# New York University Polytechnic School of Engineering

Computer Science
Course Outline CS-GY 6823/CS-UY3933 Network Security
**Fall 2018**
**Professor Thomas Reddington**
Wednesday 12:25 – 2:55; RGSH 215

To contact professor: treddington@nyu.edu
Office hours: by appointment

# Network Security CS 6823/3933

**Graduate Assistants**

| | |
|---|---|
| Shanmathi Chockalinggam | sc6677@nyu.edu |
| Geet Pradhan | grp270@nyu.edu |

**Overview**:
Information is a critical asset in both the corporate/business environment as well as the military. The computer networks that carry this information are becoming the "lifeblood" of these government and private sector organizations. Network security is an increasingly important topic in order to insure that these mission critical networks remain available and are resistant to malicious use and attack.

In order to use a network a computer user relies on a number of services in the network This course introduces the student to the fundamentals of the security of those network services and how to establish a secure networking environment. As cryptography is an essential tool in providing many network services we will touch on cryptography in this course.

The emphasis will be on practical concepts such as attack methodologies, forensics defensive techniques and tools such as IDS, firewalls, VPNs, etc. which are used to design and build a secure network. The student is expected to write short Python/SCAPY programs in a provided lab environment that illustrate the security of network services and their protocols.

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

- A firm grasp on how networks are attacked and techniques used.
- An understating of the inherent insecurity of networking and networking protocols.
- Understand the fundamentals of secure network design
- Foundation of the issues involved in providing secure network communications
- Understand the underlying cryptography required for electronic commerce, secure communications and authentication
- Obtain hands on understanding of network security through laboratory work.

**Textbooks**:
Counter Hack Reloaded: A Step-by-Step Guide to Computer Attacks and Effective Defenses (2nd Edition) Edward Skoudis ISBN: 978-0131481046
Linux Firewalls: Attack Detection Response with IPtables, SNORT, PSAD and FWSNORT Michael Rash, ISBN-10: 1-59327-141-7 ISBN-13: 978-1-59327-141-7

**Prerequisites**:
EL 5373 or CS 6843
A good foundation in networking and MAC/TCP/IP. If you have not taken Graduate Networking as a course you should not be taking this course.

**References**:
Internetworking with TCP/IP Vol1 5th Edition, Doug Comer
Operating Systems Concepts, Silbershatz, Galvin & Gagne
Troubleshooting with Wireshark, Laura Chappell, ISBN-10: 1-893939-97-9, ISBN-13 978-1-893939-97-4

Basic Understanding of Operating Systems with a working knowledge of Linux

To succeed in this course, you should be very familiar with how networking works at layers 2, 3 and 4. i.e Ethernet, IP, TCP/UDP. You should also have a working knowledge of Linux.

- Specifically, at the Ethernet layer what is ARP? What is an ARP table? How does switching work in a bridge/switch? What is a CAM table in a switch? How do Ethernet frames carry IP packets?
- At the IP layer, what is IP identification used for? What is TTL? What is the Fragment Offset and how is it used? How does routing work? What is the difference between switching and routing?
- At the TCP layer what are ports? What is the sequence number used for? What is the handshaking that is done to setup a TCP connection?

Laboratory Work: Periodic laboratory work will be assigned to reinforce the concepts that we are covering each week. The equipment in the NYU Poly virtual lab environment will be used. You will document any research performed (sources of all research must be cited), methodology which was followed to achieve the result, copies of pertinent equipment configurations and diagrams of network topologies. Most of the labs require knowledge of how to use wireshark.

Each assignment will be submitted as a single pdf (all screen shots and code in one file) file with the following file name format <Last Name_First Name_NID_LabXX>. The last file submitted before the deadline will be considered for grading.

Grades:
10% HW
30% Lab
30% Midterm
30% Final

**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 topics and schedule appropriately. Specifically we are using SCAPY so brush up on your Python programming. Given time I will introduce additional labs using SCAPY.

All homework and laboratory assignments are due on the date indicated on the course website. **Late assignments will not be accepted** (believe it) so don't ask for an extension if you are late. Failure to submit an assignment will result in a grade of zero for that assignment. You will have ample time from the time an assignment is given until it is due. We 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. You may assume that there will be one lab and/or homework for each lecture.

**Individual Work and Collaboration**

In preparing your submissions for homework and laboratory projects you are authorized to use the textbook, your notes, web sites, on-line documentation and any other reference materials to which you have access. You may also discuss the assignment in general with other members of the class or with anyone else whom you believe can be of assistance (including possibly the instructor).

The work that you submit for grading **must**, however, be exclusively your own work. If you do obtain assistance from another individual, you must include an explicit note to that effect in your submission for the assignment. Further all references used must be cited. This means that if you are using various web sites for assistance in laboratory assignments and/or homework you must cite the exact URLs. In addition, any other printed material used must be explicitly cited.

See: https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/academic-integrity-for-students-at-nyu.html

**Moses Center Statement of Disability**

If you are student with a disability who is requesting accommodations, please contact New York University's Moses Center for Students with Disabilities at 212-998-4980 or mosescsd@nyu.edu. You must be registered with CSD to receive accommodations. Information about the Moses Center can be found at www.nyu.edu/csd. The Moses Center is located at 726 Broadway on the 2nd floor.

**Schedule**

| Lectures | Date | Topic |
|---|---|---|
| 1 | 5-Sep | Introduction to Security |
| 2 | 12-Sep | SCAPY, Review of IP networks |
| 3 | 19-Sep | Reconnaissance |
| 4 | 26-Sep | Layer 2 (Ethernet) insecurities and protections |
| 5 | 3-Oct | Layer 3 (IPv4) Insecurities and protections |
| 6 | 10-Oct | Layer 4 (TCP, UDP) Insecurities and protections |
| 7 | 17-Oct | Cryptography - Kerckhoff's Principle, Randomness, Primes, DH, PKI |
| 8 | 24-Oct | Midterm |
| 9 | 31-Oct | Layer 4 (IPSec, PKI continued, SSL, TLS) |
| 10 | 7-Nov | Firewalls – IPtables |
| 11 | 14-Nov | IPtables continued |
| 12 | 21-Nov | Thanksgiving Break |
| 13 | 28-Nov | Monitoring, IDS/IPS, FWSNORT, Network Monitors |
| 14 | 5-Dec | Wireless Security |
| 15 | 12-Dec | IPv6 |
|  | 19-Dec | Final Exam |