



CompTIA S+ Course Curriculum

www.hiit.ng

Course Overview:

This CompTIA Security+ course is designed to equip participants with the foundational knowledge and skills necessary to understand and implement effective cybersecurity measures within an organization. Overall, the course aims to provide a comprehensive understanding of Cybersecurity principles and practices, preparing participants for the CompTIA Security+ certification exam and enabling them to contribute effectively to cybersecurity efforts within their organizations.

WEEK	DAY	MODULE	OBJECTIVES	TOPICS	HOURS
Week 1	Day 1	1. Introduction to Cybersecurity.	To Understand fundamental cybersecurity concepts, terminology, and principles to establish a foundation for further learning.	1. Overview of Cybersecurity Concepts, Terminology, and Principles.	1.0
✓	✓	✓	To Recognize the significance of cybersecurity in protecting assets, data, and systems within modern organizations.	1. Impact of cyber threats on business operations. 2. Legal and financial implications of cybersecurity breaches.	1.0
✓	Day 2	2. Threats, Attacks and Vulnerabilities.	To Identify various types of cyber threats and understand how they can compromise security.	1. Types of malware (e.g., viruses, worms, ransomware) 2. Techniques used in phishing and social engineering attacks	0.5
✓	✓	✓	To Recognize common attack vectors and techniques used by cyber attackers to exploit vulnerabilities.	1. Network-based attacks (e.g. DDoS, man-in-the-middle). 2. Exploiting software vulnerabilities (e.g. buffer overflow, SQL injection).	0.5
✓	✓	Setting Up Your Virtual Lab.	To Install VMware Workstation on your system To Download and install Ubuntu Desktop inside a virtual machine To Get familiar with Linux and ensure your VM has internet access		1.0
Week 2	Day 3	3. Security Technologies and Tools.	To Understand the functionality and purpose of network security devices in protecting against threats and attacks.	1. Intrusion detection systems (IDS) vs. Intrusion Prevention Systems (IPS). 2. Next-generation firewall features and capabilities.	0.5

WEEK	DAY	MODULE	OBJECTIVES	TOPICS	HOURS
Week 2	Day 3	...Security Technologies and Tools contd...	To Learn about encryption techniques and protocols for securing data in transit and at rest.	1. Symmetric vs. asymmetric encryption 2. Protocols for securing data in transit (e.g. SSH, HTTPS).	0.5
✓	✓	Understanding Hashing and Decryption.	To Try decrypting encoded messages. To Distinguish between hashing and encryption. To Identify common hashing algorithms and encryption ciphers.		1.0
✓	Day 4	4. Architecture and Design.	To Design secure network architectures by implementing appropriate protocols and services.	1. Secure Network Topologies, Protocols, and Services. *Network segmentation strategies. *Implementing secure protocols.	0.5
✓	✓	✓	To Apply security controls at different layers of the OSI model to mitigate risks effectively.	1. Implementing Security Controls at Various OSI Model Layers. 2. Application-layer security controls (e.g., web application firewalls). 3. Data-link layer security protocols (e.g., MACsec, IEEE 802.1X).	0.5
✓	✓	Secure Network Topology Design Using Draw.io	To design a secure network architecture using draw.io positioning correctly firewalls and routers and switches and other infrastructure devices.		1.0
Week 3	Day 5	5. Identity and Access Management (IAM).	To Implement authentication mechanisms to verify the identity of users and devices.	1. Authentication Mechanisms: Passwords, Biometrics *Password policies and best practices. *Biometric authentication technologies (e.g. fingerprint, facial recognition).	0.5
✓	✓	✓	To Understand access control models and implement access controls based on the principle of least privilege.	1. Role-based access control (RBAC) implementation 2. Attribute-based access control (ABAC) principles.	0.5
✓	✓	Implementing File System Permissions.	Apply access control to files using Linux permissions. Test and audit user access rights.		1.0
✓	Day 6	6. Risk Management.	To Assess, analyze, and mitigate cybersecurity risks to minimize potential impact.	1. Qualitative vs. quantitative risk assessment methods. 2. Risk treatment strategies (e.g., risk avoidance, risk transfer).	0.5

WEEK	DAY	MODULE	OBJECTIVES	TOPICS	HOURS
Week 3	Day 6	...Risk Management contd...	To Develop incident response plans and procedures to effectively respond to security incidents.	1. Incident categorization and prioritization. 2. Establishing incident response teams and communication protocols.	0.5
✓	✓	Phishing Simulation.	To understand red flags in email content, links, and sender information. To reinforce user vigilance using an interactive simulation.		1.0
Week 4	Day 7	7. Cryptography.	To Understand cryptographic concepts and their application in securing data and communications.	1. Common encryption algorithms (e.g., AES, RSA). 2. Digital signature applications and use cases.	0.5
✓	✓	✓	To Learn about cryptographic protocols used to secure data in transit over networks.	1. SSL/TLS handshake process and encryption methods. 2. IPsec tunneling and authentication protocols (e.g., IKE, ESP).	0.5
✓	✓	SSL/TLS handshake exploration using curl.	To understand each step in the SSL/TLS handshake process. To use command-line tools to inspect certificate chains and cipher negotiation.		1.0
✓	Day 8	8. Security Operations.	To Implement security monitoring, logging, and auditing techniques to detect and respond to security incidents.	1. Security information and event management (SIEM) solutions. 2. Log aggregation and correlation techniques.	0.5
✓	✓	✓	To Develop procedures for detecting, responding to, and recovering from security incidents to minimize damage and downtime.	1. Threat hunting methodologies. 2. Business continuity and disaster recovery planning.	0.5
✓	✓	Host-Based Intrusion Detection with Wazuh.	Deploy and configure HIDS on a host system. Analyze alerts generated by suspicious activities.		1.0
				Total	16