Course Syllabus

CompTIA Security+

Instructor Name: Kelly Handerhan

Instructor Website: Cybertrain.it

Instructor Contact: N/A

Course Creation Date: July 15, 2021

Course Description and Goals

Course Description: The Security+ credential is one of the most essential certifications in the world of information security today. Our students will obtain knowledge across a wide variety of topics and will demonstrate mastery of basic security skills. The course begins with an introduction to security concepts so that even students with limited experience can be brought up to speed quickly, so there are no prerequisites necessary.

After our introduction, students will study malware and examine different types of attackers, their motives, and the various attack vectors as well as the attacks themselves. We will cover the most common attacks today, such as worms, viruses, rootkits, trojans, and others. Next up is an introduction to cryptography and the security services which are provided. We begin with dissecting common cryptography terms such as initialization vectors, algorithms, keys, seeds, and salts. Then we move on to dissecting the cryptographic processes for encryption with a study on symmetric, asymmetric, and hybrid algorithms and discuss the benefits of each. Next up comes integrity checking and the use of digital signatures and other tools to provide authenticity and non-repudiation.

After cryptography, our next section introduces an assessment of a typical network environment and the importance of security through a thorough discussion of the OSI Reference Model, network protocols, network devices, security devices, detective software, and monitoring tools. Next, Operations Security focuses on maximizing the confidentiality, integrity, and availability of systems used by the organizations developing a risk-based approach. We examine standards, guidelines, and procedures and ensure their alignment to the organization's strategic goals so that we can ensure value delivery to the organization. Students will then move on to our last

topic, Identity and Access Management. In this final domain, we look at the provisioning of user accounts, authentication requirements, single sign-on, authorization, and auditing.

After this course, students should be equipped with the knowledge and skills necessary to pass the Security+ Certification exam, as well as being able to enter the workforce in a beginning role in systems or network security.

Target Audience: This course is best suited for those new to network security or those with more experience who wish to fill in any gaps in their knowledge.

Course Level: Beginner

Prerequisites: There are no prerequisites for this course, although knowledge of networking is beneficial.

Supplementary Materials: While there are no supplementary materials to this course, students are encouraged to take notes and study diligently.

Course Goals: By the end of this course, learners should be able to:

- ❏ Explain the basic tenets of security and the most common threats to each
- ❏ Discuss the differences between various types of malware and mitigating strategies for each
- ❏ Understand the basics of cryptography including its use to provide confidentiality, authenticity, integrity, and non-repudiation
- ❏ Understand network functionality and requires and recommend security controls to mitigate risks associated with telecommunications
- ❏ Provide high availability for network-based resources through understanding the processes of RAID, clustering, incident response, disaster recovery, and business continuity

Labs Used: N/A

NOTE: This course covers the five domains of the CompTIA Security+ (SYO-601) exam but does not cover them in the same order listed by CompTIA. Kelly Handerhan, the instructor, has had a lot of experience teaching Security+ and prefers to teach it in a certain order that she finds is most valuable for her students. Although the arrangement of the course material does not match up exactly with the official CompTIA domains, you can rest assured that the course is comprehensive and all of the content in the course is covered in the exam. Below is a description of how the domains of the exam are covered by the modules in this course:

- Domain 1: Attacks, Threats, and Vulnerabilities - is covered in **Module 2** of this course
- Domain 2: Architecture and Design - is covered in **Modules 3 and 6** of this course
- Domain 3: Implementation - is covered in **Modules 3, 4, and 5** of this course
- Domain 4: Operations and Incident Response - is covered in **Module 6** of this course
- Domain 5: Governance, Risk, and Compliance - is covered in **Module 1** of this course

Course Outline

Module 1 | Risk Management and Security Basics

1.1 Why Security+
1.2 Risk Management and Security Basics
1.3 Risk Management Overview
1.4 Use and Misuse Cases
1.5 Risk Assessment
1.6 Risk Mitigation
1.7 Risk Monitoring
1.8 Security Principles - Confidentiality
1.9 Integrity and Availability Threats and Mitigation
1.10 Security Principles Wrap-Up

Module 2 | Threats, Attacks and Vulnerabilities

2.1 Understanding Attacks
2.2 Social Engineering
2.3 Malware
2.4 Network-Based Attacks

2.5 Spoofing and Redirection
2.6 DNS Service
2.7 Passwords
2.8 Wireless Security Part 1
2.9 Wireless Security Part 2
2.10 Application Attacks
2.11 Code Injection and Cross Site Scripting
2.12 XSRF Race Conditions and Memory Issues

Module 3 | Cryptography
3.1 Cryptography Introduction and Services
3.2 Cryptography Definitions: Initialization Vectors
3.3 Algorithms and Keys
3.4 Desirable Qualities of Algorithms and Keys
3.5 Symmetric Cryptography
3.6 Symmetric Ciphers Stream and Block
3.7 Asymmetric Cryptography
3.8 Hashing for Integrity
3.9 MAC Message Authentication Code
3.10 Hybrid Cryptography SSL and TLS
3.11 SSL, TLS and PKI Introduction
3.12 PKI Continued
3.13 PGP and SMIME

Module 4 | Network Security
4.1 Networking Concepts
4.2 Network Connectivity
4.3 Network Services Continued: DHCP and IPAM
4.4 OSI Model Intro and Encapsulation
4.5 OSI Layers 1 and 2
4.6 OSI Continued Layers 3 and 4
4.7 OSI Layers 5 6, 7 and Summary
4.8 Ports and Protocols Introduction
4.9 Protocols of the TCPIP Suite Part 1

4.10 Protocols of the TCPIP Suite Part 2
4.11 Network Services DNS
4.12 Network Storage
4.13 Remote Access
4.14 Tunneling and IPSec Part 1
4.15 Tunneling and IPSec Part 2

Module 5 | Network Connectivity Devices
5.1 Network Connectivity Devices Part 1
5.2 Network Connectivity Devices Part 2
5.3 Switch and VLAN Configuration Part 1
5.4 Switch and VLAN Configuration Part 2
5.5 Routing
5.6 Network Address Translation
5.7 Firewalls
5.8 Firewall Best Practices
5.9 Intrusion Detection and Prevention

Module 6 | Operational Security
6.1 Introduction and Policy
6.2 Policies and Best Practices Part 1
6.3 Policies and Best Practices Part 2
6.4 Scanning Monitoring and Patching
6.5 Patch Lifecycle Baselines and Traffic Analysis
6.6 Fault Management
6.7 RAID and Data Backups
6.8 Business Continuity and Disaster Recovery Part 1
6.9 Business Continuity and Disaster Recovery Part 2
6.10 Virtualization Part 1
6.11 Virtualization Part 2
6.12 Cloud Computing
6.13 Cloud Services
6.14 Cloud Deployment Models and Cloud Wrap-Up
6.15 IoT Introduction

6.16 OWASP IoT and Wrap-up
6.17 Hardening the System Part 1
6.18 Hardening the System Part 2
6.19 Vulnerability Assessments and Penetration Tests
6.20 Incident Response
6.21 Forensic Investigations

Module 7 | Identity and Access Management
7.1 Identity and Access Management Introduction
7.2 Authentication
7.3 Single Sign-On Kerberos Part 1
7.4 Single Sign-On Kerberos Part 2
7.5 Single Sign-On with Federated Services Part 1
7.6 Single Sign-On with Federated Services Part 2
7.7 Network Access Control and Authentication Wrap-Up
7.8 Authorization
7.9 Auditing and Wrap-Up