Course Code: 8H131GW

Course Title: Network Security & Database Vulnerabilities

Description:

This course provides a background of network security. You will learn the about Local Area Networks, TCP/IP, the OSI Framework and routing basics, how networking affects security systems within an organization, and about 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.This course is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the fourth 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:

- Contrast stateful and stateless inspection
- Contrast intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)
- Define network address translation (NAT)
- Distinguish between static and dynamic IP address translation
- Describe how Ethernet networks work
- Distinguish between the Layer 2 and Layer 3 addressing schemes
- Differentiate between collision and broadcast domains
- Identify the ways to segment broadcast domains
- Describe various network devices
- Distinguish between an IP address and a MAC address
- Describe how broadcasting domains are used
- Describe how address resolution protocol (ARP) tables are used
- Describe the use of routing tables in network routing
- Convert numbers between binary, octal, decimal, and hexadecimal number systems
- Describe IPv4’s four-octet format and the five ranges of IPv4’s classful addressing schema
- Explain how IP addresses work
- Describe the purpose of subnet masks and gateways
- Contrast IPv4 and IPv6 addressing
- Differentiate between the TCP and UDP transport layer protocols
- Describe the domain name system (DNS), including the service that it provides
- Describe the dynamic host configuration protocol (DHCP), including the service that it provides
- Define the Syslog protocol
- Explain how to use flow utilities such as NetFlow to collect and visualize network traffic flow statistics on routing devices
- Identify the legitimate and illegitimate uses of port mirroring
- Contrast traditional firewalls with next-generation firewalls (NGFWs)
- Explain how NGFWs can inspect and block more intrusion types than is possible with traditional firewalls
- Describe the flow of packets through an NGFW
- Describe high availability in information technology
- Describe how to achieve high availability through clustering
- Identify various data source types
- Identify the many data sources present in a typical organization

- Describe structured data, semi-structured data, and unstructured data
- Differentiate between a flat-file database and a relational database
- Describe the activities typically contained in each step of the data security process
- Identify sources to consult for data security best practices
- Discuss a typical database access setup
- Describe a vulnerability assessment test report, including its contents and how to read it
- Determine the security controls required to protect data given the potential sources of threats and the hosting model used
- Discuss how each step in the data security process applies to the entire IT and data security landscape
- Describe the key components of data logging and monitoring
- Explain the value of real-time policy violation alerts and activity blocking
- Explain how to generate metrics for logging and audit reporting
- Describe the event attributes to include in logging
- Explain how to configure systems to monitor for cybersecurity events
- Describe the nature of various injection attacks and their prevalence on the threat landscape
- Describe OS command injection attacks and the operating system flaws that allow them to occur
- Identify preventative measures against OS command injection attacks
- Explain how SQL injection works
- Identify common types of SQL injection
- Identify preventive measures against SQL injection
- Describe non-SQL injection attacks such as NoSQL, XPath, and LDAP
- Identify common vulnerability attacks and defense against them
- Analyze a web application’s vulnerabilities using OWASP ZAP
- Create and modify repositories on GitHub
- Detect and analyze code vulnerabilities using Snyk
- Examine a repository’s code vulnerabilities using Snyk
- Evaluate your peers’ completion of GitHub and Snyk tasks using the provided rubric
- Fork a public GitHub repository

Duration:

10.4 Hrs

Topics:

Unit 1 -TCP/IP Framework

Unit 2 - Basics of IP Addressing and the OSI Framework

Unit 3 - Introduction to Databases

Unit 4 - Deep Dive - Injection Vulnerability

Audience:

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