COURSE SYLLABUS
SEC340 OS HARDENING

COURSE DESCRIPTION

This course is designed to further provide students with the tools necessary to apply known attack techniques to an organization to locate security vulnerabilities, analyze the business risk implications, write or develop modern exploits, and recommend mitigations before those vulnerabilities are exploited by real-world attackers.

GENERAL COURSE INFORMATION

Number of Units/Weeks	4/10
#Hours Lecture/#Hours Laboratory/#Hours ELP	40/0/80
Prerequisite(s)	None
Co-requisite(s)	None
Course Developer(s)	Thomas Byrne BA
Date Approved / Last Review	July 2015 /June 2015

LEARNING OUTCOMES

- Implement Hardening Security Tools
- Appraise hardening mitigations for emergent network problems
- Develop a secure hardened network environment
- Implement solutions to current and emergent network threats.

INSTRUCTIONAL METHODS EMPLOYED IN THIS COURSE

- Lecture and reading assignments
- Hands-on exercises
- In-class discussion of current trend in OS hardening
- Weekly homework to apply principles to real-world examples Independent Research and Case Study analysis

INFORMATION RESOURCES FOR THIS COURSE

Textbook

Weaver, Randy and Dawn, Farwood, Dean. Guide to Network Defense and Countermeasures, Third Edition, Course Technology, Cengage Learning 2014 ISBN-13: 978-1-133-72794-1

Supplemental Reading
This Course will also include required reading from selected sources available online

Supplemental Reading Assignments		
Reading	**Topic**	**URL**
1	Common Vulnerabilities and Exposures (CVE)	www.cve.mitre.org
2	Internet Storm Center	http://isc.sans.org
3	CERT Coordination Center	www.cert.org
4	Forum of Incident Response and Security Teams (FIRST)	www.first.org
5	National Institute of Standards and Technology	www.nist.gov
6	NIST Computer Security Division, Computer Security Resource Center (CSRC)	http://csrc.nist.gov
7	Network World Security Research Center	www.networkworld.com/topics/security.html

Online Supplemental Materials

SANS InfoSec Reading Room
http://www.sans.org/reading-room/

U.S. National Institute of Standards and Technology Information Security Handbook:
A Guide for Managers
http://csrc.nist.gov/publications/nistpubs/800100/SP800-100-Mar07-2007.pdf

U.S. National Institute of Standards and Technology Risk Management Framework
http://csrc.nist.gov/groups/SMA/fisma/framework.html

Supplemental Tools

Wireshark Network Analyzer https://www.wireshark.org/

TABLE/TOPICS & ASSIGNMENTS

Types of Assignments:

Lecture –
Considered Lecture Hours

Classroom Discussion – Considered Lecture Hours

In-Class (IC) Exercise –
Considered Lecture Hours

Homework (HW) Exercise –
Considered Enhanced Learning Project (ELP), work done outside class

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

Type	Topic/Description	Lec Time	ELP Time	Point Value	Due
Lecture 1A	Network Security Fundamentals	.5	0	0	
Lecture 1B	TCP/IP	1	0	0	
Reading	TEXT: Chapters 1,2 (78 pages)	0	8	0	Session 1 Evaluated by Quiz 1, Week 3
IC Ex	Week 1…Hands On Chapters 1 and 2	2.5	0	50	
HW 1	End of chapter review questions (40)	0	2	40	

	Total Session 1	4	10	90	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 2A	Network Traffic Signatures	2	0	0	
Lecture 2B	Routing Refresher (Overview of Ch4)	2	0	0	
Reading	TEXT: Chapters 3,4 (76 pages) Supplemental reading 1	0	8		Session 2 Evaluated by Quiz 1, Week 3
HW 2	End of chapter review questions (20)	0	1	20	
	Total Session 2	4	9	20	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 3A	Cryptography	1	0	0	
IC Ex	Quiz 1 on Chapters 1-3	.5	0	50	
IC Ex	Week 3 …Hands On Chapters 3 and 5	2.5	0	50	
Reading	TEXT: Chapters 5 (36 pages)	0	4	0	Session 3 Evaluated by Mid Term Exam, Week 5
HW 3	End of chapter review questions (20)	0	1	20	
	Total Session 3	4	5	120	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 4A	Wireless Networks	2	0	0	
Lecture 4B	Wireless Security	2	0	0	
Reading	TEXT: Chapters 6 and 7 (70 pages)	0	7	0	Session 4 Evaluated by Mid Term Exam, Week 5
HW 4	End of chapter review questions (40)		2	40	

Mid-Term Exam Review	Prior week's readings (189 pages) Omit Chapter 4	0		0	
	Total Session 4	4	9	40	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 5A	Intrusion detection and Prevention	2	0	0	
Reading	TEXT: Chapter 8 (40 pages)	0	4	0	Session 5 Evaluated by Quiz 2, Week 8
HW 5	End of chapter review questions (20)	0	1	20	

Mid-Term Exam	Chapters 1-3, 5-7	2		200	
	Total Session 5	4	5	220	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 6A	Firewalls	.5	0	0	
Lecture 6B	Firewall Design and Management	.5	0	0	
IC Ex	Week 6 …Hands On Chapter 8 and 9	3		50	
Reading	TEXT: Chapters 9 and 10 (80 pages)	0	8	0	Session 6 Evaluated by Quiz 2, Week 8
HW 6	End of chapter review questions (40)		2	40	
	Total Session 6	4	10	90	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 6	VPN Concepts	0.5	0	0	
Lecture 7A	Internet and World Wide Web Security	0.5	0	0	
IC Ex	Week 7 … Hands On Chapter 10	0	0	40	
Reading	TEXT: Chapters 11 and 12 (90 pages)	0	8	0	Session 7 Evaluated by Quiz 2, Week 8

HW7	End of chapter review questions (35)		2	35	
	Total Session 7	1	10	75	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 8A	Security Design and Implementation	1	0	0	
IC Ex	Quiz 2 on Chapters 8-12	0	0	40	
Reading	TEXT: Chapter 13 (50 pages) Supplemental Reading 2,3,4	0	5	0	Session 8 Evaluated by Final Exam
ELP1A	Week 8… Hands On Chapter 11	0		40	
HW 8	End of chapter review questions (15)	0	1	15	
	Total Session 8	1	6	95	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
Lecture 9	Ongoing Security Management	1	0	0	
IC Ex	Week 9 … Hands On Chapter 12		0	40	
Reading	TEXT: Chapter 14 (23 pages) Supplemental Reading 5,6.7	0	2.3	0	Session 9 Evaluated by Final Exam
HW 9	End of chapter review questions (10)		0.5	10	
	Total Session 9	1	3	50	
Type	**Topic/Description**	**Lec Time**	**ELP Time**	**Point Value**	**Due**
IC Ex	Review	2	3		
Final Exam Review	Prior week's readings (220 pages)	0	4		
Final Exam	Chapters 8-14	2		200	
	Total Session 10	2	7	200	

Course Hours Summary:

Session	Topic	Lec Time	ELP Time
1	Network Security TCP/IP	4	10
2	Network Traffic Signatures	4	9
3	Cryptography	4	5
4	Wireless	4	9
5	IPS/IDS	2	5
5	MidTerm Exam	2	6
6	Firewalls	4	10
7	VPN and Internet	4	10
8	Security Design	4	6
9	Ongoing Security management	4	3
10	Review	2	4
10	Final Exam	2	3
Total		**40**	**80**

YOUR GRADES FOR THIS COURSE

Your final grade for this course will be based on an assessment by the Instructor of your performance on a number of course activities, which may include objective tests, classroom exercises, laboratory demonstrations, project papers, or other type of activities. The chart below indicates in what activities you will engage, how many possible points can be earned for each activity, and the percentage of your final grade that will be accounted for by each activity. Students in this course should be graded following Coleman University assessment practices and policies. A point system is used in the University to indicate student performance on various required activities or projects. For this course, points will be distributed as follows:

Week	Assignment	Points Possible	Percent of Grade

1 – 9	End of chapter review questions	240	24%
1	Hands On Week 1	50	5%
3	Quiz 1	50	5%
3	Hands On Week 3	50	5%
5	MidTerm Exam	200	20%
6	Hands On Week 6	50	5%
7	Hands On Week 7	40	4%
8	Quiz 2	40	5%
8	Hands On Week 8	40	4%
9	Hands On Week 9	40	4%
10	Final Exam	200	20%
Total		**1000**	**100%**

Late Submission Policy
All assignments (including projects, lab work, quizzes and exams) must be completed as scheduled , deadlines will be defined 1st day of class.

COLEMAN UNIVERSITY GRADE ASSIGNMENT POLICY

The Coleman University guidelines for the assignment of grades to total points earned is as follows:

Percent	Letter Grade	Grade Points
94-100	A	20%
90-93	A-	10%
87-89	B+	20%
84-86	B	30%

80-83	B-	5%
77-79	C+	5%
74-76	C	2.0
70-73	C-	1.7
67-69	D+	1.33
64-66	D	1.0
60-63	D-	.67
59 or below	F	0

EXPECTATIONS FOR WRITTEN ASSIGNMENTS

Academic Quality
Unless explicitly stated otherwise, all written assignments will be submitted in APA format unless otherwise specified. This includes the Team Assignment paper and any Homework assignments. Note that WebClass Discussion Forum posts are not required to follow APA format.

Students with questions about the quality of their writing style are STRONGLY encouraged to consult the Coleman University Center for Academic Success. Located in Room 232, the CAS is a service available to all Coleman University students to review the grammar and style prior to submission. The CAS has a number of tools available to help students improve their ability to communicate clearly in writing.

Coleman University Students should pay close attention to the Spelling and Grammar Check functions of Microsoft Word®. In addition, the Coleman University Library Resource section of WebClass includes a version of TurnItIn, which allows students to check their work for plagiarism and grammar errors.

Scholarly References
All written assignments will include references to scholarly sources. Scholarly sources include peer-reviewed technical and business journals, papers presented at conferences sponsored by professional organizations (e.g., IEEE, ACM, INCOSE, PMI, etc.), and academic books (i.e., textbooks). Scholarly sources can be found using the EBSCO Host and Harvard Business Review databases available in the Coleman University Library Resource section of WebClass, Google Scholar, plos.org, or the Directory of Open Access Journals. If the option is available in the search engine, please limit your search results to peer-reviewed sources.

The following types of sources **WILL NOT** be accepted as scholarly resources:

- Commercial Webpages (except those included in Online Supplemental Materials section of this document, or with written approval by instructor)
- Open-source wiki sites such as wikipedia.com, ask.com, about.com, answers.yahoo.com
- Blogs such as wordpress.com, blogspot.com (except those included in Online Supplemental Materials section of this document, or with written approval by instructor)
- Postings from open discussion forums

White papers published by commercial organizations MAY be considered scholarly references, but tread lightly. Students are encouraged to review the Coleman University presentation regarding evaluation of resources ("CAARBs") available on the Coleman University Library Resources section of WebClass.

CLASS DECORUM REQUIREMENTS

Attendance

Classes begin and end as indicated in the published schedule. It is required that students be present at the beginning of each class session and stay until class is dismissed, including lab periods. Excessive tardiness, leaving early and/or absences (from either lecture or lab sessions) are causes for dismissal from the University. A student that arrives in class beyond 30 minutes late will be considered absent. A student leaving more than 30 minutes before the end of class will also be considered absent.

Conduct

Students are expected to conduct themselves in a professional manner while on campus. Rules of conduct are outlined in the University Catalog and students are required to adhere to such policies.

COLEMAN UNIVERSITY POLICY ON ACADEMIC DISHONESTY

Academic dishonesty is cause for dismissal from Coleman University. Presenting another person's ideas, methods, course work, or test answers with the intention that they be taken as one's own is theft of a special kind. It defrauds the originator of the work, the institution, its graduates, its students, and its future students. The student has full responsibility for the authenticity of all academic work and examinations submitted. A student who appears to have violated this policy must submit to a hearing with the reporting instructor and the associate dean. If it is determined that a violation occurred, the matter will be referred to an Officer of the

University with recommendations for an appropriate penalty. The student may be dismissed, suspended, or given another penalty.