IT230: Computer Systems Security

Description

IT 230 introduces the applied topic of Computer Security. Students will learn ways of preventing, identifying, understanding, and recovering from attacks against computer systems. It also presents the evolution of computer security, the main threats, attacks and mechanisms, applied computer operation and security protocols, main data transmission and storage protection methods, cryptography, network systems availability, recovery and business continuity procedures.

Upon completion of this course, students will:

- Have a sound understanding of computer system vulnerabilities and threats, and ways to mitigate them to protect computers against attacks
- Design, develop and implement a computer information security strategy
- Understand the job market for computer security and be prepared for an potential interview
- Have a good foundation for taking the CompTIA Security+ exam

Prerequisites

- IT120: Introduction to Network Technology.

Instructor Information

Instructor: Karl Giannoglou

Office Location & Hours:

GITC3902B Tuesday:1:30pm-2:30pm

Wednesday & Friday: 11:30am-1pm

Email: karl.giannoglou@njit.edu

Responses to emails: Within 48 hours

Class Meetings

- The class will meet during the assigned time slots
- This class utilizes the Canvas learning management system. You can find Assignments, Tests, and Forums there: https://canvas.njit.edu

Resources

- In the course, we will be reviewing information that can be found under the PluralSight CompTIA Sec+ SYO-601 module
- This module is completely optional, but I highly recommend it.

Grading

I will deliver feedback on each forum post, homework, lab, midterm, and final within two weeks time. All assignments and assessments will be graded via SpeedGrader, comments, etc. within two weeks time.

Students are expected to complete all their assignments in their own words. TurnItIn is used for all my assignments.

Homework	25%
Labs	25%
Midterm	25%
Final	25%

Exams

The midterm will take place during a regular class period. The final exam will be during finals week. The final is not cumulative and covers the material from the midterm until the end of the course, but some of the information from the first half of the semester will still be required.

Paper notes will be allowed during the exams and they will require a LockDown Browser with a camera enabled.

Course Schedule

Each week, students will watch one lecture of class, and they will be expected to complete labs and homework assignments between each class session. All assignments are due at the end of the weekend.

Please note some of the order of material may change.

Week	Material
1	Class Orientation Intro to Cybersecurity • What is cybersecurity? • Think like a hacker • Threat actors • Jobs in cybersecurity
2	Cryptography • Hashing algorithms • Symmetric/Asymmetric Encryption • Certificates • Block Chain

3 Malware

- Types of malware
- Delivery of malware
- Cyber killchain
- Security Assessment Techniques

4 Secure Network Protocols/Ports

- Common ports
- Secure protocols

5 Attack Methods

- Poison attacks
- Injection attacks
- Interceptions
- Overflows
- Forgeries

6 Midterm Review

7 Midterm Exam

8 Security Solutions

- EDR
- SIEM
- Firewalls
- VPNs
- Email

9 Access Control

- Physical security
- Authentication
- IAM

10 Vulnerability/Risk Management

- Vulnerability management tools
- Risk assessment/tolerance in a company
- Patch management

Governance and Compliance

- Laws and regulations
- Company policies

11 Disaster Recovery and Redundancy

- Redundancy planning
- RAID configurations
- Disaster recovery and proactive planning

Incident Response

- MITRE ATT&CK
- Containment methods
- Incident Indicators

12 Securing Devices

- Hardening OSes
- IoT
- Mobile devices
- Securing computer hardware and peripherals
- Asset management
- Blacklisting/Whitelisting

13 Cloud and Virtualization

- Public Cloud Providers
- Benefits of using cloud

- IaaS, PaaS, SaaS
- VMs
- Containerization

14 Final Review

15 Final Exam

Policies

Academic Integrity

Academic Integrity is the cornerstone of higher education and is central to the ideals of this course and the university. Cheating is strictly prohibited and devalues the degree that you are working on. As a member of the NJIT community, it is your responsibility to protect your educational investment by knowing and following the academic code of integrity policy

(Links to an external site.)

.

Please note that it is my professional obligation and responsibility to report any academic misconduct to the Dean of Students Office. Any student found in violation of the code by cheating, plagiarizing or using any online software inappropriately will result in disciplinary action. This may include a failing grade of F, and/or suspension or dismissal from the university. If you have any questions about the code of Academic Integrity, please contact the Dean of Students Office at dos@njit.edu

Requesting Accommodations

If you are in need of accommodations due to a disability please contact the Office of Accessibility Resources & Services (OARS)

(Links to an external site.)

, Fenster Hall Room 260 to discuss your specific needs. A Letter of Accommodation Eligibility from the OARS authorizing your accommodations will be required.

Resources for NJIT Students

NJIT Service for Students

 (Links to an external site.)

, including Technical Support

Class Etiquette

Students are expected to respect their classmates, stay quiet in class, and keep phone usage to a minimum.

Late Work/Makeups

Homework/Labs will be due before the start of class.

Late work will be accepted at half credit until the next exam.

- First half of the semester's homework/labs/forums will not be accepted after the Midterm.
- Second half of the semester's homework/labs/forums will not be accepted after the Final.