REGIS UNIVERSITY

COLLEGE OF COMPUTER & INFORMATION SCIENCES

Syllabus

Course Title: Ethical Hacking and Defense
Course Number: CN 462

Course Description:

Explores security threats and vulnerabilities that face computer network engineers by using penetration testing techniques. Examines requirements for a formal hacking lab and discusses ethical boundaries between white and black hat hacking.

Prerequisite Courses:

CN 461 Fundamentals of E-Security II

Course Overview

This course exposes the student to online threats and vulnerabilities through the use of penetration testing techniques. This very hands on approach introduces the students to the tools and techniques that are used by both white hat and black hat hackers, and examines the ethics of penetration testing.

Key concepts to be covered in this course include:

- Creating and using penetration testing targets in Lab
- Penetration testing metrics
- Security issues in ubiquitous computing
- Running a penetration test

Course Outcomes:

Upon completion of this course, learners should be able to:

- Explore the security threats and vulnerabilities that face computer network engineers by using penetration testing techniques
- Identify and analyze a formal hacking lab that will demonstrate and allow the student to document vulnerabilities within the network
- Analyze ethical boundaries to demonstrate and understand what is necessary and appropriate when conducting penetration tests

Course Materials:

Required Texts:

Wilhelm, T. (2013). *Professional Penetration Testing: Volume 1: Creating and Learning in a Hacking Lab* (2nd ed.): Syngress. ISBN 1597499935, 978-1597499934.

American Psychological Association. (2010). *Publication Manual of the American Psychological Association (6th ed.).* Washington, DC: American Psychological Association. ISBN 1433805618, 978-1433805615. Companion website: http://www.apastyle.org.

Required Resources:

The following resources are provided for you in the online Course Resources folder. Make certain you can access the all of these course materials/files the first day of this online course. Should any of these files not be successfully accessed, contact your facilitator immediately so alternative methods can be arranged. You will have access to this course the Friday prior to the start date/first day of the class. The following Supplemental Resources are provided for you in the Course Resources folder in WorldClass.

- Essential Writing Knowledge
- General APA Guidelines v6
- Electronic Resources Citations v6
- Reference Book Citations Methods v6
- Supplemental APA Resources

Technology Tools:

The labs are designed to run either as a live CD or as a virtualized computer using a software package such as VMware, Parallels, or Virtual Box. Different parts of the DVD that accompanies the text have different system requirements. While it is possible to run the different LiveCDs and Virtual Machine images on some low end systems, the following system specifications are recommended minimum requirements:

Minimum Requirements for Live CDs

- 800MHz x86 processor Intel-based processor
- 1 Gigabyte (GB) RAM
- Graphics card capable of 1024x768 resolution
- Sound card
- A network or Internet connection
- A DVD drive

Minimum Requirements for Virtualization

- 1 GHz processor (2 GHz or higher recommended)

- 1 GB RAM (2 GB or higher recommended)
- 10 GB available hard disk space (30 GB recommended)

Pre-Assignment:

Online Format: Sign on to D2L (Home Page) and become familiar with the course navigation of the Web Curriculum. Read Chapters 1, 2, & 3 of Wilhelm text. Review Personal Ethics Statement.

Classroom-based Format: Read Chapters 1, 2, & 3 of Wilhelm text. Review Personal Ethics Statement. Instructor will make assignments.

Pre-Assignment Due Dates:

Classroom-based Format: This assignment is due the first night of class.

Online Format: The instructor will specify the due date for this assignment.

Course Assignments and Activities:

	Topics	Readings	Activities Assignments and Associated Points
1	Preparing for Penetration Test	Text : Chapters 1, 2 & 3	Class Discussion: • Introductions Written Assignment: • Personal Ethics Statement Paper (100 points)
2	Creating and Using Penetration Testing Targets in Lab	White Paper: Stajano, F. (2009). Understanding scam victims: seven principles for systems security. London, UK. University of Cambridge Computer Laboratory OR http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-754.pdf Text: Chapter 4	Class Discussion: • Creating a personal lab using VMware (25 points)
3	Penetration Testing Metrics	Text: Chapter 7 View DVD in back of book- "Heorot.net Penetration Testing Fundamentals Course" Banco do Brazil Case Study	Class Discussion: • Team Work: Risk Analysis for Banco de Brazil (25 points)

4	Security Issues in Ubiquitous Computing	White Paper: Stajano, F. Security issues in ubiquitous computing. (2009)	Class Discussion: • Securing Hand Held Device Network Access (25 points) Written Assignment: • Midterm Paper-Mobile Devices Paper (100 points)
5	Running a Penetration Test – Part One	Text: Chapters 9, 10 & 11	Lab (25 points)
6	Running a Penetration Test – Part two	Text: Chapter 12, 13 & 14	Lab – Pen Tests (25 points)
7	Wrapping Everything Up	Text: Chapters 15 & 16	Review Lab (25 points)
8	Final Presentation	Text: Chapters 17 & 18	Class Discussion: • Final Discussion (25 points) Written Assignment: • Penetration Testing Paper (200 points) • Peer Report and Evaluation (25 points) Penetration Testing – Oral Presentation (100 points)
			Maximum Points Possible: 700

Course Policies and Procedures

CC&IS Grading Scale

Letter Grade	Percentage	Grade Point
A	93 to 100	4.00
A–	90 to less than 93	3.67
B+	87 to less than 90	3.33
B	83 to less than 87	3.00
B–	80 to less than 83	2.67
C+	77 to less than 80	2.33
C	73 to less than 77	2.00
C–	70 to less than 73	1.67
D+	67 to less than 70	1.33
D	63 to less than 67	1.00
D-	60 to less than 63	.67
F	Less than 60	0

Additional information about grading can be found in the latest edition of the University Catalog, available at http://www.regis.edu/Academics/Course%20Catalog.aspx.

CC&IS Policies and Procedures

Each of the following CC&IS Policies & Procedures is incorporated here by reference. Students are expected to review this information each term, and agree to the policies and procedures as identified here and specified in the latest edition of the University Catalog, available at http://www.regis.edu/Academics/Course%20Catalog.aspx or at the link provided.

- The CC&IS Academic Integrity Policy.
- The Student Honor Code and Student Standards of Conduct.
- Incomplete Grade Policy, Pass / No Pass Grades, Grade Reports.
- The Information Privacy policy and FERPA. For more information regarding FERPA, visit the U.S. Department of Education.
- The HIPPA policies for protected health information. The complete Regis University HIPAA Privacy & Security policy can be found here: http://www.regis.edu/About-Regis-University/University-Offices-and-Services/Auxiliary-Business/HIPAA.aspx.
- The Human Subjects Institutional Review Board (IRB) procedures. More information about the IRB and its processes can be found here: http://regis.edu/Academics/Academic-Grants/Proposals/Regis-Information/IRB.aspx.

The CC&IS Policies & Procedures Syllabus Addendum summarizes additional important policies including, Diversity, Equal Access, Disability Services, and Attendance & Participation that apply to every course offered by the College of Computer & Information Sciences at Regis University. A copy of the CC&IS Policies & Procedures Syllabus Addendum can be found here: https://in2.regis.edu/sites/ccis/policies/Repository/CCIS%20Syllabus%20Addendum.docx.