CyberGuardian CompTIA Security+ Course Breakdown

A structured breakdown of your training sessions

Day 1:

What we will cover:

- Course Introduction
- Security Concepts
- Security Controls
- Threat Actors
- Attack Surface
- Social Engineering
- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

Hands-On Labs:

- ➔ Exploring the Lab Environment
- ➔ Perform System Configuration Gap Analysis
- ➔ Configuring Examples of Security Control Types
- ➔ Finding Open Service Ports
- ➔ Using SET to Perform Social Engineering
- ➔ Using Storage Encryption
- ➔ Using Hashing and Salting

Day 2:

What we will cover:

- Authentication
- Authorization
- Identity Management
- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications
- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture
- Asset Management

- Redundancy Strategies
- Physical Security

Hands-On Labs:

- Managing Password Security
- Managing Permissions
- Using IPSec Tunneling
- Setting up Remote Access
- Using Virtualization
- Using Containers
- Performing Drive Sanitization
- Implement Backups

Day 3:

What we will cover:

- Device and OS Vulnerabilities
- Application and Cloud Vulnerabilities
- Vulnerability Identification Methods
- Vulnerability Analysis and Remediation
- Network Security Baselines
- Network Security Capability Enhancement
- Implement Endpoint Security
- Mobile Device Hardening
- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

Hands-On Labs:

- Exploiting and Detecting SQLi
- Working with Threat Feeds
- Performing Vulnerability Scans
- Understanding Security Baselines
- Implementing a Firewall
- Using Group Policy
- System Hardening
- Performing DNS Filtering
- Configuring System Monitoring

Day 4:

What we will cover:

- Incident Response
- Digital Forensics
- Data Sources
- Alerting and Monitoring Tools
- Malware Attack Indicators
- Physical and Network Attack Indicators
- Application Attack Indicators

Hands-On Labs:

- ➔ Incident Response: Detection
- ➔ Performing Digital Forensics
- ➔ Using Network Sniffers
- ➔ Performing Root Cause Analysis
- ➔ Detecting and Responding to Malware
- ➔ Understanding On-Path Attacks

Day 5:

What we will cover:

- Policies, Standards, and Procedures
- Change Management
- Automation and Orchestration
- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments
- Data Classification and Compliance
- Personnel Policies
- Course Summary/Exam Practice

Hands-On Labs:

- ➔ Using a Playbook
- ➔ Implementing Allow Lists and Deny Lists
- ➔ Use Cases of Automation and Scripting
- ➔ Performing Reconnaissance
- ➔ Performing Penetration Testing
- ➔ Training and Awareness through Simulation
- ➔ Challenge Lab: Network Incident Investigation and Remediation