Course Code: 8H101GW

Course Title: Introduction to Cybersecurity Tools & Cyber Attacks

Description:

This course provides an introduction to cybersecurity tools and attacks. You will learn the history of cybersecurity, the types and motives of cyber attacks, and current threats to organizations and individuals. Key terminology and basic system concepts and tools will be examined to introduce you to the cybersecurity field. You will learn about critical thinking and its importance to anyone looking to pursue a career in cybersecurity. Finally, you will begin to learn about organizations and resources to further research cybersecurity issues in the Modern era.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the first course in a series to acquire the skills to work in the field as a Cybersecurity Analyst**.**

Objectives:

By completing this course you should be able to:

- Describe the five key skills of critical thinking
- Discuss each component of the critical thinking model
- Summarize how rapidly changing technology and tools make critical thinking necessary for cybersecurity
- Explain what makes critical thinking an essential skill for anyone working in cybersecurity
- Summarize the numerous challenges that make comprehensive cybersecurity complex to implement
- Describe key terms and characters from the well-known Alice and Bob cryptogray scenario
- List and describe essential elements of an organization’s cybersecurity program
- Explain why comprehensive cybersecurity architecture is difficult to implement
- Summarize what recent statistics demonstrate about the current state of cybersecurity
- Discuss critical events that have shaped the United States’ attention and posture toward cybersecurity
- Summarize the event that led to the creation of the first national policy on cybersecurity
- Discuss typical roles in an information security department
- Describe vulnerability assessment and common ways that vulnerabilities end up in systems
- Contrast human and natural security threats and discuss examples of each threat
- Define vulnerability, threat, exploit, and risk
- Describe the three components of the CIA Triad
- Define cybersecurity
- Describe security operations centers (SOCs) and IBM Security Command Centers
- Discuss various resources that can help your organization protect against cybercrime
- Describe important elements of recent cyberwarfare operations
- Compare and contrast ishing and vishing campaigns
- Explain social engineering and how cybercriminals use it
- Explain what the Intrusion Kill Chain is and how each of its ases contributes to a cyberattack’s success
- Describe rogue software processes and how to protect against them
- Define host insertion and summarize how to counter it
- Describe denial of service attacks and how to reduce their impact
- Summarize IP spoofing and how to defend against it
- Describe packet sniffing and countermeasures for it
- Explain network mapping and how to protect against it
- Summarize technical and administrative controls for protecting against malware
- Describe botnets, keyloggers, logic bombs, and advanced persistent threats (APTs)

- Define malware, virus, worm, trojan horse, spyware, adware, remote access tool (RAT), rootkit, and ransomware
- Summarize the attack models for interruption, interception, modification, fabrication, and diversion
- Describe types of passive and active attacks
- Define attack in terms of cybersecurity
- Differentiate between accidental and intentional threats
- Explain what constitutes a cybersecurity threat
- Summarize network security's architectural, motivational, and protective elements
- Describe a general model for network security
- Define security mechanism and describe the various types
- Contrast active and passive attacks
- Recall recent examples of significant cyberattacks and their impacts
- List major cybercrime and hacker organizations and identify upcoming challenges for cybersecurity
- Describe the primary actors in cybercrime and their motives
- Discuss what the Open Web Application Security Project (OWASP) Top 10 is and why it's an invaluable resource for cybersecurity professionals
- Explain ethical hacking and the penetration testing process
- Contrast internal and external security audits and three ases for completing them
- Discuss cybersecurity compliance policies that most organizations must follow
- Describe the components of IT governance
- Explain the purpose of frameworks, baselines, and best practices in cybersecurity
- Summarize what happens in each of the three ases of cybersecurity incident response
- Describe key concepts of cybersecurity incident response
- Define cybersecurity incident management and discuss its essential components
- Describe access management methods and concepts
- Define non-repudiation and its measures for implementation
- Explain availability in the context of the CIA triad and how organizations can implement it
- Describe the integrity component of the CIA triad and discuss how organizations can achieve it
- Explain confidentiality in the context of the CIA triad and how organizations implement it
- Define digital forensics and describe some of its essential concepts and tools
- Summarize the process for performing a vulnerability assessment
- Describe each ase of penetration testing outlined in the Penetration Testing Execution Standard (PTES)
- List common methodologies for penetration testing
- Describe different types of threat actors
- Differentiate attackers, offensive security researchers, and gray hat hackers
- Define penetration testing
- Describe basic principles of symmetric key cryptogray like the data encryption standard (DES) and the advanced encryption standard (AES)
- Discuss common forms of cryptograic attack
- Compare and contrast the main encryption types used today: symmetric, asymmetric, and hash
- Differentiate stream and block ciers
- Describe cryptogray and its key concepts
- Explain how antivirus and antimalware programs work
- Contrast stateless, stateful, and proxy firewalls
- Describe XML gateways and their purpose
- Summarize the limitations of firewalls
- Contrast application gateways with packet filters
- Describe packet filtering and how packet filters work
- Explain the purpose of using a firewall
- Define security service and describe the various types

Duration:

15.2 Hrs

Topics:

Unit 1: History of Cybersecurity

Unit 2: A brief overview of actors and their motives

Unit 3: An overview of key security concepts

Unit 4: An overview of key security tools

Audience:

Anyone who wants to gain a basic understanding of Cybersecurity or as the first course in a series of courses to acquire the skills to work in the Cybersecurity field as a Jr Cybersecurity Analyst.