



IT & ENGINEERING SERVICES

TRAINING

PROJECTS

PLACEMENTS

www.engineers3d.com

Penetration Testing and Ethical Hacking

1. Catalog Description (3 credit hours)
Introduction to the principles and techniques associated with the cybersecurity practice known as penetration testing or ethical hacking. The course covers planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The student discovers how system vulnerabilities can be exploited and learns to avoid such problems.
2. Pre-requisites and Co-requisites
Cybersecurity (CIS 3XXX)
3. Course Objectives:
This course teaches students the underlying principles and many of the techniques associated with the cybersecurity practice known as *penetration testing* or *ethical hacking*. Students will learn about the entire penetration testing process including planning, reconnaissance, scanning, exploitation, post-exploitation, and result reporting. The course will provide the fundamental information associated with each of the methods employed and insecurities identified. In all cases, remedial techniques will be explored. Students will develop an excellent understanding of current cybersecurity issues and ways that user, administrator, and programmer errors can lead to exploitable insecurities.
4. Contribution of course to meeting the professional component:
This course provides 2 credit hours of engineering design.
5. Relationship of course to program outcomes:
Skills student will develop in this course Students will learn how to apply knowledge of engineering to security evaluations, design and conduct security assessment experiments and analyze and interpret the resulting data, understand professional and

ethical responsibility, communicate effectively, understand the impact of security practices in a global and societal context, recognize the need for life-long learning in the quickly changing cybersecurity environment, develop knowledge of contemporary cybersecurity issues, and use techniques, skills and modern engineering tools necessary for computer security engineering practice.

6. Teaching Assistant
No TA at this time.
7. Meeting Times
T 7
R 7-8
8. Class/laboratory schedule
Class meetings only, 50 minutes per class
9. Meeting Location
MAEB 211
10. Material and Supply Fees
N/A
11. Textbooks and Software Required
Text: *Hacking Exposed 7: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray, George Kurtz, © 2012, McGraw Hill, ISBN 978-0-07-178028-5.
Software: VirtualBox or VMWare Player, Kali Linux.
12. Recommended Reading
Numerous security-related documents, twitter feeds, and other online information sources.
13. Course Outline (43 lecture hours)
 1. Introduction, software installation, Pre-engagement, scoping
 2. Ethical requirements and legal issues
 3. Penetration test report structure and components
 4. Reconnaissance
 5. DNS, web reconnaissance
 6. TCP, UDP, connections
 7. Scanning using nmap
 8. File transfer protocols: ftp, http, telnet
 9. SSL and TLS encryption
 10. NetBIOS and NFS
 11. Encryption essentials
 12. Windows passwords, hashes
 13. Rainbow tables, linux passwords, hashes with salt
 14. Searching linux and Windows file systems
 15. Metasploit exploitation framework
 16. Use of netcat and pivoting
 17. VOIP
 18. Wireless networks and encryption
 19. Lock picking, master keys, and oracle hacks
 20. Cryptography weaknesses
 21. Http, javascript, and command injection

- 22. Nov 5 (1) Databases, SQL, SQL injection
 - 23. Nov 7 (2) Browser proxies and non-rendered content, cross-site scripting
 - 24. Nov 12 (1) Cross-site scripting and cross-site request forgery
 - 25. Nov 14 (2) Web authentication and session management
 - 26. Nov 19 (1) Mobile device security issues
 - 27. Nov 21 (2) Mobile devices and student presentations
 - 28. Nov 26 (1) Student presentations
 - 29. Dec 3 (1) Student presentations and recap for final exam
14. Attendance and Expectations:
Students are expected to attend every class. University of Florida policy for excused absences applies.
15. Grading:
Grading is based on attendance, lab exercises (in which the student must successfully solve a number of challenge problems (one per week), participation in Sakai discussions, group project grade, and final examination. Group projects will involve either reports on current security issues or contribution to open-source security projects. The final examination will be similar to an industry examination such as SANS GIAC or ECCouncil CEH.
Attendance: 10%
Sakai Discussion Participation: 10%
Lab Exercises: 30%
Group Project: 20%
Final Examination: 30%
16. Grading Scale
- A [90-100]
 - B+ [87-90)
 - B [83-87)
 - B- [80-83)
 - C+ [77-80)
 - C [73-77)
 - C- [70-73)
 - D+ [67-70)
 - D [63-67)
 - D- [60-63)
 - F [0-60)

Note: A C- will not be a qualifying grade for critical tracking courses. In order to graduate, students must have an overall GPA and an upper-division GPA of 2.0 or better (C or better). Note: a C- average is equivalent to a GPA of 1.67, and therefore, it does not satisfy this graduation requirement. For more information on grades and grading policies, please visit:

<http://www.registrar.ufl.edu/catalog/policies/regulationgrades.html>

17. Make-up Exam Policy:

Make-up examinations will be available to all students facing situations for which University of Florida policy requires that a make-up examination be provided.

18. Honesty Policy – All students admitted to the University of Florida have signed a statement of academic honesty committing themselves to be honest in all academic work and understanding that failure to comply with this commitment will result in disciplinary action. This statement is a reminder to uphold your obligation as a UF student and to be honest in all work submitted and exams taken in this course and all others.

19. Accommodation for Students with Disabilities:

Students Requesting classroom accommodation must first register with the Dean of Students Office. That office will provide the student with documentation that he/she must provide to the course instructor when requesting accommodation.

20. UF Counseling Services:

Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:

UF Counseling & Wellness Center, 3190 Radio Rd, 392-1575, psychological and psychiatric services.

Career Resource Center, Reitz Union, 392-1601, career and job search services.

21. Software Use:

All faculty, staff and student of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.