

# EEL 4789—Ethical Hacking and Countermeasures

Department of Electrical & Computer Engineering  
Florida International University  
Spring 2015

**Faculty** : Dr. Alexander Pons  
**Office Hours** : By Appointment only  
**Phone** : 305-348-7253  
**Email** : apons@fiu.edu

**Textbook** : Alfred Basta, Nadine Basta and Mary Brown, *Computer Security and Penetration Testing, 2nd Edition*. Course Technology Incorporated, 2014, ISBN-10: 0840020937. ISBN-13: 9780840020932

## Course Description

No matter what field you work in, you cannot help but notice the impact that the Internet has had on society. It has opened up opportunities and markets that people only dreamed of before. As with any technology, there is always a positive and negative aspect. The positive side is tremendous business opportunities; the business world relies increasingly upon data communications, and modern data networks are based mainly on the Internet. The negative side is the huge security risk that is now posed to so many companies, yet few companies are truly aware of the potential danger.

Information is the asset that must be protected. Without adequate protection or network security, many individuals, businesses, and governments are at risk of losing that asset. It is imperative that all networks be protected from threats and vulnerabilities so that a business can achieve its fullest potential. Security risks cannot be eliminated or prevented completely; however, effective risk management and assessment can significantly minimize the existing security risks.

This course is intended to provide a practical survey of network security applications and standards. The emphasis is on applications that are widely used on the Internet for corporate networks, and on standards that have been widely deployed. It also provides students with the knowledge and skills to begin supporting network security and best practices for implementing security.

## Course Objectives

1. Exposure to security issues in telecommunications and networks.
2. Understanding the design aspects of security including threat identification and risk assessment.
3. Understanding the best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development, forensics, privacy implications, and ethics.
4. Understand different ways of securing Communication.
5. Exposure to various penetration testing tools, maltego, nmap, wireshark, metasploit, openVas, ettercap, john the ripper, etc.
6. Understand the various phases involved in targeting computer networks and systems.

## Topics Covered

1. Ethics of Hacking and Cracking
2. Reconnaissance
3. Scanning Tools
4. Sniffers
5. TCP/IP Vulnerabilities
6. Encryption and Password Cracking
7. Spoofing
8. Session Hijacking
9. Hacking Network Devices
10. Trojan Horses
11. Denial-of-Service Attacks
12. Buffer Overflows
13. Programming Exploits
14. Mail Vulnerabilities
15. Web Application Vulnerabilities
16. Windows Vulnerabilities
17. Linux Vulnerabilities

## Relationship of course to program objectives

In this course, the student will have to show:

1. An ability to apply knowledge of mathematics, science, and engineering,
2. an ability to design and conduct experiments, as well as to analyze and interpret data,
3. an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability,
4. an ability to identify, formulate, and solve engineering problems (homework),
5. the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
6. an ability to communicate effectively (through teamwork),
7. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice,
8. a knowledge of contemporary issues,
9. a knowledge of advanced mathematics.

## Grading Scheme

<b>Assignments</b>	<b>5%</b>
<b>Individual Video Project</b>	<b>20%</b>
<b>Group Research Paper/Project</b>	<b>25%</b>
<b>Midterm Exam</b>	<b>20%</b>
<b>Final Exam</b>	<b>30%</b>
<b>Total</b>	<b>100%</b>

## Tentative Grading Scale

<b>A</b>	<b>100-95</b>	<b>B+</b>	<b>86-89</b>	<b>C+</b>	<b>76-79</b>	<b>D+</b>	<b>66-69</b>	<b>F</b>	<b>0-59</b>
<b>A-</b>	<b>90-94</b>	<b>B</b>	<b>83-85</b>	<b>C</b>	<b>73-75</b>	<b>D</b>	<b>63-65</b>		
		<b>B-</b>	<b>80-82</b>	<b>C-</b>	<b>70-72</b>	<b>D-</b>	<b>60-62</b>		

## **Individual Video Projects**

1. This is an individual project. Just make a video of yourself discussing a topic of your choice that is related to Ethical Hacking and/or other security related issues.
2. Please upload your video to YouTube and submit a copy of your finished video.
3. The assessment is going to be based on the overall quality of the project. For example, if your video is only based on PowerPoint, you will not get full points. PowerPoint accompanied with hands-on demonstration of the topic makes you qualified for the maximum possible points.
4. Following are some guidelines to create and upload the video:
5. You can use video editing software of your own choice.
6. Your face must be completely visible most of the time. This is to make sure that you are the one doing the presentation.
  - a. You can use PowerPoint or any other presentation software.
  - b. The video must be at least 15 minutes long
  - c. Introduce yourself, start with a brief discussion of what is this video about followed by any demo/implementation. In the end properly conclude your video.
  - d. Select a suitable title and description that reflects the content of the video.
  - e. If applicable, video Category should be Education, HowTo, or Science and Technology.
  - f. In order for people to be able to find your video, use proper keywords in the Tag section. You can use your name, instructor name, and any other important keywords.
  - g. In the start of the video, you should announce that you are doing this as a part of Ethical Hacking course, your name, your instructor name and the purpose of the video.
  - h. Try to introduce some humor to make it funny so that people don't get bored.

## **Group Research Paper**

1. The course includes a substantial group project (25%) requiring the review and the implementation of attacks or defenses of a non-trivial network security issue.
2. The group contains 3-4 students working together throughout the semester.
3. Students will give submit the paper in IEEE format and a PowerPoint presentation of the paper, follow link for IEEE format:  
[http://www.ieee.org/conferences\\_events/conferences/publishing/templates.html](http://www.ieee.org/conferences_events/conferences/publishing/templates.html)

## **University's Code of Academic Integrity**

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.

More information can be found at [http://academic.fiu.edu/academic\\_misconduct.html](http://academic.fiu.edu/academic_misconduct.html)

## Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see Instructor. All missed work must be finished before last two weeks of the next term

## University policies on sexual harassment, and religious holidays, and information on services for students with disabilities

Please visit the following websites: <http://academic.fiu.edu/> and <http://drc.fiu.edu>

## Course Policies

- **Attendance:** Attendance in the course is **mandatory** and student is not allowed to miss any class during the semester. There will be a **penalty** for missing classes and it may affect your final grade.
- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (1 point per absence above two, 3 points per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to [apons@fiu.edu](mailto:apons@fiu.edu).
- **On Time:** As in the workplace, on time arrival and preparation are required. Two “lates” are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me by an appointment.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.
- **Any work submitted should display Panther ID number and should be signed, as the students’ own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

## Exam policy

1. Make sure to complete the assigned homework in order to do well in the exam.
2. All exams are closed book and closed notes.
3. The exams will require the use of a computer and access to the Internet, but other electronic devices are not allowed, such as cellphone.
4. No discussion is permitted during the exams, including electronic communications, email, Messaging Services, etc.
5. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

## Class Schedule

<b>Week</b>	<b>Date</b>	<b>Weekly Topic</b>
1	1/12	Class Introduction Chapter 1: Ethics of Hacking and Cracking
2	1/19	Chapter 2: Reconnaissance
3	1/26	Chapter 3: Scanning Tools
4	2/2	Chapter 4: Sniffers
5	2/9	Chapter 5: TCP/IP Vulnerabilities
6	2/16	Chapter 6: Encryption and Password Cracking
7	2/23	Chapter 7: Spoofing
8	3/2	Chapter 8: Session Hijacking <b>Mid Term Exam</b>
9	3/9	<b>Spring Break</b>
10	3/16	Chapter 9: Hacking Network Devices
11	3/23	Chapter 10: Trojan Horses Chapter 11: Denial-of-Service Attacks
12	3/30	Chapter 12: Buffer Overflows Chapter 13: Programming Exploits
13	4/6	Chapter 15: Web Application Vulnerabilities
14	4/13	Chapter 14: Mail Vulnerabilities
15	4/20	Chapter 16: Windows Vulnerabilities Chapter 17: Linux Vulnerabilities
16	4/27	<b>Course Final Exam</b> <b>Group/Paper Presentations</b>