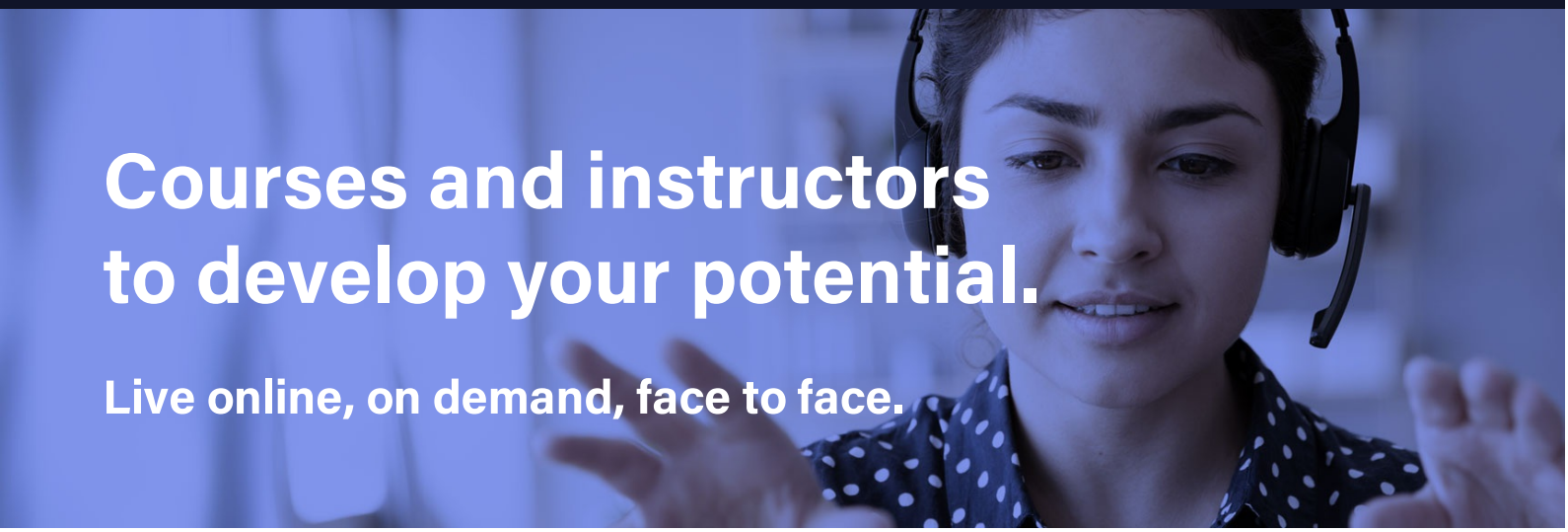
GO.COURSES



Courses and instructors to develop your potential.

Live online, on demand, face to face.

Comptia Security+

The CompTIA Security+ exam will certify the successful candidate has the knowledge and skills required to install and configure systems to secure applications, networks, and devices; perform threat analysis and respond with appropriate mitigation techniques; participate in risk mitigation activities; and operate with an awareness of applicable policies, laws, and regulations.

What will I learn?

LESSON 1

Threats, Attacks, and Vulnerabilities: Indicators of Compromise - Why is Security Important? - Security Policy - Threat Actor Types - The Kill Chain - Social Engineering - Phishing - Malware Types - Trojans and Spyware

LESSON 2

Open Source Intelligence - Lab - VM Orientation - Lab - Malware Types - Critical Security Controls - Security Control Types - Defence in Depth - Frameworks and Compliance - Vulnerability Assessments and Pentests

LESSON 3

Key features

- **Live Online Training with a real person - not dull e-learning**
- **Fully certified trainer**
- **Get key skills and practical knowledge**
- **This course is available for groups and 1-2-1 live online**
- **Course materials included**
- **Recognised course certificate**

Interested?

Call us: 01225 308979

Email us: info@go.courses

Security Assessment Techniques - Pen Testing Concepts - Vulnerability Scanning Concepts - Exploit Frameworks - Lab - Using Vulnerability Assessment Tools - Security Posture Assessment Tools - Topology Discovery

LESSON 4

Service Discovery - Packet Capture - Packet Capture Tools - Remote Access Trojans - Honeypots and Honeynets - Lab - Using Network Scanning Tools 1 - Lab - Using Network Scanning Tools 2 - Lab - Using Steganography Tools - Incident Response - Incident Response Procedures - Preparation Phase - Identification Phase - Containment Phase - Eradication and Recovery Phases

LESSON 5

Identity and Access Management: Cryptography - Uses of Cryptography - Cryptographic Terminology and Ciphers - Cryptographic Products - Hashing Algorithms - Symmetric Algorithms - Asymmetric Algorithms

LESSON 6

Diffie-Hellman and Elliptic Curve - Transport Encryption - Cryptographic Attacks - Lab - Implementing Public Key Infrastructure - Public Key Infrastructure - PKI Standards - Digital Certificates - Certificate Authorities

LESSON 7

Types of Certificate - Implementing PKI - Storing and Distributing Keys - Key Status and Revocation - PKI Trust Models - PGP / GPG - Lab - Deploying Certificates and Implementing Key Recovery - Identification and Authentication - Access Control Systems - Identification - Authentication - LAN Manager / NTLM - Kerberos - PAP, CHAP, and MS-CHAP - Password Attacks - Token-based Authentication - Biometric Authentication

LESSON 8

Common Access Card - Lab - Using Password Cracking Tools - Identity and Access Services - Authorization - Directory Services - RADIUS and TACACS+ - Federation and Trusts - Federated Identity

Protocols - Account Management - Formal Access Control Models - Account Types - Windows Active Directory - Creating and Managing Accounts - Account Policy Enforcement - Credential Management Policies - Account Restrictions -

LESSON 9

Accounting and Auditing - Lab - Using Account Management Tools

LESSON 10

3Architecture and Design (1): Secure Network Design - Network Zones and Segments - Subnetting - Switching Infrastructure - Switching Attacks and Hardening - Endpoint Security - Network Access Control - Routing Infrastructure - Network Address Translation - Software Defined Networking - Lab - Implementing a Secure Network Design - Firewalls and Load Balancers - Basic Firewalls - Stateful Firewalls - Implementing a Firewall or Gateway - Web Application Firewalls - Proxies and Gateways - Denial of Service Attacks - Load Balancers - Lab - Implementing a Firewall - IDS and SIEM - Intrusion Detection Systems - Configuring IDS - Log Review and SIEM - Data Loss Prevention - Malware and Intrusion Response - Lab - Using an Intrusion Detection System - Secure Wireless Access - Wireless LANs - WEP and WPA - Wi-Fi Authentication - Extensible Authentication Protocols - Additional Wi-Fi Security Settings - Wi-Fi Site Security - Personal Area Networks - Physical Security Controls - Site Layout and Access - Gateways and Locks - Alarm Systems - Surveillance Hardware Security

LESSON 11

Environmental Controls

LESSON 12

Architecture and Design (2): Secure Protocols and Services - DHCP Security - DNS Security - Network Management Protocols - HTTP and Web Servers - SSL / TSL and HTTPS - Web Security Gateways - Email Services

LESSON 13

S/MIME - File Transfer - Voice and Video Services (VoIP and VTC) - Lab - Implementing Secure Network Addressing Services - Lab - Configuring a Secure Email Service - Secure Remote Access - Remote

Email Service - Secure Remote Access - Remote Access - Architecture - Virtual Private Networks - IPSec - Remote Access Servers - Remote Administration Tools - Hardening Remote Access Infrastructure - Lab - Implementing a Virtual Private Network - Secure Systems Design

LESSON 14

Trusted Computing - Hardware / Firmware Security - Peripheral Device Security - Secure Configurations - OS Hardening - Patch Management - Embedded Systems - Security for Embedded Systems - Secure Mobile Device Services - Mobile Device Deployments - Mobile Connection Methods - Mobile Access Control Systems - Enforcement and Monitoring - Secure Virtualization and Cloud Services - Virtualization Technologies - Virtualization Security Best Practices - Cloud Computing - Cloud Security Best Practices

LESSON 15

Risk Management: Forensics - Forensic Procedures - Collecting Evidence - Capturing System Images - Handling and Analyzing Evidence - Lab - Using Forensic Tools - Disaster Recovery and Resiliency - Continuity of Operations Plans - Disaster Recovery Planning - Resiliency Strategies - Recovery Sites - Backup Plans and Policies - Resiliency and Automation Strategies - Risk Management - Business Impact Analysis - Identification of Critical Systems - Risk Assessment - Risk Mitigation - Secure Application Development - Application Vulnerabilities - Application Exploits - Web Browser Exploits - Secure Application Design - Secure Coding Concepts

LESSON 16

Auditing Applications - Secure DevOps - Lab - Identifying a Man-in-the-Browser Attack - Organizational Security - Corporate Security Policy - Personnel Management Policies - Interoperability Agreements - Data Roles

LESSON 17

Data Sensitivity Labeling and Handling - Data Wiping and Disposal - Privacy and Employee Conduct Policies - Security Policy Training