Course Code: An Introduction to Cybersecurity for Alumni

Ed Amoroso

Spring, 2020

E-mail: memon@nyu.edu
Office Hours: M 10-11:45am
Office: Zoom

Web: **https://engineering.nyu.edu**
Class Hours: Async
Class Room: NYU Classes

Course Description

This course offers a broad introduction to important topics in Cybersecurity. This course was designed to help alumni with a technical (though not necessarily computer science) background learn about modern information systems and how they can be exploited and protected in practice. This includes the topics of threat modeling, basic cryptography, authentication, access control models, enterprise security, and system attacks.

This course is conducted entirely on-line. Each week you will be provided with video lectures, readings, and an exercise. This course has no evaluation, so you can follow it at your own pace and complete the readings and exercises at your own pace.

Required Materials

All required materials are provided. These include lecture videos, readings, and exercises.

Prerequisites/Corequisites

There are no prerequisites for this course. However, this course does assume some technical background and general knowledge about computers.

Course Objectives

By the end of this course, successful students will be able to:

1. Approach problems with a security mindset.
2. Reason about security threats to a system.
3. Reason about security threats to enterprise networks.
4. Reason about solutions to security problems.

5. Apply security fundamentals to solve security problems.
6. Reason about good authentication practices.

Course Structure

Class Structure

This course is performed entirely online. Video lectures and readings will be assigned each week to cover a specified topic. For each week, the video lectures and readings should take no longer than 2 hours.

Assessments

This class contains no graded assessments. However, each week we provide an exercise for you to complete. These exercises take the theoretical information provided and synthesizes it into practical, hands-on application. Therefore, to truly understand the material it is vital to complete each assignment in the course.

Lecture

Video lectures in this course were recorded by Dr. Ed Amoroso. Each video lecture lasts between 5 and 15 Minutes. Each week has multiple video lectures, arriving at about an hour of video lectures per week.

Grading Policy

This class contains no assessment or traditional grading.

Accommodations for Disabilities

Schedule and weekly learning goals

The learning goals below should be viewed as the key concepts you should grasp after each week, and also as a guide to what you should be considering when completing each week's exercise.

Week 01: Adversaries, Types of Attacks, and Threat Modeling

- Video: Adversary Types (Coursera) - 7 Minutes
- Video: Vulnerability Types (Coursera) - 5 Minutes
- Video: Threat Types (Coursera) - 5 Minutes
- Video: IP Packet Attacks - 15 Minutes
- Video: Soda Machine - 15 Minutes
- Video: Threat Trees and Completeness of Analysis - 6 Minutes
- Reading: Who is the Opponent? Security Engineering Chapter 2.

- Reading: Threat Modeling: 12 Available Methods
- Reading: OWASP Threat Modeling Cheat Sheet.
- Exercise: Threat tree for campaign (Web frontend, database, donation processing, email server, etc.)

Week 02: Risk

- Video: Assets and Infrastructure (Coursera) - 8 Minutes
- Video: Calculating Risk (Coursera) - 8 Minutes
- Video: Making Security and Cost decisions Based on Risk (Coursera) - 5 Minutes
- Video: Mapping Assets to Threats (Coursera) - 7 Minutes
- Video: Estimating Risk for Threat-Asset Pairs (Coursera) - 5 Minutes
- Video: Example Case Study Matrix (Part 1) (Coursera) - 8 Minutes
- Video: Example Case Study Matrix (Part 2) (Coursera) - 9 Minutes
- Video: Example Cast Study Matrix (Part 3) (Coursera) - 7 Minutes
- Video: Mapping Assets, Threats, Vulnerabilities, and Attacks (Coursera) - 5 Minutes
- Reading: 7 considerations for cyber risk management.
- Exercise: Risk estimation and Matrix

Week 03: Cryptography Basics

- Video: Basic Cryptography - 12 Minutes
- Video: Public Key Cryptography - 10 Minutes
- Video: Cryptanalysis - 10 Minutes
- Video: Key Distribution and Certification Authority - 13 Minutes
- Video: Chaum's Blinding Algorithm - 10 Minutes
- Reading: OWASP Cryptographic Storage Cheat Sheet.
- Reading: OWASP Password Storage Cheat Sheet.
- Exercise: Confidentiality and Integrity against cloud providers

Week 04: Authentication

- Video: General Authentication Schema - 18 Minutes

- Video: Handheld Authentication - 7 Minutes
- Video: RSA Secure ID - 8 Minutes
- Video: Kerberos Part 1 - 15 Minutes
- Video: Kerberos Part 2 - 10 Minutes
- Reading: Biometrics and continuous authentication
- Reading: Biometric Issues
- Exercise: Designing Authentication

Week 05: Enterprise Network Security Considerations

- Video: Enterprise Premier Weaknesses - 9 Minutes
- Video: Cyber Offensive and Defensive Schema - 11 Minutes
- Video: Basic Scanning - 8 Minutes
- Video: PacketFilter and Firewall Configuration - 12 Minutes
- Video: Intrusion Detection Basics - 9 Minutes
- Video: Botnets and DDOS - 8 Minutes
- Reading: Phishing and Don't take the bait
- Reading: Lateral movement
- Exercise: Detecting Phishing

Week 06: System Attacks and Blockchain

- Video: Classic Unix Kernel Attack - 17 Minutes
- Video: Trojan Horse Code Insertion - 10 Minutes
- Video: SQL/ Slammer Worm of 2003 (Coursera) - 5 Minutes
- Video: Nachi Worm of 2003 (Coursera) - 10 Minutes
- Reading: What is Bitcoin? What is Blockchain?
- Reading: Bitcoin and trust and blockchain's problems.
- Reading: Buffer Overflows