Course Code: 8H111GW

Course Title: Cybersecurity Roles, Processes & Operating System Security

Description:

This course provides information about cybersecurity people, processes, and technology. You will learn the key cybersecurity roles and processes within an organization. Then move to the architecture, file systems, and basic commands for various operating systems. Finally, you will learn how virtualization relates to cybersecurity.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the second course in a series to acquire the skills to work in the field as a Cybersecurity Analyst**.**

Objectives:

In this course, you will learn to:

- Define IT security
- Explain the purpose of frameworks, baselines, and best practices in cybersecurity
- Discuss typical roles in an information security department
- Define security operation center (SOC)
- Define process in the context of business management and describe its attributes
- Describe standard process roles
- Explain what makes a process successful
- Discuss typical process performance metrics
- Summarize continual process improvement
- Define information technology infrastructure library (ITIL)
- Describe each ase of the ITIL lifecycle
- Describe key terms and characters from the Alice and Bob cryptogray scenario
- Define confidentiality, integrity, and availability in the context of cybersecurity and discuss their important components
- Define authenticity and accountability in the context of cybersecurity
- Explain identification and AAA in the context of cybersecurity
- Identify the three types of authentication methods
- Discuss the types of access control and their subcategories
- Describe common access control methods
- Discuss access control best practices
- Identify examples of ysical and logical access control methods
- Discuss types of monitoring and access control processes
- Summarize how to use the Open Web Application Security Project (OWASP) to discover the top ten web application vulnerabilities for a given year and how to address them
- Compare and contrast Windows’s two modes: user and kernel
- Define file system and hierarchical structure
- Contrast the NTFS and FAT file systems that Windows uses
- Describe the Windows directory structure
- Summarize how Windows handles the separation of 32-bit and 64-bit applications
- Describe various useful keyboard shortcuts applicable to Windows
- Discuss important characteristics of Linux
- Explain the relationship between Linux’s kernel and shell
- Describe Linux’s file system and directory structure
- Explain what happens at each Linux run level
- Recall basic Linux shell commands and the functions that they perform

- Describe Linux’s file and directory permission structure
- Explain how to use the Linux shell to change a file’s permissions and owner
- Install and run a Kali Linux virtual machine using VirtualBox
- Perform administrative tasks to strengthen security on Kali Linux
- Explain how to view system information, current activity, and log files in macOS
- Summarize the various security settings within macOS
- Discuss macOS’s recovery partition and the services that it offers
- Contrast virtualized and traditional environments
- Describe the roles of hosts, hypervisors, and virtual machines in a virtualized environment
- Summarize how organizations move from virtualized to cloud environments
- List the steps required to deploy services to the cloud
- Define cloud computing
- Discuss the advantages and disadvantages of cloud computing
- Contrast the three cloud deployment models: public, private, and hybrid
- Summarize essential functions listed in the cloud computing reference model
- Contrast the three cloud service models: software as a service, platforms as a service, and infrastructure as a service
- Describe important components of cloud security
- Summarize the alignment between governance, service, and organization needed to achieve an effective cloud security strategy

Duration:

8.8 Hrs

Topics:

Unit 1 - People Process & Technology

Unit 2 - Examples & Principles of the CIA Triad

Unit 3 - Authentication and Access Control

Unit 4 - Windows Operating System Security Basics

Audience:

This course is intended for anyone who wants to gain a basic understanding of Cybersecurity or as the second course in a series of courses to acquire the skills to work in the Cybersecurity field as a Jr Cybersecurity Analyst.