PCAC2014 IT Fundamentals for Cybersecurity – II (3-0-0)

OVERALL COURSE OBJECTIVES: The objective of this course series is to provide a robust foundation in cybersecurity, emphasizing practical skills in network and database security, the application of generative AI tools in cybersecurity challenges, and detailed methodologies in penetration testing and incident response. This comprehensive approach is designed to prepare students for advanced roles in the cybersecurity field, ensuring they can effectively address and mitigate potential security threats.

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

1. Gain knowledge of Local Area Networks, TCP/IP, the OSI Framework, and routing basics, and comprehend how networking affects security systems within an organization.
2. Learn about common vulnerabilities in various databases including SQL, Oracle, Mongo, and Couch, and apply knowledge to mitigate risks such as SQL Injection.
3. Apply generative AI tools to combat cyber threats by detecting vulnerabilities and automating the creation of cybersecurity content like playbooks and threat intelligence reports.
4. Develop skills to perform penetration testing using various tools, gather essential data, and understand the phases of testing to improve organizational security.
5. Understand the phases of incident response, from planning and preparation to documentation and recovery, and develop skills in managing and responding to security breaches effectively.
6. Learn key forensic processes and the collection of important digital evidence, enhancing capabilities in analyzing and responding to cybersecurity incidents.

COURSE CONTENT:

Module 1: Network Security & Database Vulnerabilities [18 Hours]

This course gives you the background needed to understand basic network security. You will learn the about Local Area Networks, TCP/IP, the OSI Framework and routing basics. You will learn how networking affects security systems within an organization. You will learn the network components that guard an organization from cybersecurity attacks.

In addition to networking, you will learn about database vulnerabilities and the tools/knowledge needed to research a database vulnerability for a variety of databases including SQL Injection, Oracle, Mongo and Couch.

Sub-Topics
Basics of IP Addressing and the OSI Model
Deep Dive - Injection Vulnerability
Final Project
Introduction to Databases
TCP/IP Framework

Formative Assessments:
4 Graded Quizzes & 1 Peer Review Assignment

Module 2: Generative AI: Boost Your Cybersecurity Career [10 Hours]

This short course provides cybersecurity professionals and enthusiasts with the latest Generative AI tools to address complex cybersecurity challenges.

The course focuses on combating the exploitation of undetected vulnerabilities for which organizations increasingly turn to Artificial Intelligence (AI) and Machine Learning (ML). Generative AI, a transformative technology, emerges as a vital cybersecurity tool, detecting and preventing attacks by identifying and neutralizing unknown vulnerabilities before causing significant harm.

The course explores foundational generative AI principles and their application in real-world cybersecurity, encompassing User and Entity Behavior Analytics (UEBA), threat intelligence, report summarization, playbooks, and its impact on phishing, malware, misinformation, and deepfakes. Additionally, participants learn about potential Natural Language Processing (NLP) attack techniques, like prompt injection, and strategies to mitigate them.

Sub-Topics
Final Project and Exam
Get Started with Gen AI in Cybersecurity
SIEM and SOC Tasks Using Generative AI

Formative Assessments:
3 Staff Graded Assessments

Module 3: Penetration Testing, Incident Response and Forensics [16 Hours]

This course gives you the background needed to gain Cybersecurity skills as part of the Cybersecurity Security Analyst Professional Certificate program.

You will learn about the different phases of penetration testing, how to gather data for your penetration test and popular penetration testing tools. Furthermore, you will learn the phases of an incident response, important documentation to collect, and the components of an incident response policy and team. Finally, you will learn key steps in the forensic process and important data to collect. This course also gives you a first look at scripting and the importance to a system analyst.

Sub-Topics
Digital Forensics
Incident Response
Introduction to Scripting
Penetration Testing

Formative Assessments:
4 Graded Quizzes

ASSESSMENT:
For summative assessments, Coursera will provide question banks for which exams can be conducted on the Coursera platform or the faculty will create their own assessments.

Note: If a Course or Specialization becomes unavailable prior to the end of the Term, Coursera may replace such Course or Specialization with a reasonable alternative Course or Specialization.