PCAC2007 IT FUNDAMENTALS FOR CYBERSECURITY – I (3-0-0)

OVERALL COURSE OBJECTIVES: The objective of this course is to equip learners with a comprehensive understanding of Cybersecurity, from foundational knowledge and terminology to practical skills in system operations, role-based security processes, and advanced topics like encryption and compliance standards. This holistic view aims to prepare participants for junior-level analyst roles in the Cybersecurity field, ensuring they are well-versed in both theoretical and practical aspects of cyber defense.

Module 1 : Introduction to Cybersecurity Tools & Cyber Attacks [18 Hours]

This course gives you the background needed to understand basic Cybersecurity. You will learn the history of Cybersecurity, types and motives of cyber attacks to further your knowledge of current threats to organizations and individuals. Key terminology, basic system concepts and tools will be examined as an introduction to the Cybersecurity field. You will learn about critical thinking and its importance to anyone looking to pursue a career in Cybersecurity.

Sub-Topics
A brief overview of types of actors and their motives
An overview of key security concepts
An overview of key security tools
History of Cybersecurity

Formative Assessments:
4 Graded Quizzes

Module 2 :Cybersecurity Roles, Processes & Operating System Security [15 Hours]

This course gives you the background needed to understand basic cybersecurity around people. process and technology. You will understand the key cybersecurity roles within an organization; list key cybersecurity processes and an example of each process; describe the architecture, file systems, and basic commands for multiple operating systems including Windows, Mac/OS, Linux, and Mobile; and also understand the concept of virtualization as it relates to cybersecurity.

Sub-Topics
Authentication and Access Control
Examples & Principles of the CIA Triad
Linux Operating System Security Basics
macOS Security Basics
Overview of Virtualization
People Process & Technology
Windows Operating System Security Basics

Formative Assessments:
6 Graded Quizzes

Module 3 :Cybersecurity Compliance Framework & System Administration [21 Hours]

This course gives you the background needed to understand the key cybersecurity compliance and industry standards. This knowledge will be important for you to learn no matter what cybersecurity role you would like to acquire or have within an organization.

You will learn the basic commands for user and server administration as it relates to security. You will need this skill to be able to understand vulnerabilities within your organizations operating systems.

Sub-Topics
Client System Administration, Endpoint Protection and Patching
Compliance Frameworks and Industry Standards
Cryptography and Compliance Pitfalls
Linux and Encryption: Final Project
Server and User Administration

Formative Assessments:
4 Graded Quizzes

LEARNING OUTCOMES: On successful completion of the course the students shall be able to:

1. Understand basic Cybersecurity concepts, gaining foundational knowledge of the Cybersecurity landscape including types, motives of cyber attacks, and the history behind them.
2. Grasp key Cybersecurity terminology and tools, learning essential terms and introductory tools relevant to Cybersecurity, facilitating a deeper understanding of system concepts.
3. Recognize the key roles and typical processes within a Cybersecurity organization, enhancing comprehension of operational security.
4. Develop skills to navigate and manage Windows, MacOS, Linux, and mobile operating systems from a security perspective.
5. Understand and apply cybersecurity compliance standards and protocols to maintain the integrity and security of information systems.
6. Learn fundamental concepts and practices of cryptography and encryption, crucial for protecting information against cyber threats.