NYU TANDON SCHOOL OF ENGINEERING

Network Security

Spring 2025

CS 6823 - Lecture 0
Introduction, Expectations, and Policies

Phillip Mak
pmak@nyu.edu

Who am I?

- Phillip Mak
  - Cybersecurity Officer at a major international organization
  - Formally Security Operations Center Lead at a large government agency
  - Formally 12 years career as Cybersecurity Lead at the Department of Defense
  - Network Communications Intern at N.Y.S.E
  - Provide systems and security engineering services to Army programs during the development lifecycle
  - Cybersecurity monitoring during live operational testing of networked system
  - Cybersecurity protections for DoD systems

Course Organization

WARNING

You will be learning potentially dangerous techniques in this course. By continuing the beyond this point you agree that all of the knowledge gained will be used in an ethical manner.

The point of this course is to learn about network security not to harm people or systems. If you do, you will end up in jail and I won't be able to (or will) save you.

Contact Information

- The best way to reach me by email:
  - pmak@nyu.edu

- Office hours: By appointment on Slack
  - Send me a message with your availability
  - Let me know if you prefer voice or video
  - Feel free to make an appointment for general discussions.

- Slack
  - You can also send me a message anytime on Slack, but that's more informal.

- 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.

Course Website

- https://brightspace.nyu.edu/d2l/home/444512

- Assignments are located on Gradescope
  - An account has been created for you

- **Syllabus** - subject to change so check the NYU Classes "Syllabus"
- **Lecture Slides** - will be posted prior to class. Students must review the slides before the corresponding lecture
- **Assigned Readings** are typically news and research articles related to current events in Cybersecurity

SEED Labs

- Allows usage and practice of security tools in a controlled environment on your own computer.
- We are using version **SEED 2.0: Ubuntu 20.04 VM (64-bit)**
- SEED website: https://seedsecuritylabs.org/labsetup.html

Virtual Box (Windows & non-Apple Silicon Macs):
- Download SEED-Ubuntu20.04.zip
- VM Manual: follow this manual to install the VM on your computer

VMWare Fusion (Apple Silicon Macs (M-series Macs))
- For Apple Silicon Macs, follow the instructions here: https://github.com/seed-labs/seed-labs/tree/master/lab-setup/apple-arm#building-the-seed-vm-on-fusion

Cloud Version:
- Alternatively, you can use the cloud version. I recommend DigitalOcean. It's a guaranteed $12/month -- no overages -- so it'll be $48 for the semester. Currently, there is a promotion of $100 credit via the GitHub Student Developers program if you sign up using your NYU email address: https://www.digitalocean.com/github-students/

- Instructions: https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/seedvm-cloud.md

- **Tip**: You will need a US IP address when signing up. Use the NYU VPN. You already have an account, just follow the instructions to download the client and sign in.
- **Tip 2**: Some students had better performance with the $24/mo plan, but it's not required.

- If this is your only option, and you do not have the financial means for the subscription, you may apply to the NYU Student Emergency Fund for cases when students face unexpected emergencies that have impacted their financial situation.

Course Goals

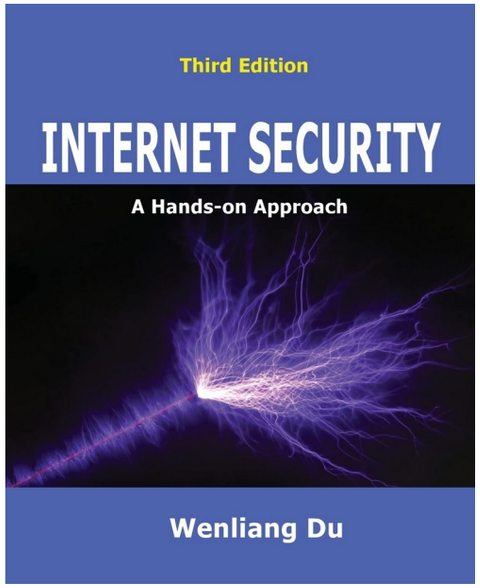
- Understand the problems of securing a network

- Understand the underlying protocols and technologies
  - Crypto, IPsec, TLS

- Examine the methods and tools for attacking and defending a network
  - network reconnaissance, enumeration, exploits, tools.
  - defense tools (firewalls, ids, router, switches, wireless)

- Explore some advanced topics
  - E.g., Firewalls, Wireless

Textbook



Internet Security: A Hands-on Approach
Wenliang Du
ISBN: 978-1733003964
Published: 2022
Amazon link

Reading materials (such as URLs, papers, news articles) will be regularly assigned and posted on NYU Classes. These materials may be on the exam.

Prerequisites

- Good Foundation in Networking and TCP/IP. CS 684 or equivalent course in computer networking.
  - *Reference: Internetworking with TCP/IP, Vol 1, 5th Edition, Doug Comer*

- Basic understanding of operating systems with a working knowledge of Linux.

Course Policies

- 10% Homework & Quizzes
- 40% Labs
- 25% Midterm
- 25% Final
- 2% Weekly Bonus

- Bonus points given for optional weekly exercises

- Labs & Homeworks have a varying due date. Extra percentage points for submitting early and deducted for lateness.
- Exceptions
  - -Family/Personal/Medical – Excused Absence Form
  - -Work emergency: Speak to Prof. Mak
- Academic Dishonesty/Plagiarism policy – Don't do it
  - -https://www.nyu.edu/about/policies-guidelines-compliance/policies-and-guidelines/academic-integrity-for-students-at-nyu.html

Usage of Generative AI

- Welcomed to use generative AI tools (e.g. ChatGPT, etc.) for idea generation only in labs and assignments.
  - **Not allowed for exams**
- You are responsible for the information submitted
  - for instance: that it does not violate intellectual property laws, or contain misinformation or unethical content
  - No personal information
- must be properly documented and cited in each case
  - E.g. quote + [paragraph from ChatGPT]
- Must not violate NYU's Academic Integrity Policy, which forbids "submitting work (papers, homework assignments, computer programs, experimental results, artwork, etc.) that was created by another, substantially or in whole, as one's own."

Weekly Exercises – Bonus (Optional)

- During lecture each week, there are optional exercises during the lecture
- Submit responses in the “Week X Exercises” assignments
- Weekly Exercises are due 2 hours prior to the next class
- Total bonus would be an additional 2 percentage points added to the top of the final course grade

Course Expectations

Learning Time Element	Asynchronous* / Synchronous**	Time on Task for Students (weekly)	Notes
Lecture	Asynchronous	2 - 3 hours	Attending live lecture or view recordings. Although asynchronous, must be performed within a week.
Research	Asynchronous	3	Learners review background materials to understand concepts discussed in the lecture slides.
Readings	Asynchronous	1	Learners complete recommended readings (online journal articles and tutorials).
Lab Assignments	Asynchronous	6	Learners independently complete lab assignments using the SEED Virtual Machines, which can include scapy coding and troubleshooting programs, setting up networks, sniffing traffic, and writing firewall rules.
Homeworks	Asynchronous	1	Learners independently complete homework assignments, which typically consists of multiple choice, short answers, and Immersive Labs activities.

Prepping for Class

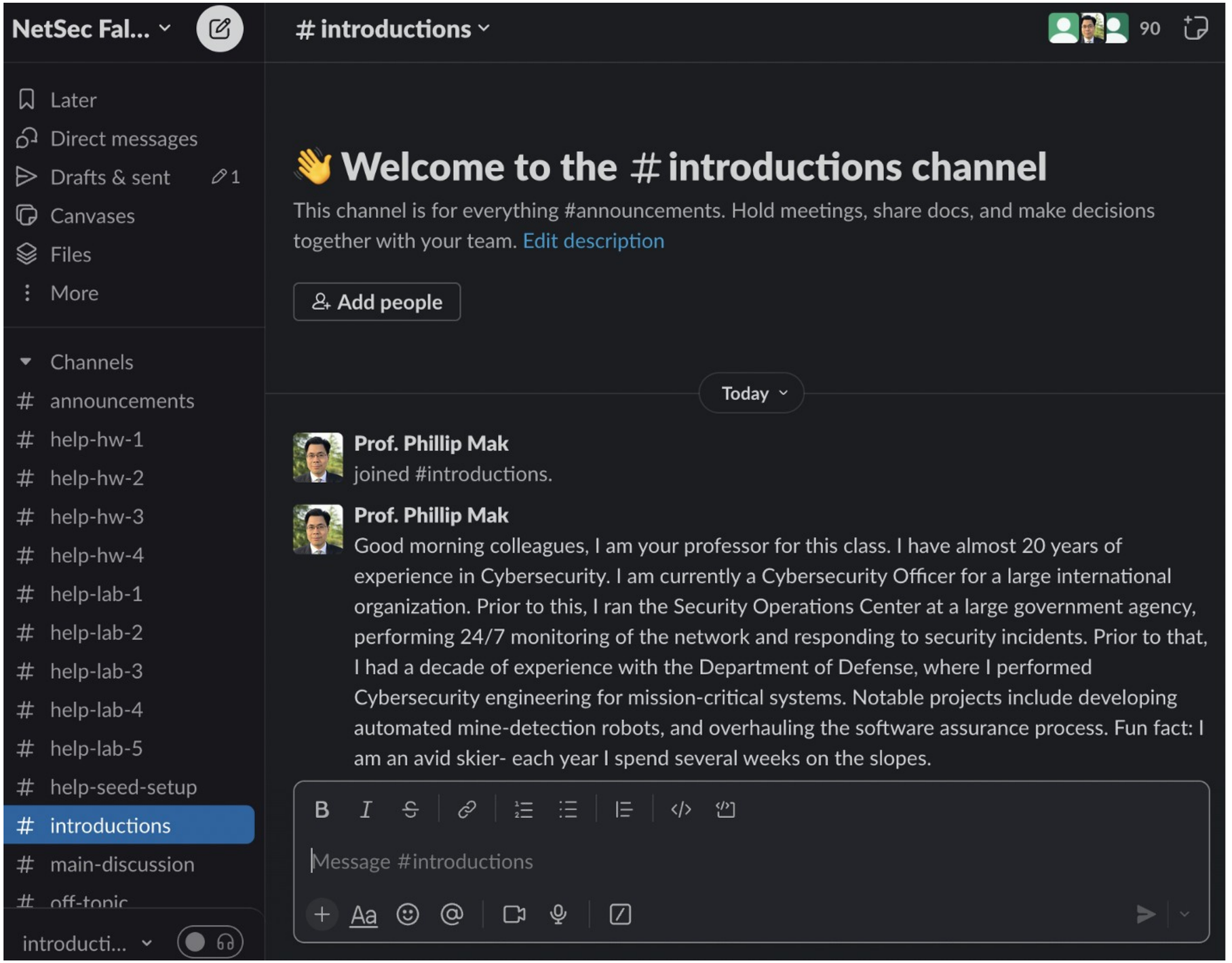
- Join Slack
  - -Provide a quick intro to include
    - -Info about yourself, e.g., major, expected graduation
    - -Any prior Cyber experience or Cyber classes
    - -Any particular topic you're interested in
    - -An interesting fact about yourself
    - -Using Slack is a required part of the class – announcements, details, and discussions are a part of the class

- Subscribe to the calendar feed on your mobile device
  - -Brightspace -> Calendar -> Subscribe

- Set up SEED Labs

Slack

- You will receive an invite to the Slack workspace
- Please introduce yourself in the #introductions channel
- Usage of Slack is required for this class



Things That I Won't Do at the End of the Course

- Give you extra work so that you can try and improve your grade

- Bump your grade up because you feel that you deserve it, need it for a scholarship, etc.

- Review earlier assignments in an effort to try and "find' points.

- Unless there is a true grading error, do not come asking for extra points.

NYU TANDON SCHOOL OF ENGINEERING

Syllabus

***Class Schedule**
Live Class 4-6 PM ET

Week	Date	Lesson	Readings (from *Internet Security: A Hands-on Approach*. 3rd Edition)
1	Mon, 27 Jan	**Lesson 0: Introduction, Expectations, and Policies** **Lesson 1: Security Basics** •What is Network Security, Thinking Differently and the Larger System in Play •Risk Management •Qualitative Risk Assessment	Ch 1: Network Security Basics, 1.2-1.6 Ch 6: Attacks on the TCP Protocol
2	Mon, 3 Feb	**Lesson 2: Network Recon – Part I** •The Cyber Kill Chain •Performing OSINT •Network Scanning and Enumeration: whois, DNS, traceroute, host discovery •DNS Reconnaissance •Port and Service Discovery	
3	Mon, 10 Feb	Lesson 2: Network Recon – Part II	
	Mon, 17 Feb	**NO CLASS -- Presidents' Day**	
4	**Tue, 18 Feb**	**Lesson 3: Vulnerabilities and Exploits – Part I** •Vulnerability Identification •Spoofing •Session Hijacking •DOS/DDOS Attacks •DNS Attacks •Metasploit	Ch 3. The Internet Protocol (IP) and Attacks
5	Mon, 24 Feb	**Lesson 3: Vulnerabilities and Exploits – Part II**	Ch 10. DNS and DNS Attacks, 10.1, 10.2, 10.5-10.11
6	Mon, 3 Mar	**Lesson 4: Post-Exploitation** •Persistence •Data Exfiltration •Removing Evidence	Ch 14. Reverse Shell
		This lesson will be asynchronous only **Lesson 5: Cryptography** •Cryptography Basics: Caesar's Cipher, Substitution Cipher, Vigenère •Symmetric Key Cryptography •Block Ciphers Mode of Operations •Public Key Cryptography: RSA, DH	Ch 15. Secret-Key Encryption, 15.1-15.5
7	Mon, 10 Mar	Midterm Review	
	Sat, 15 Mar	Midterm on Lesson 1-5 Only Starting time: 10 AM - 12 NOON ET	

NYU TANDON SCHOOL OF ENGINEERING

Syllabus

***Class Schedule**
Live Class 4-6 PM ET

Week	Date	Lesson	Readings (from *Internet Security: A Hands-on Approach*. 3rd Edition)
8	Mon, 17 Mar	**Lesson 6: Message Integrity, Public Key Infrastructure, and TLS – Part I** •Message Integrity •Protection Diffie-Hellman Exchanges •Message Integrity: hashing, nonce •Securely Sending Messages	Ch 4. Packet Sniffing and Spoofing, 4.3.5, 4.4, 4.5 Ch 16. One-Way Hash Function, 16.1-16.5
	Mon 24 Mar	**NO CLASS -- Spring Break**	
9	Mon, 31 Mar	**Lesson 6: Message Integrity, Public Key Infrastructure, and TLS – Part II** •Public Key Infrastructure •Digital Signatures •Certificate Authorities, X509v3 Certificates •Certificate Issuance and Validation	Ch 18. Public Key Infrastructure
10	Mon, 7 Apr	**Lesson 6: Message Integrity, Public Key Infrastructure, and TLS – Part III** •Transport Layer Security •TLS Ciphersuites •Types of TLS Certiticates: DV, OV, and EV •TLS Full Handshake •Perfect Forward Secrecy •TLS Protocol in Detail	Ch 19. Transport Layer Security (TLS)
11	Mon, 14 Apr	No Live Class - This lesson will be asynchronous only **Lesson 7: Firewalls** •Basic filtering rules •Proxies and Gateways •Tunneling Protocols •Iptables	Ch 7. Firewall
12	Mon, 21 Apr	**Lesson 8: Layer 2 Security** •ARP Attacks •VLAN Attacks •DHCP Attacks •Spoofing •Spanning Tree Protocol	Ch 2. The MAC Layer and Attacks
13	Mon, 28 Apr	**Lesson 9: Wireless Security** •IEEE 802.11 Overview •Wireless Authentication and Association •802.1x •Wi-Fi Security Protocols: WEP/WPA/WPA2/WPA3	
14	Mon, 5 May	Final Review	
	Sat, 10 May	Final on Lesson 6 Onward Only Starting time: 10 AM - 12 NOON ET	

NYU Tandon Cybersecurity Industry Partner Badges

CHECK POINT™ · Security Scorecard · CYBR · snyk · IMMERSIVELABS · splunk> · Qualys. · ThreatModeler

NYU Tandon Cybersecurity Industry Partner Badges