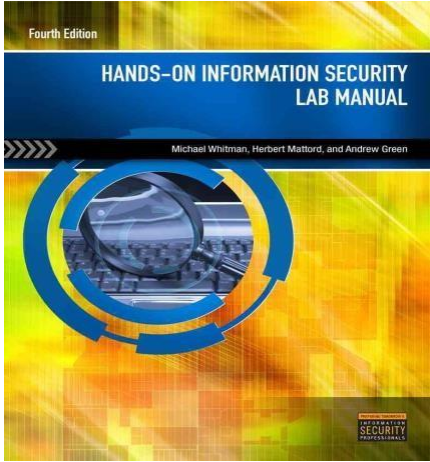
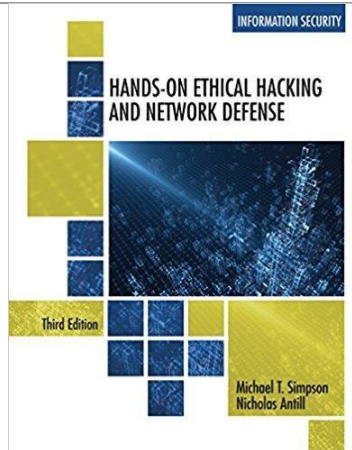


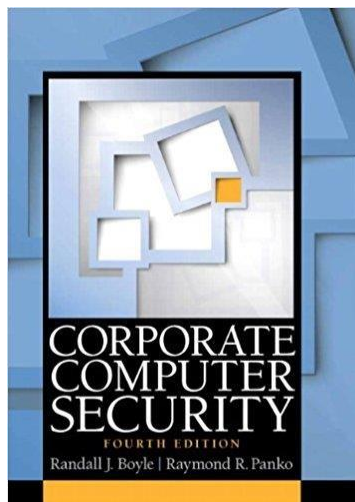
Syllabus CSI4480/5480-Information Security Practice (4 Credits) Winter 2018

Meeting Day and Time: Tuesdays and Thursdays 1:00PM – 2:47 PM
Lecture Classroom and Computer Lab: EC554

Course Description	This <i>course</i> surveys the concepts and methods of security policies, models and mechanisms for secrecy, integrity, availability, and authentication. Topics covered include security policies; access control; introduction to cryptography; footprinting, scanning, and enumeration; common system vulnerabilities and countermeasures; and System remediation and hardening;
Prerequisites	CSI 2470 and major standing in CS/IT
Instructor Details	Dr. Khalid Mahmood Malik Office: EC532 Email: mahmood@oakland.edu Office Hours: Friday, 3pm – 4 pm, or by appointment
TA Details	Abdelnasser Bani Hani Email: abanihani@oakland.edu
Textbooks	<ol style="list-style-type: none"> 1. Michael E. Whitman Herbert J. Mattord Andrew Green, <i>Hands-on Information Security Lab Manual, 4th Edition, 2014</i>. Publisher: Course Technology, Cengage Learning. (e-copy is acceptable) <div style="text-align: center;">  </div> <ol style="list-style-type: none"> 2. Michael T. Simpson, Nicholas Antill <i>Hands on Ethical Hacking and Network Defense</i>(e-copy is acceptable)



3. Randy J Boyle, Raymond R. Panko *Corporate Computer Security (4th Edition)*, Pearson, 2015 (3rd edition is also acceptable and one may find it online)



Reference Books

Patrick Engebretson, *The Basics of Hacking and Penetration Testing, Second Edition*; Publisher: Syngress, 2013

David Kim and Michael G. Solomon, *Fundamentals of Information Systems Security, 2014*. Publisher: Jones & Bartlett learning.

Michael Gregg, *Cert Guide of Certified Ethical Hacker (CEH)*. Publisher: Pearson IT certification.

John R. Vacca, *Computer and Information Security Handbook*, Morgan Kaufmann, 2013.

William Stallings, Lawrie Brown, *Computer Security, Principles and Practice, 3rd Edition*, Pearson.

<p>Course Objectives</p>	<ol style="list-style-type: none"> 1. Define the key concepts in information security, e.g., confidentiality, integrity, authentication and availability 2. Explain cryptographic concepts, e.g., encryption, decryption, and key; 3. Gain hands-on experience on information security; 4. Conduct footprinting, scanning, and enumeration; 5. Identify and validate common system vulnerabilities; 6. Practice system remediation and hardening; 7. Interpret intrusion detection; 8. Describe access control and firewalls; 9. Construct security policies
<p>Course Website</p>	<p>A session specific website is located at https://moodle.oakland.edu/moodle. Use your OU email account name and password to login to the system. This website will include notes, schedules, labs, assignments, etc. for this class. Assignments and practice labs should be submitted using the Moodle. Please check this site often for updates. Also use the forums of moodle page for sharing interesting reading material, new security breaches and new developments in area of cybersecurity.</p>
<p>Evaluation</p>	<p>Your final grade will be evaluated based on the following components and weights</p> <ul style="list-style-type: none"> • <u>Labs and Homework</u>: 50%, 500 points • <u>Midterm Exam</u>: 15%, 150 points • <u>Final Exam</u>: 20%, 200 points • <u>Presentation/Project</u>: 15%, 150 points • <u>Extra Credit: Class Participation, completion of optional parts in labs and lab 13 (listed below), and active learning</u>: 10%, 100 points <p>Labs and Assignments (50%)</p> <p>Lab assignments come from the lab manual and are performed on the lab equipment. Students answer a short quiz or deliver a brief checklist confirming their understanding of the lab material. Generally, homework assignments require students to write short essays, summarizing reading from the textbook. Homework is due one week from the day it is assigned. Unless specified explicitly, students are expected to finish each assignment independently. For a question that allows collaboration, the level of collaboration will be specified in the question description. The submission of your homework will be due to Moodle, and the required form of submission (e.g., code or report) will be given along with the homework itself. Late submission will not be graded.</p> <p>Lab sessions and accompanying assignments are due throughout the term. Details and due dates are announced in class. Each of these lab assignments is weighted equally. No lab make-up sessions are available, and late assignments will not be accepted! If you are unable to arrive at the lab on time on the day of the lab session and must then perform the lab work on your own, you are responsible for turning in the lab assignment on time. You may turn the assignment in early. Assignments are submitted via Moodle unless specified otherwise.</p> <p>Exams (35%, 350 points)</p> <p><u>Midterm Exam</u>: The midterm exam (15%) covers basic concepts, ethics, information assets, threats, common attacks and defenses. It also confirms understandings of software covered in the early labs.</p>

Final Exam: The final exam (20%) covers all other course material, homework, lab assignments plus selected material from student presentations. **There will be no make-up examinations.**

Group Project/Presentation (15%, 150 points)

Each group (with 4 or 6 students) will prepare and deliver a 5-10 minute presentation of a security-related software utility. Presentations will be graded on applicability, brevity and clarity, in the following areas:

Part 1 – Statement of problem

Part 2 – Statement of how to solve the problem

Part 3 – Diagram (or demonstration) of how utility solves the problem

Part 4 – References, website, or where to go for more detailed information

Each group will choose a topic of project before **February 03 (11:55 pm)**. Students choose their own presentation date on a first come, first served basis. Groups may present on any class day, providing no more than three groups present on any given class day. Confirm software choice and presentation date with instructor by email.

Grading criteria	Points Earned	Grade
	975-1000	4.0
950-974	3.9	
925-949	3.8	
900-924	3.7	
875-899	3.6	
850-874	3.5	
825-849	3.4	
800-824	3.3	
775-799	3.2	
750-774	3.1	
725-749	3.0	
700-724	2.9	
675-699	2.8	
650-674	2.7	
625-649	2.6	
600-624	2.5	
500-599	2.0-2.4	
Less than 500	0.0	

Important Dates	Class begins: 1/3 Mid-term exam: 02/27 Final Exam: Tuesday April 24, Noon-3:00 PM
------------------------	---

Tentative Topics, Schedule (with mapping of course objectives):	Week1: Introduction, Logistics Preparation & Installation of Operating Systems (objective 3) Week 2: Footprinting, Web Reconnaissance and social Engineering (Objective 3 and 4) Week 3: TCP overview, Port Scanning, TCP and UDP Scanning Techniques (Objective 3 and 4) Week 4: Enumeration (Objective 3 and 4) Week 5: OS Fingerprinting and Vulnerability identification, Vulnerability Scanners- Nessus and MBSA (Objective 3 and 5) Week 6: Penetration Testing using Metasploit (Objective 3 and 5) Week 7: System Hardening; Host Hardening and Remediation (Objective 3 and 6) Week 8: Introduction to application and web security (Objective 3 and 5) Week 09: Access Control using Firewalls, and Network defense (Objective 3,8 and 9) Week 10 &11: Security Policies and its Implementation in Firewalls (Objective 3,8 and 9) Week 12: Network based Intrusion Detection and Prevention (Objective 3 and 9) Week 13: Cryptography and Network Security (objective 1 and objective 2)
---	--

Attendance	<p>In order to achieve the best outcomes, every student is required in principle to attend every meeting of the class. Attendance will be taken in randomly selected classes. To account for unexpected situations that are out of the control of the student, each student is allowed with at most <u>4</u> unexcused missing lectures.</p> <p>Beyond that 4-lecture limit, a student who cannot attend a lecture must send the instructor an email notification at least 4 hours before the class to explain the reason why he/she cannot attend the class. Beyond the 4-lecture limit, each unexcused missing lecture will receive a 0.1 penalty in the student’s final GPA (4.0 scale). Late arrival and side talking during the meeting are strongly discouraged.</p>
Course Expectations	<p>In order to be successful in this course a student must:</p> <ol style="list-style-type: none"> 1) Regularly follow all the lectures. Notes and examples given during lecture will be most helpful for completing the homework assignments. 2) Turn in homework and lab assignments on time and follow the submission guidelines. Each assignment is building upon previous ones. Missing one assignment will make it difficult to complete the following ones. 3) Spend extra care to make your assignments readable, concise, and complete. 4) <u>It is very important to review the lab for 30 minutes before coming to class. Labs will be posted 24 hours in advance. This will help you to complete the labs on time during class. You are highly encouraged to complete theoretical part of labs before coming to class.</u>
Academic Integrity	<p>Students are expected to comply with the Academic Conduct Policy of the Oakland University. Suspected breaches of academic honesty will be taken before the Academic Conduct Committee. Academic misconduct includes—but not limited to—cheating in quizzes and exams, unauthorized collaborations in assignments, and plagiarizing the work of others. Students found guilty of academic misconduct in this course will receive a grade <u>0.0</u> for the course in addition to any penalties imposed by the conduct committee. Please refer to the undergraduate catalog and on-line Academic Conduct Regulations at http://www.oakland.edu/handbook/ for details.</p>

White Hat Agreement	Because of the nature of this course (security), students in this course are expected to familiarize themselves with the ethics and laws peculiar to information security. Read and understand the White Hat Agreement posted under this course on Moodle. Submit to your instructor a copy of this agreement bearing your signature before using university equipment for lab work for this course.
Disability Statement	Any student with a documented disability needing academic adjustments is requested to notify the instructor as early in the semester as possible, and must do so before the midterm exam. Verification from OU Disabled Student Support Services is required. All discussions will remain confidential.

ABET Outcome Mapping

Component	Program Outcome													
	a	b	c	d	e	f	g	h	I	J	k	l	m	n
<u>Lectures</u>	✓				✓				✓	✓			✓	
<u>Lab 0:</u> Installations, logistic preparation, <i>white hat agreement</i>	✓				✓									
<u>Lab 01:</u> Performing network reconnaissance using Command Line, interpreting different output of commands.									✓	✓				
<u>Lab 02:</u> Interpreting web information for recon analysis, Performing reconnaissance using online and locally deployed tools (Domain Dossier, Whois, Internic, OWASP ZAP)		✓							✓	✓			✓	
<u>Lab 03:</u> Performing Scanning, enumeration and fingerprinting using different tools (APS, Nmap...)		✓							✓	✓			✓	
<u>Lab 04:</u> Perform system benchmarking, registry and log configurations and interpretation on Windows and Linux		✓							✓	✓				
<u>Lab 05:</u> Perform research and analysis of System vulnerabilities, Vulnerability Identification using Advanced tools such as Nessus		✓							✓	✓			✓	
<u>Lab 06:</u> Perform Vulnerability Validation using state-of-the-art tools such as Metasploit		✓							✓	✓			✓	
<u>Lab 07:</u> Perform Log Auditing and System Hardening on Windows and Linux Machines.									✓	✓			✓	
<u>Lab 08:</u> System and Services Hardening on Linux Machines (Apache, DNS, Postfix...)		✓							✓	✓			✓	
<u>Lab 09:</u> XSS and SQL injection using OWASP WebGoat														
<u>Lab 10:</u> File and Disk Encryption, File permission manipulation on Linux Systems									✓	✓				
<u>Lab 11a:</u> Maintaining System Firewalls using iptables (software firewalls).														
<u>Lab 11b:</u> Hardware firewall: Administering CISCO switch configurations that mimic real-world scenarios, and manipulate the configuration to									✓	✓			✓	

achieve better security														
<u>Lab 12:</u> Deploy and maintain intrusion detection mechanisms using fundamental tools such as SNORT									<u>✓</u>	<u>✓</u>			<u>✓</u>	
<u>Lab 13 Extra Credit Lab :</u> File Integrity Authentication and Validation on Windows Machines for host intrusion detection & to understand Network Security concepts									<u>✓</u>	<u>✓</u>				
<u>Midterm Exam</u>		<u>✓</u>							<u>✓</u>	<u>✓</u>			<u>✓</u>	
<u>Final Exam</u>		<u>✓</u>							<u>✓</u>	<u>✓</u>			<u>✓</u>	
<u>Course Project</u>		<u>✓</u>							<u>✓</u>	<u>✓</u>			<u>✓</u>	
<u>Extra Credit Work</u>									<u>✓</u>	<u>✓</u>			<u>✓</u>	

ABET Program Outcomes

a	An ability to apply knowledge of computing and mathematics appropriate to the discipline.
b	An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution.
c	An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs.
d	An ability to function effectively on teams to accomplish a common goal.
e	An understanding of professional, ethical, legal, security, and social issues and responsibilities.
f	An ability to communicate effectively with a range of audiences.
g	An ability to analyze the local and global impact of computing on individuals, organizations and society.
h	Recognition of the need for, and an ability to engage in, continuing professional development.
i	An ability to use current techniques, skills, and tools necessary for computing practice.
j	An ability to use and apply current technical concepts and practices in the core information technologies.
k	An ability to identify and analyze user needs and take them into account in the selection, creation, evaluation and administration of computer-based systems.
l	An ability to effectively integrate IT-based solutions into the user environment.
m	An understanding of best practices and standards and their application.
n	An ability to assist in the creation of an effective project plan.

Tentative Schedule*

Date	Activities
4-Jan-18	Discussion: Syllabus and semester plan, Team formation for project plus labs
9-Jan-18	Lab0 and Lecture
11-Jan-18	Lab1 & Lecture
16-Jan-18	Lecture
18-Jan-18	Lab2 & Lecture
23-Jan-18	Lecture
25-Jan-18	Lab3 & Lecture
30-Jan-18	Lecture
1-Feb-18	Lab4 & Lecture (FEB 03 is deadline of Project proposal)
6-Feb-18	Lecture
8-Feb-18	Lab5 & Lecture
13-Feb-18	Lecture
15-Feb-18	Lab6 & Lecture
20-Feb-18	Winter recess
22-Feb-18	Winter recess
27-Feb-18	Mid-term exam
1-Mar-18	Lecture
6-Mar-18	Lab7 & Lecture
8-Mar-18	Lecture
13-Mar-18	Lab8 & Lecture
15-Mar-18	Lecture
20-Mar-18	Lab9 & Lecture
22-Mar-18	Lecture
27-Mar-18	Lab10 & Lecture
28-Mar-18	Project Submission, 11:55pm
29-Mar-18	Lecture
3-Apr-18	Lab11 & Lecture
5-Apr-18	Lecture, Project Presentations
10-Apr-18	Lab12 & Lecture
12-Apr-18	Lecture, Project Presentations
17-Apr-18	Project Presentations
19-Apr-18	Study day
24-Apr-18	Final exam

Note: Lecture topics and project assignments are subject to continuous change at the discretion of the instructor. For deadline of lab submission, see the dates on Moodle.