EEL 4806—Ethical Hacking and Countermeasures

Department of Electrical & Computer Engineering

Florida International University

Fall 2018

Classroom	**:**	EC 3239
Class Time	**:**	8:00 am—12:30 pm
Faculty	**:**	Dr. Alexander Pons
Office Hours	**:**	T & R 10:00-12:00 am or by Appointment
Office	**:**	EC 3145
Phone	**:**	305-348-7253
Email	**:**	apons@fiu.edu
Prerequisite	**:**	EEL 2880 or COP 2210 or permission from instructor
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.

Topics Covered

- Ethics of Hacking and Cracking
- Ethical issues, social responsibility and decision tools
- Cyber crimes
- Cyber Crime types , Stalking, Bullying, Identity Theft, Terrorism, Crime Laws
- Reconnaissance
- Scanning Tools
- Sniffers
- TCP/IP Vulnerabilities
- Encryption and Password Cracking
- Spoofing
- Session Hijacking
- Hacking Network Devices
- Trojan Horses
- Denial-of-Service Attacks
- Buffer Overflows
- Programming Exploits
- Mail Vulnerabilities
- Web Application Vulnerabilities
- Windows & Linux Vulnerabilities
- Patching (OS and Applications)

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

Homework/Labs	**15%**
Weekly Quizzes	**10%**
Hack Case Project/Video	**15%**
Midterm Exam	**30%**
Final Exam	**30%**
Total	**100%**

Tentative Grading Scale

A	**100-95**	**B+**	**86-89**	**C+**	**74-77**	**D**	**60-69**
A-	**90-94**	**B**	**82-85**	**C**	**70-73**	**F**	**0-59**
		B-	**78-81**				

Tentative Dates

- **Final Exam** is scheduled on the last Wednesday of the semester.

Tutorial/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 on a CD/USB attached to a paper copy of the tutorial.
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.

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

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.
- **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, except when instructed to do so.
- 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. Use of any electronic device with keyboard is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

Class Schedule

Once a week, 240 minutes each session: Wednesday

Week	Date	Weekly Topic
1	8/20 (8/22)	Class Introduction Chapter 1: Ethics of Hacking and Cracking Chapter 2: Reconnaissance Assign Lab 1
2	8/27 (8/29)	Chapter 3: Scanning Tools Chapter 4: Sniffers Chapter 5: TCP/IP Vulnerabilities Take Quiz 1(chapters 1 and 2) Lab 1 due before class begins Assign Lab 2 Turn-in Individual tutorial proposal.
3	9/3 (9/5)	Chapter 6: Encryption and Password Cracking Chapter 7: Spoofing Chapter 8: Session Hijacking Take Quiz 2 (chapters 3, 4 and 5) Lab 2 due before class begins Assign Lab 3
4	9/10 (9/12)	**Mid Term Exam** Chapter 9: Hacking Network Devices Chapter 10: Trojan Horses Take Quiz 3 (chapters 6, 7 and 8) online before midterm Lab 3 due before class begins Assign Lab 4
5	9/17 (9/19)	Chapter 11: Denial-of-Service Attacks Chapter 12: Buffer Overflows Take Quiz 4 (chapters 9 and 10) Lab 4 due before class begins Assign Lab 5 Turn-in Individual tutorial script draft.
6	9/24 (9/26)	Chapter 13: Programming Exploits Chapter 14: Mail Vulnerabilities Take Quiz 5 (chapters 11 and 12) Lab 5 due before class begins Assign Lab 6
7	10/1 (10/3)	Chapter 15: Web Application Vulnerabilities Chapter 16: Windows Vulnerabilities Chapter 17: Linux Vulnerabilities Take Quiz 6 (chapter 13 and 14) Lab 6 due before class begins Assign Lab 7
8	10/8 (10/10)	Take Quiz 7 (chapter 15, 16 and 17) online before final Lab 7 due before class begins **Course Final Exam**
	10/8 (midnight)	Due: Tutorial and Video (upload to shared drive folder)

Course Hands-on Labs

Lab 1 – Open Source Intelligence (OSINT) or Reconnaissance
Using publicly available data conduct information gathering in the form of Email address, phone numbers, IPs, OS info, software versions, Geo locations, business or personal details, etc. **Tools:** Google Dorks, Wayback machine, Whos.is, Netcraft, Host, NSLookup, dig, Maltego, IP2location, HTTrack, Email Harvester.
Lab 2 – Network Enumeration and Port Scanning
Determine which systems are accessible and the services/ports that are accessible with an active connection to target hosts. Rendering and discovering potential attack vectors in the system. Determine IP tables, port status, active services, banners, hostnames, settings, etc. **Tools:** netdiscover, ping, fping, hping3, Nmap/Zenmap, OpenVas, Nessus and CVE information https://CVEDetails.com and National Vulnerability Database https://nvd.nist.gov/vuln/search.
Lab 3 – Password Cracking and Packet Sniffing
Perform offline and online password cracking applying dictionary, brute force, and rainbow table attacks. Capturing data transmitted over a network (wired or wireless) looking for protocol and http traffic. **Tools:** Cain and Abel, John the Ripper, The Hydra, Medusa, OphCrack, Wfuzz, Brutus, Wireshark and Tcpdump.
Lab 4 – System Exploitation with Metasploit
From the discovered CVEs in Lab 2, identify know vulnerabilities and associated Metasploit exploits and payloads to compromise the target system. Lean to use Meterpreter a module of Metasploit that works on the principle of DLL injection. Use Meterpreter to get shell access to the system and run a list of Meterpreter commands. **Tools:** Metasploit, msfconsole, and Armitage
Lab 5 – Buffer Overflow and Steganography
Determine the conditions for a buffer overflow to occur and use Steganography to demonstrate the manner to hide messages within a picture or other media.
Lab 6 – Man-in-the-Middle (MitM)
Perform a MitM attack by using ARP poising and capture images, Urls and web content using Driftnet and SSLStrip to remove security from an https site. **Tools:** Etttercap, arpspoof, driftnet and SSLStrip.
Lab 7 –Web Hacking
Identify website vulnerabilities and attempt to exploit them using various tools. Perform SQL injection, web proxy, and Cross-Site Scripting (XSS) attacks. Tools: Nitko, W3af, WebScarp, OWASP-Zap and Social Engineering Toolkit (SET).