Information is a critical asset in both corporate and military environments. Computer networks that carry this information are the "lifeblood" of these organizations. Information and network security is an important topic in order to insure that these networks remain available, are resistant to attacks and protect the information that they carry.

This course introduces the student to the fundamentals of creating a secure networking environment and will cover the topics of hacking, attack methodologies, firewalls, IDS, VPNs, cryptography and wireless networking.

Learning Objectives

Upon completion of this course you will have acquired the following knowledge:

- Understand hacking techniques.
- Understand the fundamentals of secure network design.
- Understand the issues involved with providing secure networks.
- Understand underlying cryptography required for secure communications, authorization and authorization.
- Obtain hands on experience in cryptography and network security through laboratory work.

Instructor:

Phillip Mak

Email: pmak@nyu.edu

Skype: phillip.mak

Please do email me any suggestions, questions, topics, or interesting tidbits or articles you may have, which I will try go over them at the next class. This allows me to talk about topics that you have an interest with.
Office Hours: By appointment on Skype or phone.

Prerequisites:

Good working knowledge of networking and TCP/IP (e.g., CS 6843, EL5363/5373)
Basic understanding of operating systems with a working knowledge of Linux (e.g., CS6233)

Textbook:
No textbook assigned. Reading materials will be regularly assigned and posted on NYU Classes.

Grades:
10% Homework & Quizzes
30% Labs
30% Midterm
30% Final
~2% Bonus
Late assignments are not accepted.

Bonus - Class Participation
Bonus points may be given to active participants in this class, be it live during lecture or afterwards

Class Schedule
Weekly Webinar – Mondays 7-9PM on "WebEx"

Course Structure
Each week, lesson slides and reading materials will be posted before the lecture. Students are expected to review the materials before class, and the class time will be used to go over items of particular interest, confusion, or difficulty. Please be prepared for lecture to obtain the most out of this class. The video will be posted online.

Online Class Expectations

An online environment has different interaction model than a regular in-person class. Online classes, students need to be significantly more proactive by asking questions and letting me know if there are any topics of confusion.

Policies

The exact topics listed in this syllabus are subject to change. As the class progresses we will gauge where your interests lie and may adjust the topics and schedule appropriately.

If you need help or have any questions do not hesitate to contact me. If you would like to have a phone or skype video conversation please email to setup a time. You will have ample time from the time an assignment is given until it is due. I will not consider a network outage, unavailability of your computer or a computer in the lab (whether a specific computer or any computer in general), or other computer problem that occurred the night before the due date to be a justification for submitting an assignment late. However, systemic lab problems will be accounted for. Lab issues should be taken up with the lab admin whom you will receive contact information.

Interaction Policy

The best way to reach me is by email, which I generally respond very quickly. In addition, you can ask questions during the lecture time. Otherwise, I prefer course related questions to be asked in the Forums for the benefit of other students in the class.

Week  Date    Lesson
1    Mon, 10 Sept    Lesson 0: Introduction, Expectations, and Policies
Lesson 1: Security Basics: Terms & Definitions, Risk Assessment
2    Mon, 17 Sept    Lesson 2: Recon
3    Mon, 24 Sept    Lesson 3: Vulnerabilities and Exploits Part I
4    Mon, 1 Oct     Lesson 3: Vulnerabilities and Exploits Part II
     Mon, 8 Oct     NO CLASS - Fall Recess
5    Tue, 9 Oct     Lesson 4: Attacks - Owning the Box, Post-Exploitation
<table>
<thead>
<tr>
<th></th>
<th></th>
<th>Lesson</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Mon, 15 Oct</td>
<td>Lesson 5: Cryptography - Randomness, Primes, RSA, DH</td>
</tr>
<tr>
<td></td>
<td>Mon, 22 Oct</td>
<td>NO CLASS - Exam Week</td>
</tr>
<tr>
<td></td>
<td>Sat, 27 Oct</td>
<td>MIDTERM on Lessons 1-5 Only</td>
</tr>
<tr>
<td>7</td>
<td>Mon, 29 Oct</td>
<td>Lesson 6: Message Integrity, PKI and TLS Part I</td>
</tr>
<tr>
<td>8</td>
<td>Mon, 5 Nov</td>
<td>Lesson 6: Message Integrity, PKI and TLS Part II</td>
</tr>
<tr>
<td>9</td>
<td>Mon, 12 Nov</td>
<td>Lesson 7: Layer 2 Security</td>
</tr>
</tbody>
</table>

Lesson 8: IPSec, Firewalls, and IDS

|   | Mon, 19 Nov | Lesson 9: Authentication                                               |
| 10| Mon, 26 Nov | Lesson 10: Wireless Security                                            |
| 11| Mon, 3 Dec  | Lesson 11: IPv6 Security                                                |
| 12| Mon, 10 Dec | Final Review                                                           |
| 13| Sat, 15 Dec | FINAL EXAM on Lesson 6-11                                               |
Learning Time for NYU Tandon Online Courses

Moses Center Statement of Disability

NYU School of Engineering Policies and Procedures on Academic Misconduct