Course Code: 8H141GW

Course Title: Pen Testing, Incident Response & Forensics

Description:

This course provides information about the different ases of penetration testing, how to gather data for your pentest, and popular pentest tools. You will also learn the ases 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 is intended for anyone who wants to gain a basic understanding of cybersecurity. This is the fifth 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:

- Describe industry-leading tools used for pentesting
- Define pentesting and explain its importance
- Summarize common approaches to pentesting
- Describe each component of the planning ase of pentesting
- List directives that pentesters and clients should document in the planning ase of pentesting
- Contrast open box, closed box, and gray box approaches to pentesting
- Define vulnerability analysis and explain its role in pentesting
- Describe methods for the discovery ase of pentesting
- Summarize what happens in each step of the attack ase of pentesting
- Describe commonly exploited vulnerabilities
- Discuss the components of a penetration test report’s executive summary and technical review
- Distinguish events from incidents in the context of cybersecurity
- Explain what incident response is and why it’s important
- Contrast the three models for incident response teams
- Discuss the departments within an organization with which the incident response team should establish a working relationship
- List common attack vectors for cybersecurity incidents
- Recall essential components of an incident response policy
- Describe the three types of resources needed for effective incident response
- Summarize recommended practices for securing networks, systems, and applications
- Distinguish between precursors and indicators and list their common sources
- Describe the types of monitoring systems used for incident detection
- Discuss standard topics and impact categories to include in incident analysis documentation
- List parties that may require notification of a detected incident
- Summarize considerations for selecting an incident containment strategy
- Explain why forensics is an essential part of incident containment
- Describe the goals of the eradication and recovery ases of incident response
- Recall questions from the Sysadmin, Audit, Network, and Security (SANS) Institute’s checklist for incident response
- Describe “lessons learned” meetings and other activities that may be appropriate for post-incident analysis
- List common cybersecurity threats
- Describe three modern cybersecurity tools: QRadar, McAfee ePolicy Orchestrator (ePO), and next-generation firewalls

- Summarize how to manage a QRadar SIEM incident response queue
- Investigate QRadar offenses using QRadar SIEM
- Generate a QRadar report
- Modify QRadar’s network hierarchy settings
- Define digital forensics
- List standard data sources for digital forensics
- Summarize the objectives of digital forensics
- Discuss the challenges that various data collection methods present
- Describe the National Institute for Standards and Technology’s (NIST’s) three steps for data collection
- Explain the role that chain of custody plays in data collection
- Summarize the obstacles inherent in forensic examination
- Describe the analysis step in digital forensics
- Summarize the components of a forensic report and the best practices for writing them
- Describe essential methods, tools, and considerations for collecting, preserving, and analyzing data files
- Contrast volatile and non-volatile data and explain best practices for collecting each data type
- Summarize recommended forensic methods for collecting log information from Windows, macOS, and Linux systems
- Explain how different application components and types provide meaningful forensic data
- Describe the four layers of the TCP/IP model and their relevance for digital forensics
- Summarize the various sources of network data and the value of data obtainable from each
- Discuss methods for using network data to identify a cyberattacker
- Summarize the history of scripting languages and their common uses today
- Explain basic scripting concepts including script, variable, argument, parameter, if statement, and loop
- Describe the purpose and features of the JavaScript, Bash, Perl, PowerShell, binary, and hexadecimal scripting languages
- Summarize the benefits of using Python
- Recall Python rules for syntax, data types, and strings
- Describe Python data structures
- Explain the basic syntax of conditions in Python branching
- Discuss what Python functions and methods are
- Explain what a Python library is and describe examples

Duration:

16 Hrs

Topics:

Unit 1: Penetration Testing

Unit 2: Incident Response

Unit 3: Digital Forensics

Unit 4: Introduction to Scripting

Audience:

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