JOHNS HOPKINS
WHITING SCHOOL
of ENGINEERING

Syllabus
EN.650.431
Ethical Hacking
Spring 2020

Description

Cyber security is the premier issue of our time. It affects every facet of industry and our government, and thus is now a threat to our U.S. National Security. This course is designed to introduce students to the skills needed to defend computer network infrastructure by exposing them to the hands-on identification and creation of vulnerabilities in servers (i.e., Windows and Linux), wireless networks, websites, and cryptologic systems. These skills will be tested by having teams of students develop and participate in instructor lead capture-the-flag competitions. Also included are advanced topics such as shell coding, IDA Pro analysis, fuzzing, and writing or exploiting network-based applications or techniques such as web servers, spoofing, and denial of service.

Instructor

Dr. Lanier Watkins, lanier.watkins@jhuapl.edu or lanierwatkins@gmail.com
Office: 210 Hodson Hall
Office hours: by appointment through email
Phone: 404-406-5426

Meetings

4:30-7:00 pm, Thursday

Textbook

Required: Cameron Buchanan. Kali Linux CTF Blueprints, Packt Publishing, 2014
Recommended: Jon Erickson. Hacking, 2nd Edition: The Art of Exploitation, 2008

Online Resources

Please log in to Blackboard for all materials related to this course. [Or provide a URL if using another online course management system.]

Course Objectives

(1) Students will learn how to identify and create vulnerabilities in servers, wireless networks, websites, and cryptologic systems
(2) Students will learn how to develop and participate in capture-the-flag exercises.

Course Topics

- Penetration testing
- Network hardening
- Capture-the-flag exercise creation, strategy, and scoring

Topics and Schedule:

Date	Topic	Comments

Week #1
1/30/2020
	Exploiting Windows
	○ Focus on planting flags for windows for various scenarios (i.e., securing windows environment except for vulnerable software which leads to flag)
	○ Chapter 1: Page 7 - 15
		• Syllabus Review
		• Ethics Discussion
		• Discuss semester long Capture-the-Flag (CTF) student projects
		  • See week #13 for details
		• Discuss Bonus
		  • Attend National Collegiate Cyber Defense Competition (http://maccdc.org)
		• 2-hour hands-on creating and/or exploitation of server vulnerabilities
		• Two 5 min breaks (7 & 8pm)
		• Groups Collaborate
		  • 20 minutes

Week #2 2/6/2020	**Exploiting Windows** ○ Focus on planting flags for windows for various scenarios (i.e., securing windows environment except for vulnerable software which leads to flag) ○ Chapter 1: Page 15 – 35 ○ Homework #1	• 2-hour hands-on creating and/or exploitation of server vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate ○ 20 minutes
Week #3 2/13/2020	**Exploiting Linux** ○ Focus on planting flags for Linux for various scenarios (i.e., securing Linux environment except for vulnerable software which leads to flag) ○ Chapter 2: Page 37 – 47 ○	• Video lecture will be posted to Blackboard • TA will host Metasploit training • TA will provide homework help • Groups can meet and collaborate

Week #4 2/20/2020	**Exploiting Linux** ○ Focus on planting flags for Linux for various scenarios (i.e., securing Linux environment except for vulnerable software which leads to flag) ○ Chapter 2: Page 47 – 59	• Video lecture will be posted to Blackboard • TA will host Metasploit training • TA will provide homework help • Groups can meet and collaborate • Email instructor executive summary for CTF and project task list for CTF completion
Week #5 2/27/2020	**Exploiting Wireless and Mobile** ○ Focus on planting flags for wireless or mobile devices for various scenarios (i.e., securing wireless or mobile device environments except for vulnerability which leads to flag) ○ Chapter 3: Page 61 – 71 ○ Review Homework #1 ○ Homework #2	• 2-hour hands-on creating and/or exploitation of wireless vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate • 20 minutes
Week #6 3/5/2020	**Pivoting** ○ We will discuss pivoting theory and practical application ○ Special Topic	• 2-hour hands-on creating and/or exploitation of wireless vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate ○ 20 minutes

Week #7
3/12/2020
	Social Engineering Websites and Pictures
	○ Focus on extracting info from people via cross-site scripting or passing/extracting info in/out of pictures for various scenarios (i.e., securing websites environments except for vulnerability which leads to flag)
	○ Chapter 4: Page 81 -91
	○ Review Homework #2
	○ Homework #3
		• Exam 1
		  • 1 hour
		• 1-hour hands-on creating and/or exploitation of website vulnerabilities
		• Two 5 min breaks (7 & 8pm)
		• Groups Collaborate
		  • 20 minutes

Week #8 3/26/2020	**Social Engineering Websites and Pictures** ○ Focus on extracting info from people via cross-site scripting or passing/extracting info in/out of pictures for various scenarios (i.e., securing websites environments except for vulnerability which leads to flag) ○ Chapter 4: Page 91 - 101	• 2-hour hands-on creating and/or exploitation of website vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate ○ 20 minutes
Week #9 4/2/2020	**Exploiting Cryptology** ○ Focus on using basic tools to exploit improperly implemented encryption on previously placed flags ○ Chapter 5: Page 103 – 113 ○ Review Homework #3 ○ Homework #4	• 2-hour hands-on creating and/or exploitation of improperly implemented encryption vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate 20 minutes

Week #10 4/09/2020	**Exploiting Cryptology** ○ Focus on using basic tools to exploit improperly implemented encryption on previously placed flags ○ Chapter 5: Page 113 - 123	• 2-hour hands-on creating and/or exploitation of improperly implemented encryption vulnerabilities • Two 5 min breaks (7 & 8pm) • Groups Collaborate • 20 minutes
Week #11 4/16/2020	**Capture the Flag Basics** ○ Basic rules and strategies ○ How to score flag captures and report team progress ○ Chapter 6: Page 125 – 132 ○ Review Homework #4 ○ Homework #5	• Two 5 min breaks (7 & 8pm) • Groups Collaborate • 20 minutes
Week #12 4/23/2020	**Capture the Flag Walkthrough** ○ In class walkthrough of a capture the flag challenge ○ Discussions on scoring and reporting status of walkthrough ○ Student CTF Dry Runs ○ Chapter 6: Page 132 - 162	• Exam 2 • I hour • Two 5 min breaks (7 & 8pm) • Two 5 min breaks (7 & 8pm)

Week #13 4/30/2020	**Capture the Flag Tournament** • From start of semester, the class will be divided into two large teams and tasked with creating Capture the Flag (CTF) Challenges. The large teams will exchange CTF challenges, split into smaller teams which will compete against each other in the unseen challenge. The large team that created the CTF challenge will score and report the status of the competition. • The CTF challenges will be done in class and will be timed. These challenges will be semester long projects for the students.	• Team CTF projects • Two 5 min breaks (7 & 8pm)

Course Expectations & Grading

Grading Rubric

Assignment	# of Assignments	Percentage of Grade	Comments
Windows, Linux, and Wireless Hacking Exam #1	1	15%	In class, closed notes exam
Social Engineering, Cryptology, and CTF Exam# 2	1	15%	In class, closed notes exam
Class Participation: •	13	20%	Following along with in-class hacking assignments
Home Work	5	20%	Homework Assignments
Team CTF Project • Project Plan • CTF Implementation	2	30%	Both groups will develop a CTF tournament

Grading:

A letter grade will be assigned according to this formula: 100-98%=A+, 97-94%=A, 93-90%=A-, 89-87%= B+, 86-83%= B, 82-80%= B-, 79-70%= C, <60%=F. Appropriate curving will be made as necessary.

What kinds of work you'll be doing in this course. Weekly homework assignments, two midterms, one final. Active participation in class discussion, oral presentation. And explain the grading basis and policy.

Key Dates
Dates for exams, presentations, etc. This can be on Blackboard instead of here.

Assignments & Readings
For those who specify this explicitly in advance. Or say explicitly that these are posted on the Blackboard site for this course.

Ethics
The strength of the university depends on academic and personal integrity. In this course, you must be honest and truthful, abiding by the *Computer Science Academic Integrity Policy*:

> Cheating is wrong. Cheating hurts our community by undermining academic integrity, creating mistrust, and fostering unfair competition. The university will punish cheaters with failure on an assignment, failure in a course, permanent transcript notation, suspension, and/or expulsion. Offenses may be reported to medical, law or other professional or graduate schools when a cheater applies.
>
> Violations can include cheating on exams, plagiarism, reuse of assignments without permission, improper use of the Internet and electronic devices, unauthorized collaboration, alteration of graded assignments, forgery and falsification, lying, facilitating academic dishonesty, and unfair competition. Ignorance of these rules is not an excuse.
>
> Academic honesty is required in all work you submit to be graded. Except where the instructor specifies group work, you must solve all homework and programming assignments without the help of others. For example, you must not look at anyone else's solutions (including program code) to your homework problems. However, you may discuss assignment specifications (not solutions) with others to be sure you understand what is required by the assignment.
>
> *If* your instructor permits using fragments of source code from outside sources, such as your textbook or on-line resources, you must properly cite the source. Not citing it constitutes plagiarism. Similarly, your group projects must list everyone who participated.
>
> Falsifying program output or results is prohibited.
>
> Your instructor is free to override parts of this policy for particular assignments. To protect yourself: (1) Ask the instructor if you are not sure what is permissible. (2) Seek help from the instructor, TA or CAs, as you are always encouraged to do, rather than from other students. (3) Cite any questionable sources of help you may have received.
>
> On every exam, you will sign the following pledge: "I agree to complete this exam without unauthorized assistance from any person, materials or device. [Signed and dated]". Your course instructors will let you know where to find copies of old exams, if they are available.

[In addition, the specific ethics guidelines for this course are:
(1) (Insert unique rules here, such as your policy regarding collaboration on assignments or use of old exams.)
(2) (etc.)]
Report any violations you witness to the instructor.

You can find more information about university misconduct policies on the web at these sites:

- For undergraduates: http://e-catalog.jhu.edu/undergrad-students/student-life-policies/
- For graduate students: http://e-catalog.jhu.edu/grad-students/graduate-specific-policies/

Students with Disabilities

Any student with a disability who may need accommodations in this class must obtain an accommodation letter from Student Disability Services, 385 Garland, (410) 516-4720, studentdisabilityservices@jhu.edu .

ABET Outcomes

- An ability to apply knowledge of computing and mathematics appropriate to the discipline (a)
- An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution (b)
- An ability to design, implement, and evaluate a computer-based system, process, component, or program to meet desired needs (c)
- An ability to function effectively on teams to accomplish a common goal (d)
- An understanding of professional, ethical, legal, security and social issues and responsibilities (e)
- An ability to communicate effectively with a range of audiences (f)
- An ability to analyze the local and global impact of computing on individuals, organizations and society (g)
- Recognition of the need for and an ability to engage in continuing professional development (h)
- An ability to use current techniques, skills, and tools necessary for computing practice (i)
- An ability to apply mathematical foundations, algorithmic principles, and computer science theory in the modeling and design of computer-based systems in a way that demonstrates comprehension of the tradeoffs involved in design choices (j)
- An ability to apply design and development principles in the construction of software systems of varying complexity (k)