

Syllabus

COURSE GENERAL INFORMATION

Course Title: Introduction to Ethical Hacking Code: PWHI 1010 Contact Hours: 43 Term: June 21, 2022 to July 1, 2022 Teacher: Joel Vargas Ramos 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. The Need for Cybersecurity

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

Chapter 2. Attacks, Concepts and Technique

- The Cybersecurity Sorcery Cube
- CIA Triad
- States of Data
- Cybersecurity Countermeasures



- IT Security Management
- Framework

Chapter 3. Protecting Data and Privacy

- Malware and Malicious Code
- Trickery
- Attacks

Chapter 4. Protecting the Organization

- Cryptography
- Access Controls
- Obscuring Data

Chapter 5- Will Your Future Be in Cybersecurity

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

Days	Modules	Works
Class #1 Module 1	 The Need for Cybersecurity The Cybersecurity World Cyber Criminals Versus Cyberheroes 	 Pre-Test Comprehension Test Lab 1- Incident Handling
Class #2 Module 1	 Threats to the Kingdom The Dark Forces of Cybersecurity 	 Lab 2- Exploring Processes, Threads, Handles, and Windows Registry Quiz 1
Class #3	Attacks, Concepts and	• Assessment 1-
Module 2	 Technique: The Cybersecurity Sorcery Cube CIA Triad States of Data 	Hunt



Class #5	Protecting Data and Privacy	• Quiz 2
Module 3	Malwares and Malicious Code	
Class #6 Module 3	TrickeryAttacks	Special Project- Attack Incident
Class #7 Module 4	 Protecting the Organization: Cryptography Access Control Obscuring Data 	• Quiz 3
Class #8 Module 5	 Will Your Future Be in Cybersecurity: Types of Data integrity controls Digital Signatures Certificates Database Integrity Enforcement 	 Post-Test Comprehension Final Exam

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 (2021). Introduction to Ethical Hacking. *passwordtech.edu20*.

https://passwordtech.edu20.org/

- Mile 2 (2020). Cybersecurity Security Information. *Mile2*. <u>http://mile2.com/</u>
- Cisco Network Academy (2022). Introduction to Ethical Hacking. *Netacad*.

https://netacad.com.

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