COURSE SYLLABUS
SEC 320. Intermediate Network Security

Course Description

Students will learn about the tools and techniques used by security professionals to monitor and protect corporate computer networks. Students will be able to understand the different life cycles attacker's use to compromise networks, and how to identify and interpret evidence in different data sources using a variety of analysis techniques.

General Course Information

Number of Units/Weeks	4/10
#Hours Lecture/#Hours Laboratory/#Hours ELPs*	40/00/80
Prerequisite(s)	NET 240
Co-requisites (s)	None
Course Developer(s)	Lydia Zeman, MS
Date Approved / Last Review	September, 2017

*Enhanced Learning Projects

Learning Outcomes

- Select appropriate network security monitoring system tools based on particular interpretation needs
- Analyze network security monitoring data collection
- Interpret network security monitoring data to detect network attacks
- Make use of network security monitoring systems to detect and protect networks from intruder's attacks

Instructional Methods Employed in this Course

- Lecture and reading assignments
- Hands-on exercises and labs
- Research
- Student presentations
- Practical application of theory and skills in authentic projects
- Build on prior knowledge and experience of students to enhance richness of class activities

Information Resources for this Course

□ **Textbook**

Bejtlich, Richard. The Practice of Network Security Monitoring, Understanding Incident Detection and Response. No Starch Press. ISBN 1593275099

□ **Other Materials**

Security Onion
https://securityonion.net/

Security Onion Cheat Sheet
http://chrissanders.org/SO-CheatSheet.pdf

□ **Web Site Readings**

Security Onion Introduction Walkthrough
https://github.com/Security-Onion-Solutions/security-onion/wiki/IntroductionWalkthrough

Wireshark
https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html

Basic Snort Rules Syntax and Usage
http://resources.infosecinstitute.com/snort-rules-workshop-part-one/#gref

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 Homework (HW), work done outside of class

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

Lab Work -
Considered Lab Hours

Quiz, Midterm or Final -
Considered Lecture Hours

Week 1

Type	Topic/Description	LEC Hours	LAB Hours	HW Hours	Point Value	Due
LEC 1A	Network Security Monitoring Rationale	1.5				
LEC 1B	Collecting Network Traffic	1.5				
IC EX 1A	Individual Project	1			15	In-class
HW 1A	Current event analysis			5	30	Week 2
Total Week 1		4		5	45	

Week 2

Type	Topic/Description	LEC Hours	LAB Hours	HW Hours	Point Value	Due
LEC 2A	Stand-alone NSM deployment and installation	1				
LEC 2B	Distributed deployment	1				
IC EX 2A	Individual Project	1			15	In-class
IC EX 2B	Individual Project	1			15	In-class
HW 2A	Research project			6	40	Week 3
Total Week 2		4		6	70	

Week 3

Type	Topic/Description	LEC Hours	LAB Hours	HW Hours	Point Value	Due
LEC 3A	Security Onion platform housekeeping	2				
IC EX 3A	Individual Project	1			15	In-class
IC EX 3B	Individual Project	1			15	In-class
HW 3A	Current event analysis			5	30	Week 4
Total Week 3		4		5	60	

Week 4

Type	Topic/Description	LEC Hours	LAB Hours	HW Hours	Point Value	Due

LEC 4A	Command Line Packet Analysis Tools	1.5				
LEC 4B	Graphical Packet Analysis Tools	1				
IC EX 4A	Individual Project	0.5			15	In-class
IC EX 4B	Individual Project	0.5			15	In-class
IC EX 4C	Individual Project	0.5			15	In-class
HW 4A	Research project			6	40	Week 5
Total Week 4		4		6	85	
Week 5						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
Exam 5A	Midterm Exam	2			150	
IC EX 5A	Class Project	2			40	In-class
HW 5A	Current event analysis			5	30	Week 6
HW 5B	Final Team Project			7		Week 9
Total Week 5		4		12	220	
Week 6						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
LEC 6A	NSM Consoles	1.5				
LEC 6B	NSM Operations	1.5				
IC EX 6A	Individual Project	1			15	In-class
HW 6A	Research project			6	40	Week 7
HW 6B	Final Team Project			8		Week 9
Total Week 6		4		14	55	
Week 7						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
LEC 7A	Server-side Compromise	1.5				
LEC 7B	Client-side Compromise	1.5				
IC EX 7A	Individual Project	1			15	In-class

HW 7A	Current Event Analysis			5	30	Week 8
HW 7B	Final Team Project			8		Week 9
Total Week 7		4		13	45	
Week 8						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
LEC 8A	Extending Security Onion	1.5				
LEC 8B	Workflow, metrics, and collaboration	1.5				
IC EX 8A	Individual Project	1			15	In-class
HW 8A	Research project			6	40	Week 9
HW 8B	Final Team Project			8		Week 9
Total Week 8		4		14	55	
Week 9						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
LEC 9A	Proxies and checksums	2				
IC EX 9A	Cloud Computing	1				
LAB 9A	Individual Project	1			15	In-class
HW 9A	Current Event Analysis			5	30	Week 10
Total Week 9		4		5	45	
Week 10						
Type	**Topic/Description**	**LEC Hours**	**LAB Hours**	**HW Hours**	**Point Value**	**Due**
Exam 10A	Final Exam	2			150	In-class
LEC 10A	Final project presentation	2			170	In-class
Total Week 10		4			320	

Course Hours Summary

Week	Topic	LEC Hours	LAB Hours	HW Hours
1	Network Security Monitoring / Collecting Network	4		5
2	Stand-alone NSM / Distributed Deployment	4		6
3	Security Onion platform housekeeping	4		5

4	Command Line Packet analysis tools / Graphical	4		6
5	Midterm / Class Project	4		12
6	NSM Consoles / NSM Operations	4		14
7	Sever-side compromise / Client-side compromise	4		13
8	Extending Security Onion / Workflow, metrics	4		14
9	Proxies and checksums / Cloud Computing	4		5
10	Final Exam / Final project presentation	4		0
Total		40		80

Table/Point Breakdown

Week	Assignment	Possible Points	Percent of Grade
1	Individual Project	15	1.5%
1	Current Event Analysis	30	3.0%
2	Individual Project	15	1.5%
2	Individual Project	15	1.5%
2	Research Project	40	4.0%
3	Individual Project	15	1.5%
3	Individual Project	15	1.5%
3	Current Event Analysis	30	3.0%
4	Individual Project	15	1.5%
4	Individual Project	15	1.5%
4	Individual Project	15	1.5%
4	Research Project	40	4.0%
5	Midterm Exam	150	15.0%
5	Class Project	40	4.0%
5	Current Event Analysis	30	3.0%
6	Individual Project	15	1.5%
6	Research Project	40	4.0%
7	Individual Project	15	1.5%
7	Current Event Analysis	30	3.0%
8	Individual Project	15	1.5%
8	Research Project	40	4.0%
9	Individual Project	15	1.5%
9	Current Event Analysis	30	3.0%
10	Final Exam	150	15.0%
10	Final Team Project	170	17.0%
Total		1000	100%

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 types 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, it is recommended that points be distributed as follows:

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	4.0
90-93	A-	3.67
87-89	B+	3.33
84-86	B	3.0
80-83	B-	2.67
77-79	C+	2.33
74-76	C	2.00
70-73	C-	1.67
67-69	D+	1.33
64-66	D	1.00
60-63	D-	0.67
N/A	INC	0
N/A	W	0
60 or above	CR	0
59 or below	NC	0
70 or above	PASS	0

Requirements

Assignments: All assignments (including projects, lab work, quizzes and exams) must be completed as scheduled. The following will apply to late assignments:

- 1-24 hours after due date = 20% off point value
- 25-48 hours after due date = 60% off point value
- 49+ hours after due date = No points given

If an assignment equals less than 5 points, no points will be given for late work. If there are extenuating circumstances, the student must submit a written explanation to the department Senior Instructor. Upon evaluation, points will be given according to the Senior Instructor's discretion.

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.

Coleman University employs the plagiarism software known as Turnitin. Students are expected to use this tool in an appropriate manner with the sole purpose to support their own academic endeavors at Coleman University. Turnitin account information can not be shared with anyone. Contact your instructor if you have any questions about plagiarism related issues.

Academic Accommodation / Adjustment Policy:

In accordance with Section 504 of the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA), Coleman University offers accommodations to students with documented physical, psychological, and/or cognitive disabilities. Coleman University will adhere to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations as required to offer equal educational opportunities to qualified disabled individuals.

To qualify for an academic accommodation under ADA, the student must provide adequate documentation of a disability. Students seeking academic accommodations should contact the campus ADA Coordinator at 858-966-3953 or via email at ada@coleman.edu. The ADA Coordinator will review the documentation provided and verify ADA coverage. Students covered under ADA must meet with the ADA

Coordinator at the beginning of every term to determine the appropriate academic accommodations. Failing to meet with the ADA Coordinator at the beginning of every term may impact the availability of accommodations.

After the academic accommodations have been determined, the students’ instructors will be notified by the ADA Coordinator. If any problems or concerns regarding the provision of accommodations occur, the student must inform the ADA Coordinator. If the student feels accommodation is not being made appropriately, the student may follow the published Student Grievance Procedures.