PASSWORD Technical College

IT School
San Germán, PR

Syllabus

COURSE GENERAL INFORMATION

Course Title: Introduction to Ethical Hacking
Code: PWHI 1010
Contact Hours: 42.5
Term: Feb 24, 2021 to March 25, 2021
Teacher: Prof. Joel Vargas
Email: jvargas@passwordpr.com

Course Description

The Introduction to Ethical Hacking course develops foundational understanding of cybersecurity and how it relates to information and network security. The course introduces students to characteristics of cybercrime, security principles, technologies, and procedure to defend networks. Through interactive, multimedia content, lab activities, and multi -industry case studies, students build technical and professional skills to pursue careers in cybersecurity.

Objetives:

- Learn procedures to implement data confidentiality, integrity, availability and security controls on networks, servers and applications.
- Understand security principles and how to develop security policies that comply with cybersecurity laws.
- Apply skills through practice, using labs and Cisco Packet Tracer activities.
- Get immediate feedback on your work through built-in quizzes and tests.
- Connect with the global Cisco Networking Academy community.

Skill Distributions:

Chapter 1. Threat, Vulnerability and Attack

- The Cybersecurity World
- Cyber Criminals versus CyberHeroes
- Threats to the Kingdom
- The Dark Forces of Cybersecurity

Chapter 2. Hacking Web Technologies

- The Cybersecurity Sorcery Cube
- CIA Triad
- States of Data
- Cybersecurity Countermeasures
- IT Security Management
- Framework

Chapter 3. Hacking Wireless Network

- Malware and Malicious Code
- Trickery
- Attacks

Chapter 4. Maintaining Access and Covering Tracks

- Cryptography
- Access Controls
- Obscuring Data

Chapter 5- Cybercrime the Big Business

- Types of Data Integrity Controls
- Digital Signatures
- Certificates
- Database Integrity Enforcement

Describe the characteristics of criminals and heroes in the cybersecurity realm.

- Describe the common characteristics comprising the cybersecurity world
- Differentiate the characteristics of cyber criminals and professionals
- Compare how cybersecurity threats affect individuals, businesses, and organizations.
- Describe the factors that lead to the spread and growth of cybercrime.
- Describe the organizations and efforts committed to expanding the cybersecurity workforce.

Describe how the principles of confidentiality, integrity, and availability as they relate to data states and cybersecurity countermeasures.

- Describe the three dimensions of the McCumber Cube.
- Describe the principles of confidentiality, integrity, and availability.
- Differentiate the three states of data. Compare the types of cybersecurity countermeasures.
- Describe the ISO Cybersecurity Model

Describe the tactics, techniques and procedures used by cyber criminals.

- Differentiate the types of malware and malicious code.
- Compare the different methods used in social engineering.
- Compare different types of cyberattacks.

Describe how technologies, products and procedures are used to protect confidentiality.

- Explain how encryption techniques protect confidentiality.
- Describe how access control techniques protect confidentiality.
- Describe the concept of obscuring data.

Describe how technologies, products and procedures are used to ensure integrity.

- Explain processes used to ensure integrity.
- Explain the purpose digital signatures. Explain the purpose digital certificates. Explain the need for database integrity enforcement.

Laboratories and Assessments

- Lab 1- Incident Handling
- Lab 2- Exploring Processes, Threads, Handles, and Windows Registry
- Assessment 1- Cybersecurity Job Hunt
- Assessment 2- Threat Identification
- Special Project- Attack Incident

Lab Policy

1. For the student's and equipment's safety **no eating and/or drinking** is allowed in the classroom or laboratory.

2. Students must always apply preventing ESD (Electrostatic Discharge) procedures before using electronic devices.

3. The use of Smartphone or any other personal device is prohibited during lab sessions unless approved by the professor.

Evaluation Criteria

CRITERIA	Grade total
Mid-Term Exam	100
Final Exam	100
Quizzes	100
Laboratories and Assessments	100
Special Project	100
Total	500

*5 Points less for each non-excused absence.

*Assignments are always due in class on the day designated. You are responsible for any work lost due to technical problems, etc. Late papers will lose a letter grade for each day that they are late. Any exceptions must be properly documented and discussed in advance for an extension to be arranged.

Educational Resources

- Neo LMS (2020). Ethical Hacking I. *passwordtech.edu20*.
  https://passwordtech.edu20.org/home_news
- Mile 2 (2020). Cybersecurity Security Information. *Mile2*. http://mile2.com/
- Cybersecurity Essentials Course

Notes

• ***Reasonable Accommodation*****:** Any student who requires a reasonable accommodation should do the request at the beginning of the course or as soon as he / she acquires knowledge of what it requires, through the Professor in charge and this notifying the Academic Director.

• ***Honesty, fraud, plagiarism:*** The lack of honesty, fraud, plagiarism and / or any other inappropriate behavior in relation to the student's academic performance constitute violations of the Institution's Catalog, its Rules of Conduct and Student Duties. Major infractions, as determined by the Catalog, may result in the suspension of the Institution for a definite time or permanent expulsion as stipulated in the Norms of Conduct and Duties of the Students