a certain grade, or otherwise seeking to gain an unfair advantage over others in the class is academic dishonesty and will not be tolerated. It will be immediately reported for appropriate action. Using the SAME material/topic in two classes without express permission of all professors involved is against academic regulations. There is usually no objection to this practice, but it is only allowed if you check with the instructors first. Professors compare notes quite frequently, so please be sure you are not in violation of this regulation.

Course Outline

(see NUoodle for weekly assignments in addition to your reading assignments – ALL readings are to be completed PRIOR to the class for which they are assigned – CHR = Counter Hack Reloaded – CE = Chained Exploits)

Week	Topics	Chapter Readings	Other Assignments
1 (20 Jan)	Network architecture review(OSI model, protocols, etc.), IPV6, attack tools, network-centric warfare concepts	CHR: Ch 2, 3, 4	NUoodle readings
2 (27 Jan)	Network Modeling with Colored Petri Nets – Start Project 1: CPN model of the weapons range	CHR: Ch. 12, Ch 5	NUoodle Readings, CPNet Familiarization, Lab: CPNets
3 (3 Feb)	Attack Trees	CHR: Ch 6	NUoodle Readings, SecurITree Familiarization, Lab: SecurITree
4 (10 Feb)	Defense Design Using Attack Trees – Start Project 2: SecurITree Weapons Range Attack Model	CHR: Ch 7, CE: Ch 3	Lab: Web Site Attack Tree
5 (17 Feb)	Project 1 Completion Workshop	CHR: Ch 8	Complete Project 1: CPN Network Model – I am off campus
6 (24 Feb)	Snort, Nagios and NitroView – Lab Exercise: Monitor Deployment on the Weapons Range	CHR: Ch 11	NUoodle Readings
7 (3 Mar)	Red/Blue Lab Exercise 1 – Network Attack/Defend	CHR: Ch 9	Complete Project 2
8 (10 Mar)	Red/Blue Lab Exercise 2 – Web Site Attack/Defend (reverse red and blue teams)	CHR: Ch 10, CE: Ch 7	
9 (24 Mar)	Using Malware (Trojans, worms, bots, etc.)	Student Presentation	

10 (31 Mar)	Red/Blue Lab Exercise 3 – Operating System Attack/Defend	CE: Ch 4	Review CHR Ch 3 & 4 as necessary for this lab
11 (7 Apr)	Red/Blue Lab Exercise 4 – Root Kits (reverse red and blue teams)	CE: Ch 5	Review Student Presentation Notes
12 (14 Apr)	CDX Prep in Lab – Deploy Our Target Network, Monitoring, etc.		CDX Document Distribution
13 (21 Apr)	CDX – 19 to 23 April		
14 (28 Apr)	CDX Postmortem – Log analysis		
15 (5 May)	Final Exam Review		