EEL4806 - Ethical Hacking and Countermeasures
Three Credits, Four and a half hours, Engineering Topic.

Instructor: Dr. Alexander Pons.


Specific Course Information:
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.

Specific Goals for the Course
a. Specific outcomes of instruction
   Upon successful completion of this course, the student will:
   1. Assess the difference between ethical and unethical hacking and the ethics involved.
   2. Describe the basic concepts, protocols, and techniques required for networking communications.
   3. Assess the security issues in telecommunication and networks.
   4. Evaluate the techniques employed during reconnaissance and tools that facilitated the discovery of information.
   5. Evaluate the tools and techniques to conduct network scanning and collect potential system vulnerabilities.
   6. Evaluate the information obtained during system enumeration and which tools are applicable.
   7. Evaluate different vulnerabilities and measure how hackers exploit these vulnerabilities to enter networks as well as to perform privilege escalation.
   8. Analyze how malware is categorized and the manner it is investigated to gain insight on its behavior.
   9. Apply different techniques to capture network packets and dissect them using Wireshark.
   10. Evaluate the effectiveness of several types of social engineering attacks and potential mitigation actions.
   11. Assess the security aspect of wireless communications, in the form of Wi-Fi and Bluetooth, including tools employed for their exploitation.
   12. Apply best practices and guidelines for developing and verifying effective security policies and procedures, security goals, threats and vulnerabilities, standards and security policy development.
   13. Analyze the different ways of securing Communication and the various threat agents.
   14. Describe various enterprise security models and security architecture.

b. Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.
   In this course the student will have to show
   (a) an ability to apply knowledge of mathematics, science, and engineering (X)
   (b) an ability to design and conduct experiments (simulations), as well as to analyze, interpret data (X)
   (c) an ability to design a system, component, or process to meet desired needs (X)
(d) an ability to function in multi-disciplinary teams (N/A)
(e) an ability to identify, formulate, and solve engineering problems (homework) (X)
(f) an understanding of professional and ethical responsibility (X)
(g) an ability to communicate effectively (through project reports) (N/A)
(h) the broad education necessary to understand the impact of engineering solutions in a global and societal context (X)
(i) a recognition of the need, and an ability to engage in life-long learning (N/A)
(j) a knowledge of contemporary issues (X)
(k) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice (X)
(l) a knowledge of probability and statistics (X)

**Brief list of the topics to be covered**

1. Ethics of Hacking and Cracking
2. Ethical issues, social responsibility and decision tools
3. Cyber crimes
4. Cyber Crime types, Stalking, Bullying, Identity Theft, Terrorism, Crime Laws
5. Reconnaissance
6. Scanning Tools
7. Sniffers
8. TCP/IP Vulnerabilities
9. Encryption and Password Cracking
10. Spoofing
11. Session Hijacking
12. Hacking Network Devices
13. Trojan Horses
14. Denial-of-Service Attacks
15. Buffer Overflows
16. Programming Exploits
17. Mail Vulnerabilities
18. Web Application Vulnerabilities
19. Windows & Linux Vulnerabilities
20. Patching (OS and Applications)

**GRADING:**

<table>
<thead>
<tr>
<th>Course Requirements</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Quizzes</td>
<td>5%</td>
</tr>
<tr>
<td>Assignments</td>
<td>25%</td>
</tr>
<tr>
<td>Midterm Exam</td>
<td>35%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>35%</td>
</tr>
<tr>
<td>Overall Grade</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Conversion of Numerical Grade to Letter Grade**

<table>
<thead>
<tr>
<th>Numerical Grade</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>90&lt;=A&lt;=100</td>
<td>A</td>
</tr>
<tr>
<td>82&lt;=B&lt;85</td>
<td>B</td>
</tr>
<tr>
<td>70&lt;=C&lt;73</td>
<td>C</td>
</tr>
<tr>
<td>90&lt;=A&lt;94</td>
<td>A-</td>
</tr>
<tr>
<td>78&lt;=B&lt;81</td>
<td>B-</td>
</tr>
<tr>
<td>60&lt;=D&lt;69</td>
<td>D</td>
</tr>
<tr>
<td>86&lt;=B+&lt;89</td>
<td>B+</td>
</tr>
<tr>
<td>74&lt;=C+&lt;77</td>
<td>C+</td>
</tr>
<tr>
<td>70&lt;=C&lt;73</td>
<td>C</td>
</tr>
<tr>
<td>F: Below 60</td>
<td>F</td>
</tr>
</tbody>
</table>