COURSE SYLLABUS
SEC360 ADVANCED NETWORK SECURITY: PENETRATION TESTING

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 ELPs*	40/0/80
Prerequisite(s)	SEC350
Co-requisite(s)	None
Course Developer(s)	Bill Reid
Date Approved / Last Review	April 2015 / June 2015

LEARNING OUTCOMES

- Develop tailored scoping and rules of engagement for penetration testing projects to ensure the work is focused, well defined and conducted in a safe manner
- Conduct detailed reconnaissance using document metadata, search engines and other publicly available information sources to build a technical and organizational understanding of the target environment
- Utilize the Nmap scanning tool to conduct comprehensive network sweeps, port scans, Operating System fingerprinting and version scanning to develop a map of target environments
- Conduct comprehensive password attacks against an environment, including automated password guessing (while avoiding account lockout), traditional password cracking, rainbow table password cracking and pass-the-hash attacks
- Utilize wireless attack tools for Wifi networks to discover access points and clients (actively and passively), crack WEP/WPA/WPA2 keys and exploit client machines included within a project's scope
- Analyze the output of scanning tools to manually verify findings and perform false positive reduction
- Utilize the Windows and Linux command lines to plunder target systems for vital information that can further overall penetration test progress, establish pivots for deeper compromise and help determine business risks
- Configure the Metasploit exploitation tool to scan, exploit and then pivot through a target environment in-depth

INSTRUCTIONAL METHODS EMPLOYED IN THIS COURSE

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

INFORMATION RESOURCES FOR THIS COURSE

Textbook

Brown, M. (2014). *Computer security and penetration testing (2nd ed.)*. Stamford, CT: Cengage Learning. IBSN10: 0-8400-2093-7 ISBN13: 978-0-8400-2093-2

Kim, P. (2015). *The Hacker Playbook 2: Practical Guide to Penetration Testing.* North Charleston, SC: Secure Planet LLC. ISBN10: 1512214566 ISBN13: 978-1512212567

Supplemental Reading

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

Supplemental Reading Assignments		
Reading	**Topic**	**URL**
1	Spearphishing	http://www.sans.org/reading-room/whitepapers/forensics/reducing-catch-fighting-spear-phishing-large-organization-35547
2	Zero-day Exploits	http://www.sans.org/reading-room/whitepapers/bestprac/defenses-zero-day-exploits-various-sized-organizations-35562
3	Password Cracking	http://www.sans.org/reading-room/whitepapers/basics/password-security-thirty-five-years-35592
4	Encryption	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201408_en.pdf#__utma=216335632.1172287603.1428117700.1428117700.1428162973.2&__utmb=216335632.68.8.1428164431613&__utmc=216335632&__utmx=-&__utmz=216335632.1428117700.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=70519507
5	Denial of Service	http://www.sans.org/reading-room/whitepapers/basics/denial-service-deterrence-35877
6	Data Breach	http://www.sans.org/reading-

	Preparation	room/whitepapers/dlp/data-breach-preparation-35812
7	Advanced Persistent Threat	http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-Threats-Awareness-Study-Results.aspx
8	Intrusion Prevention	http://www.sans.org/reading-room/whitepapers/intrusion/active-security-or-learned-stop-worrying-ips-incident-handling-34465
9	Risk Management Framework	http://csrc.nist.gov/groups/SMA/fisma/framework.html
10	Security State of the Web	https://www.menlosecurity.com/resources/Vulnerability_Report_Mar_2015.html
11	Cloud Computing Security	http://www.sans.org/reading-room/whitepapers/cloud/proposal-standard-cloud-computing-security-slas-key-metrics-safeguarding-confidential-dat-35872
12	Defense in Depth	http://www.sans.org/reading-room/whitepapers/leadership/defense-in-policy-begets-defense-in-depth-35882
13	Incident Response	http://www.sans.org/reading-room/whitepapers/analyst/automation-incident-response-process-creating-effective-long-term-plan-35802

Online Supplemental Materials

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

Information Systems Audit and Control Association
http://www.isaca.org/

U.S. National Institute of Standards and Technology Information Security Handbook: A Guide for Managers
http://csrc.nist.gov/publications/nistpubs/800-100/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/

John the Ripper Password Cracker
http://www.openwall.com/john/

VirusTotal
https://www.virustotal.com/

TABLE/TOPICS & ASSIGNMENTS

Types of Assignments:

Lecture –
Considered Lecture Hours

Classroom Discussion –
Considered Lecture Hours

Delivering Oral Presentations –
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

Lab Work –
Considered Lab Hours

Session 1						
Type	**Topic/Description**	**Lec Time**	**Lab Time**	**ELP Time**	**Point Value**	**Due**
Lecture 1A	Ethics of Hacking	2	0	0	0	
Lecture 1B	Reconnaissance	2	0	0	0	
HW - Reading	Brown: Chapters 1,2 (44 pages) Kim: Pages 26-73 (47 pages)	0	0	9.1	0	Session 1 Evaluated by Quiz 1, Week 3
HW 1	End of chapter review questions (40)	0	0	2	40	
	Total Session 1	4	0	11.1	40	
Session 2						
Type	**Topic/Description**	**Lec Time**	**Lab Time**	**ELP Time**	**Point Value**	**Due**
Lecture 2A	Scanning Tools	2	0	0	0	

Lecture 2B	Sniffers	2	0	0	0	
HW - Reading	Brown: Chapters 3&4 (49 pages) Kim: Pages 74-96 (22 pages)	0	0	71.		Session 2 Evaluated by Quiz 1, Week 3
HW 2	End of chapter review questions (34)	0	0	2	40	
	Total Session 2	4	0	9.1	40	

Session 3

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 3A	TCP/IP Vulnerabilities	1	0	0	0	
Lecture 3B	Encryption and Password Cracking	2	0	0	0	
Lecture 3C	Spoofing	1	0	0	0	
IC Ex	Quiz 1				50	
HW - Reading	Brown: Chapters 5, 6,7 (61 pages) Kim: Pages 140-169 (30 pages)	0	0	9.1	0	Session 3 Evaluated by Mid Term Exam, Week 6
	Total Session 3	4	0	9.1	50	

Session 4

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 4A	Vulnerabilities: Session Hijacking and Network Hacking	2	0	0	0	
Lecture 4B	Denial of Service Attacks	2	0	0	0	
HW 3	End of chapter review questions (60)			3	60	
Reading	Brown: Chapters 8, 9 , 11 (61 pages) Kim: Pages 170-204 (34 pages)	0	0	9.5	0	Session 4 Evaluated by Mid Term Exam, Week 6
	Total Session 4	4	0	12.5	60	

Session 5

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 5A	Intrusion Prevention, NG Firewalls	1	0	0	0	
Lecture 5B	Advanced Persistent Threat	2	0	0	0	
Lecture 5C	Risk Management Framework	1	0	0	0	
HW 4	End of chapter review questions (20)	0	0	1	20	
Reading	TEXT: Chapter 14 (23 pages)	0	0	2.3	0	Session 5 Evaluated by Quiz 2, Week 8
Mid-Term Exam		2			100	
	Total Session 5	4	0	3.3	20	

Session 6

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 6	Vulnerabilities and Exploits	2	0	0	0	

Reading	Brown: Chapters 9, 12, 13 (55 pages) Kim: Pages 205-216, pages 243-262 (30 pages)	0	0	8.5	0	Session 6 Evaluated by Quiz 2, Week 8
HW 6	End of chapter review questions (60)			3	60	
	Total Session 6	4	0	11.5	160	

Session 7

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 6	Vulnerabilities and Exploits	2	0	0	0	
Lecture 7A	OS Vulnerabilities	2	0	0	0	
Reading	TEXT: Chapters 16, 17 (23 pages) Kim: Pages 263-318 (55 pages)	0	0	7.8	0	Session 7 Evaluated by Quiz 2, Week 8
HW7	End of chapter review questions (40)			2	40	
	Total Session 7	4	0	9.8	40	

Session 8

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 8A	Web Security	2	0	0	0	
Lecture 8B	Security and Cloud Computing	2	0	0	0	
Quiz 2					50	
Reading	Brown: Chapter 15 (30 pages) Kim: Pages 319-337 (18 pages)	0	0	4.8	0	Session 8 Evaluated by Final Exam
HW 8	End of chapter review questions (20)			1	20	
	Total Session 8	4	0	5.8	70	

Session 9

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
Lecture 9	Incident Response	2	0	0	0	
Reading	TEXT: Chapter 18 (23 pages)	0	0	2.3	0	Session 9 Evaluated by Final Exam
ELP 1A	Team Research Project				300	
HW 9	End of chapter review questions (20)			1	20	
	Total Session 9	4	0	3.3	320	

Session 10

Type	Topic/Description	Lec Time	Lab Time	ELP Time	Point Value	Due
ELP 1B	Group Project Presentations	2	0	4	40	Session 10
Final Exam		2			100	
	Total Session 10	4	0	4	140	

Course Hours Summary:

Session	Topic	Lec Time	Lab Time	ELP Time
1	Ethics of Hacking	4	0	11.1
2	Scanning and Sniffing	4	0	9.1
3	Vulnerabilities I: TCP/IP and Passwords	4	0	9.1
4	Vulnerabilities II: Session and Network	4	0	12.5
5	Preparing for the Advanced Threat	4	0	3.3
6	Vulnerabilities III: Application Layer Exploits	2	0	11.5
	MidTerm Exam	2	0	0
7	Vulnerabilities IV: Operating Systems	4	0	9.8
8	Security in the Cloud	4	0	5.8
9	Incident Response Planning	4	0	3.3
10	Project Presentations	2	0	4
	Final Exam	2	0	0
Total		**40**	**0**	**79.5**

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	360	36%
5	MidTerm Exam	100	10%
3	Quiz 1	50	5%
8	Quiz 2	50	5%
10	Team Project/Presentation	300/40	34%
10	Final Exam	100	10%
Total		**1000**	**100%**

Late Submission Policy
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

NOTE: 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.

Grading Structure

The following table lists the Coleman University grading structure. All grades listed will count as units attempted.
For each unit in which the student is enrolled, he or she will receive quality points as follows:

Letter Grade	Percentage	Grade Points
A	94% - 100%	4.00
A-	90% - 93%	3.67
B+	87% - 89%	3.33
B	84% - 86%	3.00
B-	80% - 83%	2.67
C+	77% - 79%	2.33
C	74% - 76%	2.00
C-	70% - 73%	1.67
D+	67% - 69%	1.33
D	64% - 66%	1.00
D-	60% - 63%	0.67
F	0% - 59%	0.00
I	N/A	0.00
W	N/A	0.00
CR	70% or above	0.00
NC	69% or below	0.00
AU	N/A	0.00
TR	N/A	0.00
WV	N/A	0.00

Note: I = Incomplete, W = Withdraw, CR = Credit, NC = No Credit, AU= Audit, TR= Transfer, WV= Course Waiver

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.

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 cannot be shared with anyone. Contact your instructor if you have any questions about plagiarism related issues.

Once an assignment is submitted in TurnItIn, it cannot be resubmitted. It is each student's responsibility to ensure he or she has submitted the correct and final version of an assignment in a TurnItIn drop box.