

# 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

### Hands-On Labs:

- Exploring the Lab Environment
- Performing System Configuration Analysis
- Configuring Examples of Security Control Types

## Day 2:

### What we will cover:

- Attack Surface
- Social Engineering
- Cryptographic Algorithms
- Public Key Infrastructure
- Cryptographic Solutions

### Hands-On Labs:

- Finding Open Service Ports
- Using SET to Perform Social Engineering
- Using Storage Encryption
- Using Hashing and Salting



### Day 3:

#### What we will cover:

- Authentication
- Authorization
- Identity Management
- Enterprise Network Architecture
- Network Security Appliances
- Secure Communications

#### Hands-On Labs:

- Managing Password Security
- Managing Permissions
- Using IPSec Tunneling
- Setting up Remote Access

### Day 4:

#### What we will cover:

- Cloud Infrastructure
- Embedded Systems and Zero Trust Architecture
- Asset Management
- Redundancy Strategies
- Physical Security

#### Hands-On Labs:

- Using Virtualization
- Using Containers
- Implement Backups
- Performing Drive Sanitization

### Day 5:

#### 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



### **Hands-On Labs:**

- Exploiting and Detecting SQLi
- Working with Threat Feeds
- Performing Vulnerability Scans
- Understanding Security Baselines
- Implementing a Firewall

### **Day 6:**

#### **What we will cover:**

- Implement Endpoint Security
- Mobile Device Hardening
- Application Protocol Security Baselines
- Cloud and Web Application Security Concepts

### **Hands-On Labs:**

- Using Group Policy
- Hardening of Systems
- Performing DNS Filtering
- Configuring System Monitoring

### **Day 7:**

#### **What we will cover:**

- Incident Response
- Digital Forensics
- Data Sources
- Alerting and Monitoring Tools

### **Hands-On Labs:**

- Incident Response: Detection
- Using Network Sniffers
- Performing Digital Forensics
- Performing Root Cause Analysis



## Day 8:

### What we will cover:

- Malware Attack Indicators
- Physical and Network Attack Indicators
- Application Attack Indicators

### Hands-On Labs:

- Detecting and Responding to Malware
- Understanding On-Path Attacks

## Day 9:

### What we will cover:

- Policies, Standards, and Procedures
- Change Management
- Automation and Orchestration
- Risk Management Processes and Concepts
- Vendor Management Concepts
- Audits and Assessments

### Hands-On Labs:

- Using a Playbook
- Implementing Allow Lists and Deny Lists
- Use Cases of Automation and Scripting
- Performing Reconnaissance
- Performing Penetration Testing

## Day 10:

### What we will cover:

- Data Classification and Compliance
- Personnel Policies
- Course Summary/Exam Practice

### Hands-On Labs:

- Training and Awareness through Simulation
- Challenge Lab: Network Incident Investigation and Remediation

