COURSE SYLLABUS
SEC350: Advanced Network Security: Ethical Hacking

Course Description
Students will learn about advanced network security topics from an attacker's perspective. The objective of the course is to get students to understand how malicious hacker attacks are done. A better understanding of the attacker, allows students to learn how to better defend organizations from an attack.

General Course Information

Number of Units/Weeks	4/10
#Hours Lecture/#Hours Laboratory/#Hours ELPs*	40/0/80
Prerequisite(s)	SEC320
Co-requisites (s)	None
Course Developer(s)	Neil Antis, MBA
Date Approved / Last Review	October 2015

Learning Outcomes
- Outline the process for organizational audits of network elements.
- Examine and describe the current network security level of a business enterprise.
- Use security tools to conduct audits and penetration testing on company assets.
- Monitor trends in external attack methods using internet resources.
- Discuss the management concerns associated with network security.
- Describe the leader's role in implementing security plans inside a business, focusing on the importance of external department buy-in.

Instructional Methods Employed in this Course
- Lecture and reading assignments
- Hands-on exercises and labs
- Team environment
- Practical application of theory and skills in authentic design projects
- Build on prior knowledge and experience of students to enhance richness of class activities.

Information Resources for this Course: Textbook

CEH: Certified Ethical Hacker
ISBN-13: 978-0-7897-5127-0
ISBN-10: 0-7897-5127-5

Table/Topics & Assignments
Types of Assignments:
Lecture -
Considered Lecture Hours

Classroom Discussion -
Considered Lecture Hours

In Class Critique -
Considered Lecture Hours

Delivering Oral Presentations -
Considered Lecture Hours

In Class (IC) Exercise -
Considered Lecture Hours

Reading -
Considered Enhanced Learning Project (ELP), work done outside of class

WebClass lesson (non-online courses) -
Considered ELP, work done outside of class

Lab Work -
Considered Lab Hours

Quiz, Midterm or Final -
Considered Lecture Hours

Week 1						
Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 1A	Ethical Hacking Basics	4	-	-	-	
HW 1A	Read Chapter 1. Evaluated by IC EX 3A	-	-	2.5	-	
HW 1B	Generate a 15 question quiz based on the chapter readings	-	-	1	15	Week 2
Total Week 1		4	0	3.5	15	
Week 2						
Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 2A	The Technical Foundations of Hacking	3.5	-	-	-	
LEC 2B	Project 1 assigned: Mandiant Report	.5	-	8	100	Week 5
HW 2A	Read Chapter 2. Evaluated by IC EX 3A	-	-	2	-	
Total Week 2		4	0	10	100	

Week 3						
Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 3A	Footprinting and Scanning / Enumeration and System Hacking	3	-	-	-	
IC Ex. 3A	Quiz 1 (Chapters 1 & 2)	1	-	-	50	Week 3
HW 3A	Read Chapter 3 & 4. Evaluated by IC EX 4A	-	-	6	-	
HW 3B	Generate a 15 question quiz based on the chapter readings	-	-	1	15	Week 4
Total Week 3		4	0	7	65	

Week 4						
Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 4A	Linux and Automated Assessment Tools / Trojans and Backdoors	3	-	-	-	
IC Ex. 4A	Quiz #2 (Chapters 3 & 4)	1	-	-	50	Week 4
HW 4A	Read Chapter 5 & 6. Evaluated by Midterm	-	-	4	-	
HW 4B	Generate a 15 question quiz based on the chapter readings	-	-	1	15	Week 5
Total Week 4		4	0	5	65	

Week 5

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 5A	Review & In-class Exercise	2	-	-	-	
HW 5A	Review of Text Readings (Chapter 1-6)	-	-	12	-	
Exam 5A	Midterm Exam	2	-	-	250	Week 5
Total Week 5		4	0	12	250	

Week 6

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 6A	Sniffers, Session Hijacking, and Denial of Service	3.5	-	-	-	
LEC 6B	Project 2 assigned: STUXNET	.5	-	8	100	Week 9
HW 6A	Read Chapter 6 & 7. Evaluated by Quiz #3	-	-	4	-	
Total Week 6		4	0	12	100	

Week 7

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 7A	Web Servers, Wireless, IDS/Firewalls/Honey pots	3	-	-	-	
IC EX 7A	Quiz 3 (Chapter 6 & 7)	1	-	-	50	Week 7
HW 7A	Read Chapter 8, 9, & 10. Evaluated by Quiz # 4	-	-	6	-	
HW 7B	Generate a 15 question quiz based on the chapter readings	-	-	1	15	Week 8
Total Week 7		4	0	7	65	

Week 8

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 8A	Buffer Overflows, Viruses, and Worms	1	-	-	-	
LEC 8B	Cryptographic Attacks and Defenses	1	-	-	-	
HW 8A	Read Chapter 11, 12, & 13. Evaluated by Final	-	-	4	-	
IC EX 8A	Quiz #4 (Chapter 8, 9, & 10)	1	-	-	50	Week 8
Total Week 8		4	0	4	50	

Week 9

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
LEC 9A	CEH Review	1	-	-	-	Week 9
IC EX 9A	CEH Exam	3				
HW 9A	Generate a 15 question quiz based on the chapter readings.		-	1	3	Week 10
Total Week 9		4	-	1	3	

Week 10

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 10A	Review & Discussion	1	-	-	-	
IC Ex. 10A	Review text reading. Chapter 1-14	-	-	20	-	
Exam 10A	Final Exam	-	-	-	250	
Total Week 10		1	0	20	250	

Course Hours Summary

Week	Topic	Lec Time	Lab Time	ELP Time
1	Ethical Hacking Basics	4	0	3.5
2	The Technical Foundations of Hacking	4	0	10
3	Footprinting and Scanning / Enumeration and System Hacking	4	0	7
4	Linux and Automated Assessment Tools / Trojans and Backdoors	4	0	5
5	Review & In-class Exercise	4	0	12
6	Sniffers, Session Hijacking, and Denial of Service	4	0	12
7	Web Servers, Wireless, IDS/Firewalls/Honeypots	4	0	7

8	Buffer Overflows, Viruses, and Worms	4	0	4
9	CEH Review	4	0	1
10	Review & Discussion	4	0	20
Total		40	0	81.5

Table/Point Breakdown

Week	Assignment	Possible Points	Percent of Grade
2	HW 1B Self Quiz	15	1.5%
3	Quiz #1	50	5%
4	HW 3B	15	1.5%
4	Quiz 2	50	5%
5	HW 4B	15	1.5%
5	Paper 1: Mandiant Report	100	10%
5	Midterm	250	25%
7	Quiz #3	50	5%
8	HW 7B	15	1.5%
8	Quiz #4	50	5%
9	HW 9A	15	1.5%
9	SCADA Lab	25	2.5%
9	Paper 2: STUXNET	100	10%
10	Final	250	25%
Total		1000	100%