**General Course Information**

**Instructor:** Mohammed Rahman

**Instructor's email:**  [mar23@nyu.edu](mailto:mar23@nyu.edu)

**Course Number:**  HIGH1-CE9074

**Dates:  March 5th, 19th, 26th and April 2nd** (4 classes, No class on March 12th)

**Day:**  Saturdays

**Time:** 1:30PM - 5:00PM

**Location:** Remote

**Instructor Bio**

Mohammed Rahman has been teaching various courses at NYU for more than 21 years. He has earned an MS in Computer Science from NYU and an MBA from Stony Brook University. Mr. Rahman is currently doing another MS in Computer and Network Security at SUNY Polytechnic Institute.

He has published three books: Get a grip on *JavaScript, Lean on Python, and Crystal Clear Java*

In addition to teaching at NYU's School of Professional Studies and writing new books, Mr. Rahman also manages the security and reliability of a robust eCommerce website – [www.MSCDirect.com](http://www.mscdirect.com).

**Course Description**

Cyber defense is a very complex and highly technical field of information systems. The scope of cyber defense spans across multiple computers and internet connected devices including mobile devices, various operating systems, countless application software, various network devices that operate in private settings as well as business environments including government agencies.

The need for more cybersecurity professionals and computer forensic experts is growing rapidly. This course offers the unique opportunity to develop your technical know-how and software expertise to enter the field of cybersecurity. You will quickly learn the science and the art of defending against cyberattacks, techniques to investigate computer crimes, and how to capture the bad guys. You will also learn how to detect vulnerabilities in systems by attacking them as a good guy. You will also learn computer forensics and cyber security through real-world examples and tools.

This course will encourage you to explore career opportunities in this fast-growing field.

**Prerequisites**

Basic computer knowledge will be enough.

**Course Structure/Method**

This course will take place in a classroom setting with the instructor present in person. The instructor will run videos, demos and illustrate cyber security concepts. Sometimes students will be asked to act as ethical hackers and demo attacks as proof of concepts. In addition, the instructor will hold interactive sessions to clarify all cybersecurity concepts. Students will have opportunities to ask questions and answer questions to clear up any confusion. There will be three take-home assignments for students to work on throughout the week.

**Course Learning Outcome**

At the completion of this course, the students will be able to:

* Detect and mitigate vulnerabilities in systems they use today.
* Apply cybersecurity techniques to protect computer systems and devices against future cyberattacks.
* Recover from attacks if their systems are ever compromised.

**Communications**

If you have any questions or concerns, please email me at: [**mar23@nyu.edu**](mailto:mar23@nyu.edu)**.** Emails will be answered as soon as possible, preferably within 24 hours.

**Course Expectations**

Students are expected to engage and participate. Homework will be assigned on a weekly basis, and each assignment is expected to take no more than an hour or two to complete. Each student should do their homework individually. Work must be original and authentic. Please see the NYUSPS academic policies.

Regular homework assignments will be assigned every week starting from the 1st class and due the following week.

|  |  |  |  |
| --- | --- | --- | --- |
| HW # | Assigned on | Due on | Points |
| 1 | Session 1 | Session 2 | 20 |
| 2 | Session 2 | Session 3 | 20 |
| 3 | Session 3 | Session 4 | 20 |
| Points from Homework | | | 60 |
| Class Participation | | | 40 |
| Total | | | 100 |

Homework assignments will be handed in via email. The email address is: [mar23@nyu.edu](mailto:mar23@nyu.edu)

Please submit homework on the due date, even if they are incomplete, so that you secure partial credits. Late submissions for homework assignments are not accepted.

**Classroom Expectations:**

As continuing education students, you are expected to conduct yourselves in a professional manner and engage and collaborate with your classmates in the Zoom meeting room. Here are our guiding principles:

* Dress as if you are in the Classroom.
* Keep your microphone muted unless asking a question or engaging in discussion.
* Check your video and audio when entering your class session.
* Think background, minimize distractions around you.
* Look into the camera instead of looking at the screen.
* Type quietly, mute if necessary.
* Don't eat during a Zoom class session and refrain from engaging in any activity such as smoking, consuming alcohol, etc. that you would not engage in if the class was in person.

SPS classrooms are diverse and include students who range in age, culture, learning styles, and levels of professional experience. To maintain an inclusive environment that ensures all students can equally participate with and learn from each other, as well as receive feedback and instruction from faculty during group discussions in the classroom, all course-based discussions and group projects should occur in a language that is shared among all participants.

**Required Material**

Recommended book: Computer & Internet Security, Second Edition by Wenliang Du, ISBN: 9781733003933. The book is for students who would like to learn and understand cyber security in depth. It is not a required textbook.

Weekly class notes detailing everything discussed in the class and other materials/links will be provided.

**Assessment Strategy**

60% assignments, three assignments

40% in-class participation as stated above.

All students will receive a letter grade for this course unless they complete and submit a Non-Evaluative Grade Form, which allows them to receive an NE in lieu of a letter grade. The grading scale for the High School Academy is based on an A-C letter scale (A, A-, B+, B, B-, C+, C). Students wishing to audit the course must obtain prior written permission from: [sps.hsacademy@nyu.edu](mailto:sps.hsacademy@nyu.edu)

**NYUSPS Policies**

"NYUSPS policies regarding the Family Educational Rights and Privacy Act (FERPA), Academic Integrity and Plagiarism, Students with Disabilities Statement, and Standards of Classroom Behavior among others can be found on the NYU Classes Academic Policies tab for all course sites as well as on the University and NYUSPS websites. Every student is responsible for reading, understanding, and complying with all of these policies."

The full list of policies can be found at the web links below:

University: <http://www.nyu.edu/about/policies-guidelines-compliance.html>

NYUSPS: <http://sps.nyu.edu/academics/academic-policies-and-procedures.html>

**Course Outline**

## Session 1

**Introduction to Cyber Security**

What is Cybercrime?

What is the CIA?

Why is Cybercrime so prevalent?

Examples of hacking

Who are the hackers?

How to implement cybersecurity

Types of Attacks

What is Ethical Hacking?

Terminologies

What is Cyber Spying?

Safe Searching

**Introduction to Computer Science**

What is the difference between a MAC Address and an IP Address?

IPConfig (or ifconfig for Linux/Mac)

What is ARP Cache?

What is ARP Spoofing/Poisoning?

What is a Domain Name?

What is DNS?

What is DNS Spoofing/Poisoning?

**Introduction to Cyber Attack**

Steganography Demo

Shellshock Attack Demo

## Session 2

**Introduction to Social Engineering**

**PCI Compliance**

**Social Engineering again!**

**Introduction to Cyber Defense**

Phases of Attack

Steps of Defense

Risk Management

**Introduction to Networking**

Internet Protocol (IP)

Transmission Control Protocol (TCP)

Client-Server Model

IP Address and Port Number

Sockets

Risks with Sockets

Netstat command

Nmap Tool

Telnet command

Networking Devices and Security

**Session 3**

**Introduction to Personal Security**

Use Virtual Private Network (VPN) on public WiFi

Emails - SMTP and POP/IMAP

Secured Emails

What is the WWW?

What is HTML?

What is HTTP?

Fiddler Tool

Symmetric vs Asymmetric Cryptography

What is Digital Certification?

How does SSL/TLS work?

Introduction to Password Protection

Password Weaknesses

Password Encryption (Hashing)

Rainbow Table

Brute Force Cracking

Better security options

Salting Password

Long Password

Use Different Passwords for Different Sites

Use Password Manager

Use Two Factor Authentication for Password Manager

## Session 4

**Introduction to Web App Security**

Weak Protocol

Weak Admin Password

Weak Password Reset

Same Password on Multiple Applications

Weak Access Control

Cross-Site Scripting (XSS)

Cross-Site Request Forgery (CSRF)

SQL Injection

App Security Issue Detection Mechanism

**Introduction to Server Security**

Pen Testing with Metasploit and Metasploitable

Final Words on Cyber Defense