skilltec training

Moving forward in knowledge and training

CompTIA
Training Course Brochure

01752 227330
enquiries@skilltec.co.uk
www.skilltec.co.uk

skilltec training

Moving forward in knowledge and training

CompTIA Training Course Brochure

CompTIA A+ Certification (Accelerated)

Course Code CPCERT
Duration 5 days

Overview

CompTIA's A+ Certification is the industry standard for validating the foundational skills needed by support technicians in today's digital world. A technical support professional does much more than fix a PC, they now have to understand how applications work across systems and be capable of solving problems that help to keep the business running smoothly.

The CompTIA A+ Certification has recently been updated to reflect the growing focus on topics such cybersecurity, Privacy, IoT, Scripting, Virtualisation and Cloud.

Audience

Entry-level IT Professionals in a technical support role.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Support basic IT infrastructure, including endpoint management, advanced device connectivity troubleshooting, and basic networking
- Configure and support PC, mobile and IoT device hardware, including components, connectors and peripherals
- Implement basic data backup and recovery methods and apply data storage and management best practices
- Demonstrate baseline security skills for IT support professionals, including detecting and removing malware, addressing privacy concerns, physical security and device hardening
- Configure device operating systems, including Windows, Mac, Linux, Chrome OS, Android and iOS and administer client-based as well as cloud-based (SaaS) software
- Troubleshoot and problem solve core service and support challenges while applying best practices for documentation, change management, and the use of scripting in IT support.

Pre-Requisites

To attend this course, you should have the following pre-requisites:

- Recognize the main components of a PC and different data media such as USB drives and DVD.
- Start the computer and navigate the desktop.
- Use Windows Explorer to create directories and subdirectories and manage files.
- Use a web browser such as Internet Explorer to view websites.

Course Contents

Supporting Operating Systems

- Identify Common Operating Systems
- Troubleshooting Methodology
- Use Windows Features and Tools
- Manage Files in Windows
- Manage Disks in Windows
- Manage Devices in Windows

Installing and Configuring PC Components

- Use Appropriate Safety Procedures
- PC Components
- Common Connection Interfaces
- Install Peripheral Devices

Installing, Configuring and Troubleshooting Display and Multimedia Devices

- Install and Configure Display Devices
- Troubleshoot Display Devices
- Install and Configure Multimedia Devices

Installing, Configuring and Troubleshooting Storage Devices

- Install System Memory
- Install and Configure Mass Storage Devices
- Install and Configure Removable Storage
- Configure RAID
- Troubleshoot Storage Devices

Installing, Configuring and Troubleshooting Internal System Components

- Install and Upgrade CPUs
- Configure and Update BIOS/UEFI
- Install Power Supplies
- Troubleshoot Internal System Components
- Configure a Custom PC

Installing, Configuring and Maintaining Operating Systems

- Configure and Use Linux
- Configure and Use macOS
- Install and Upgrade Operating Systems
- Maintain OSs

Maintaining and Troubleshooting Microsoft Windows

- Install and Manage Windows Applications
- Manage Windows Performance
- Troubleshoot Windows

Network Infrastructure Concepts

- Wired Networks
- Network Hardware Devices
- Wireless Networks
- Internet Connection Types
- Network Configuration Concepts
- Network Services

Configuring and Troubleshooting Networks

- Configure Network Connection Settings
- Install and Configure SOHO Networks
- Configure SOHO Network Security
- Configure Remote Access
- Troubleshoot Network Connections
- Install and configure IoT Devices

Managing Users, Workstations and Shared Resources

- Manage Users
- Configure Shared Resources
- Configure Active Directory Accounts and Policies

Implementing Client Virtualization and Cloud Computing

- Configure Client-Side Virtualization
- Cloud Computing Concepts

Security Concepts

- Logical Security Concepts
- Threat and Vulnerabilities
- Physical Security Measures

Securing Workstations and Data

- Implement Security Best Practices
- Implement Data Protection Policies
- Protect Data During Incident Response

Troubleshooting Workstation Security Issues

- Detect, Remove and Prevent Malware
- Troubleshoot Common Workstation Security Issues

Supporting and Troubleshooting Laptops

- Use Laptop Features
- Install and Configure Laptop Hardware
- Troubleshoot Common Laptop Issues

Supporting and Troubleshooting Mobile Devices

- Mobile Device Types
- Connect and Configure Mobile Device Accessories
- Configure Mobile Device Network Connectivity
- Support Mobile Apps
- Secure Mobile Devices
- Troubleshoot Mobile Device Issues

Installing, Configuring and Troubleshooting Print Devices

- Maintain Laser Printers
- Maintain Inkjet Printers
- Maintain Impact, Thermal and 3D Printers
- Install and Configure Printers
- Troubleshoot Print Device Issues
- Install and Configure Imaging Devices

Implementing Operational Procedures

- Environmental Impacts and Controls
- Create and Maintain Documentation
- Use Basic Change Management Best Practices
- Implement Disaster Prevention and Recovery Methods
- Basic Scripting Concepts
- Professionalism and Communication

Exam Details

This globally recognised vendor-neutral certification requires that you pass two exams: CompTIA A+ Core 1 Exam 220-1001 and Core 2 Exam 220-1002.

CompTIA CYSA+ (Cybersecurity Analyst)

Course Code	CPCYSA
Duration	5 days

Overview
The CompTIA Cybersecurity Analyst (CySA+) certification verifies that successful candidates have the knowledge and skills required to leverage intelligence and threat detection techniques, analyze and interpret data, identify and address vulnerabilities, suggest preventative measures, and effectively respond to and recover from incidents.

Audience
The CompTIA Cybersecurity Analyst (CySA+) examination is designed for IT security analysts, vulnerability analysts, or threat intelligence analysts. The exam will certify that the successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization.

Learning Objectives
The CompTIA CySA+ certification is a vendor-neutral credential. The CompTIA CySA+ exam (Exam CS0-001) is an internationally targeted validation of intermediate-level security skills and knowledge. The course has a technical, “hands-on” focus on IT security analytics.

The CompTIA CySA+ exam is based on these objectives:

- Threat Management
- Vulnerability Management
- Cyber Incident Response
- Security Architecture and Tool Sets

Pre-Requisites
While there is no required prerequisite, the CompTIA CySA+ certification is intended to follow CompTIA Security+ or equivalent experience. It is recommended for CompTIA CySA+ certification candidates to have the following:

- 3-4 years of hands-on information security or related experience
- Network+, Security+, or equivalent knowledge

Course Contents

1. Threat Management
Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.

Procedures/common tasks:
- Topology discovery
- OS fingerprinting
- Service discovery
- Packet capture
- Log review
- Router/firewall ACLs review
- Email harvesting
- Social media profiling
- Social engineering
- DNS harvesting
- Phishing

Variables:
- Wireless vs. wired
- Virtual vs. physical
- Internal vs. external
- On-premises vs. cloud

Tools:
- NMAP
- Host scanning
- Network mapping
- NETSTAT
- Packet analyzer
- IDS/IPS
- HIDS/NIDS
- Firewall rule-based and logs
- Syslog
- Vulnerability scanner

Given a scenario, analyze the results of a network reconnaissance.

Point-in-time data analysis:
- Packet analysis
- Protocol analysis
- Traffic analysis
- Netflow analysis
- Wireless analysis

Data correlation and analytics:
- Anomaly analysis
- Trend analysis
- Availability analysis
- Heuristic analysis
- Behavioural analysis

Data output:
- Firewall logs
- Packet captures
- NMAP scan results
- Event logs
- Syslogs
- IDS report

Tools:

- SIEM
- Packet analyzer
- IDS
- Resource monitoring tool
- Netflow analyzer

Given a network-based threat, implement or recommend the appropriate response and countermeasure.

Network segmentation:

- System isolation
- Jump box
- Honeypot
- Endpoint security

Group policies

ACLs:

- Sinkhole

Hardening:

- Mandatory Access Control (MAC)
- Compensating controls
- Blocking unused ports/services
- Patching

Network Access Control (NAC):

- Time-based
- Rule-based
- Role-based
- Location-based

Explain the purpose of practices used to secure a corporate environment.

Penetration testing:

- Rules of engagement

Reverse engineering:

- Isolation/sandboxing
- Hardware
- Software/malware

Training and exercises:

- Red team
- Blue team
- White team

Risk evaluation:

- Technical control review
- Operational control review
- Technical impact and likelihood

2. Vulnerability Management

Given a scenario, implement an information security vulnerability management process.

- Identification of requirements:
- Regulatory environments
- Corporate policy
- Data classification
- Asset inventory

Establish scanning frequency:

- Risk appetite
- Regulatory requirements
- Technical constraints
- Workflow

Configure tools to perform scans according to specification:

- Determine scanning criteria
- Tool updates/plug-ins
- Permissions and access

Execute scanning

Generate reports:

- Automated vs. manual distribution

Remediation:

- Prioritizing
- Communication/change control
- Sandboxing/testing
- Inhibitors to remediation
- Ongoing scanning and continuous monitoring

Given a scenario, analyze the output resulting from a vulnerability scan.

Analyze reports from a vulnerability scan:

- Review and interpret scan results

Validate results and correlate other data points

- Compare to best practices or compliance
- Reconcile results
- Review related logs and/or other data sources
- Determine trends

Compare and contrast common vulnerabilities found in the following targets within an organization.

Servers
Endpoints
Network infrastructure
Network appliances
Virtual infrastructure:

- Virtual hosts
- Virtual networks

Management interface
Mobile devices
Interconnected networks
Virtual private networks (VPNs)
Industrial Control Systems (ICSs)
SCADA devices

3. Cyber Incident Response

Given a scenario, distinguish threat data or behaviour to determine the impact of an incident.

Threat classification:

- Known threats vs. unknown threats
- Zero day
- Advanced persistent threat

Factors contributing to incident severity and prioritization:

- Scope of impact
- Types of data

Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.

- Forensics kit:
- Digital forensics workstation
- Write blockers
- Cables
- Drive adapters
- Wiped removable media
- Cameras
- Crime tape
- Tamper-proof seals
- Documentation/forms

Forensic investigation suite:

- Imaging utilities
- Analysis utilities
- Chain of custody
- Hashing utilities
- OS and process analysis
- Mobile device forensics
- Password crackers
- Cryptography tools
- Log viewers

Explain the importance of communication during the incident response process.

- Stakeholders:
- HR
- Legal
- Marketing
- Management

Purpose of communication processes:

- Limit communication to trusted parties
- Disclosure based on regulatory/legislative requirements
- Prevent inadvertent release of information
- Secure method of communication

Role-based responsibilities:

- Technical
- Management
- Law enforcement
- Retain incident response provider

Given a scenario, analyze common symptoms to select the best course of action to support incident response.

Common network-related symptoms:

- Bandwidth consumption
- Beaconing
- Irregular peer-to-peer communication
- Rogue devices on the network
- Scan sweeps
- Unusual traffic spikes

Common host-related symptoms:

- Processor consumption
- Memory consumption
- Drive capacity consumption
- Unauthorized software
- Malicious processes
- Unauthorized changes
- Unauthorized privileges
- Data exfiltration

Common application-related symptoms:

- Anomalous activity
- Introduction of new accounts
- Unexpected output
- Unexpected outbound communication
- Service interruption
- Memory overflows

Summarize the incident recovery and post-incident response process.

Containment techniques:

- Segmentation
- Isolation
- Removal
- Reverse engineering

Eradication techniques:

- Sanitization
- Reconstruction/reimage
- Secure disposal

Validation:

- Patching
- Permissions
- Scanning
- Verify logging/communication to security monitoring

Corrective actions:

- Lessons learned report
- Change control process
- Update incident response plan
- Incident summary report

4. Security Architecture and Tool Sets
Explain the relationship between frameworks, common policies, controls, and procedures.

Regulatory compliance
Frameworks:
- NIST
- ISO
- COBIT
- SABSA
- TOGAF
- ITIL

Policies:
- Password policy
- Acceptable use policy
- Data ownership policy
- Data retention policy
- Account management policy
- Data classification policy

Controls:
- Control selection based on criteria
- Organizationally defined parameters
- Physical controls
- Logical controls
- Administrative controls

Procedures:
- Continuous monitoring
- Evidence production
- Patching
- Compensating control development
- Control testing procedures
- Manage exceptions
- Remediation plans

Verifications and quality control:
- Audits
- Evaluations
- Assessments
- Maturity model
- Certification

Given a scenario, use data to recommend remediation of security issues related to identity and access management.

Security issues associated with context-based authentication:
- Time
- Location
- Frequency
- Behavioural

Security issues associated with identities:
- Personnel
- Endpoints
- Servers
- Services
- Roles
- Applications

Security issues associated with identity repositories:

- Directory services
- TACACS+
- RADIUS

Security issues associated with federation and single sign-on:

- Manual vs. automatic provisioning/deprovisioning
- Self-service password reset

Exploits:

- Impersonation
- Man-in-the-middle
- Session hijack
- Cross-site scripting
- Privilege escalation
- Rootkit

Given a scenario, review security architecture and make recommendations to implement compensating controls

Security data analytics:

- Data aggregation and correlation
- Trend analysis
- Historical analysis

Manual review:

- Firewall log
- Syslogs
- Authentication logs
- Event logs

Defense in depth:

- Personnel
- Processes
- Technologies
- Other security concepts

Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).

Best practices during software development:

- Security requirements definition
- Security testing phases
- Manual peer reviews
- User acceptance testing
- Stress test application
- Security regression testing
- Input validation
- Secure coding best practices:
- OWASP
- SANS
- Center for Internet Security

Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.

Preventative:
- IPS
- HIPS
- Firewall
- Antivirus
- Anti-malware
- EMET
- Web proxy
- Web Application Firewall (WAF)

Collective:
- SIEM
- Network scanning
- Vulnerability scanning
- Packet capture
- Command line/IP utilities
- IDS/HIDS

Analytical:
- Vulnerability scanning
- Monitoring tools
- Interception proxy

Exploit:
- Interception proxy
- Exploit framework
- Fuzzers

Forensics:
- Forensic suites
- Hashing
- Password cracking
- Imaging

Exam Details

This course leads to exam CS0-001 CompTIA CySA+. CompTIA CySA+ certification is a vendor-neutral credential.

CompTIA Cloud +

Course Code CPCLD
Duration 5 days

Overview

Learn how to protect cloud resources in a vendor-neutral environment. CompTIA Cloud+ CV0-002 provides the basic knowledge and skills needed to analyze, select, monitor, and protect cloud resources in a vendor-neutral format. This includes vulnerability management, network reconnaissance and monitoring, connecting networks to clouds, cloud migration, secure policies and procedures, host and network security, identity management systems, and incident response.

Audience

Customers interested in learning about analyzing, monitoring or protecting cloud resources and who are working with the cloud.

Learning Objectives

By actively participating in this course, you will learn about the following:

- About planning and deployment of a successful cloud system, how to view cloud deployment models and their network interactions, and how to evaluate computer resources required for successful cloud implementation
- How to test an environment before cloud deployment and how to migrate and integrate cloud services
- About security controls and about cryptography and its uses
- About data security and how to use security automation tools and techniques
- About cloud updates and patching, about cloud backup, and how to schedule and perform cloud maintenance
- About disaster planning and recovery
- About cloud resource provisioning and how to run performance analyses
- How to allocate compute resources and monitor resource usage
- About the troubleshooting process, about deployment and capacity troubleshooting, and how to troubleshoot automation issues
- How to troubleshoot network issues and about security troubleshooting

Pre-Requisites

This course assumes that students have some applied knowledge of computers, networks, and cybersecurity principles. Knowledge equivalent to the CompTIA Security+ certification is helpful but not necessary.

Course Contents

Introduction

Course setup

Chapter 1: Virtualization requirements
- Module A: Requirements and planning for successful system deployment
- Module B: Virtual network considerations
- Module C: Computer resources

Chapter 2: Deployment and migration
- Module A: Environment testing techniques
- Module B: Cloud integration and migration

Chapter 3: Security policies and compliance
- Module A: Security controls
- Module B: Cryptography and the cloud
- Module C: Applying cryptography

Chapter 4: Data and environment security
- Module A: Data security
- Module B: Security automation

Chapter 5: Environment maintenance
- Module A: Cloud updates and patching
- Module B: Cloud backup
- Module C: Cloud environment maintenance

Chapter 6: Disaster recovery and business continuity
- Module A: Business continuity

Chapter 7: Managing virtual environments
- Module A: Cloud resource provisioning
- Module B: Performance analysis

Chapter 8: Managing compute resources
- Module A: Allocating compute resources
- Module B: Monitoring resource usage

Chapter 9: Deployment troubleshooting
- Module A: The troubleshooting process
- Module B: Deployment and capacity troubleshooting
- Module C: Automation troubleshooting

Chapter 10: Infrastructure troubleshooting
- Module A: Network troubleshooting
- Module B: Security troubleshooting

Lab Topics Include:
- Creating VMs and virtual networks

- Demonstrating network isolation
- Migrating VMs from a cloud provider
- Enabling authentication and authorization controls
- Encrypting virtual disks and storage containers
- Configuring backup and recovery options
- Setting up redundancy and high availability options
- Creating and configuring web applications

Exam Details

This course maps to the CompTIA Cloud+ CV0-002 certification exam. Objective coverage is marked throughout the course.

CompTIA IT Fundamentals

Course Code CPITFD
Duration 3 days

Overview

This 3-day course is intended for those wishing to qualify with CompTIA IT Fundamentals Certification. CompTIA Information Technology (IT) Fundamentals Certification is the essential qualification for beginning a career in PC support.

The CompTIA IT Fundamentals Certification exam is designed to show that the successful candidate has the knowledge to identify and explain basic computer components, set up a basic workstation, conduct basic software installation, establish basic network connectivity, identify compatibility issues, and identify/prevent basic security risks. Further this exam will assess the candidate's knowledge in the areas of safety and preventative maintenance of computers.

Audience

CompTIA IT Fundamentals is a starter qualification for students and career changes to help decide whether they can be successful in pursuing a career in IT. It is ideal for those with no previous computer experience considering a career as an IT technician or in IT customer support / helpdesk.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Set up a computer workstation running Windows and use basic software applications.
- Understand the functions and types of devices used within a computer system.
- Apply basic computer maintenance and support principles.
- Configure computers and mobile devices to connect to home networks and to the internet.
- Identify security issues affecting the use of computers and networks

Pre-Requisites

Some experience with using a keyboard and mouse would be helpful but is not essential.

Course Contents

Module 1 – Operating Systems and Software

Computers and Operating Systems
- Information Technology
- Personal Computers (PC)
- Functions of an Operating System
- Types of Operating System
- Microsoft Windows
- Apple Mac OS X and iOS and Blackberry
- Linux, Chrome, and Android

Setting up a Workstation and Using Windows
- Setting up a PC System
- Ergonomic Concepts
- Navigating an OS
- Using Input Devices
- Icons and Windows
- File Explorer and Control Panel
- Using a Web Browser
- Exercises / Setting Up the Computer / Exploring the Start Screen / Exploring the Desktop and Taskbar

Installing and Configuring Windows
- Installing Windows
- Completing Setup
- Managing User Accounts
- Exercises / Managing User Accounts

Software Applications
- Installing and Configuring Software
- Managing Software
- Productivity Software
- Collaboration Software
- Specialized Software
- Utility Software
- Virtualization
- Exercises / Managing Software Applications

Troubleshooting and Support
- Support and Troubleshooting
- Getting Support
- Using a Search Engine
- Exercises / Using a Search Engine

Module 2 – Computer Hardware

Input Devices
- Computer Connector Types
- Input Devices
- Installing and Uninstalling Peripherals
- Configuring Peripherals
- Exercises / Configuring an Input Device

Output Devices

- Video Cards
- Display Devices
- Display Connectors and Cable Types
- Display Settings
- Multimedia Ports and Devices
- Exercises / Playing Audio

Storage Devices

- Hard Disk Drives
- Optical Discs and Drives
- Flash Memory
- Exercises / Adding a Removable Drive

File Management

- Managing the File System
- Folders
- Files
- Searching for Folders and Files
- Exercises / File Explorer / Creating, Renaming, and Copying Folders and Files / View Options and Search / Compressing Files / Deleting and Recycling Files

Printers and Scanners

- Printer Types
- Laser Printers
- Inkjet Printers
- Thermal Transfer Printers
- Printer Interfaces
- Installing and Configuring a Printer
- Scanners
- Fax Modems
- Exercises / Using a Printer

System Components

- Selecting a Computer
- Motherboard Components
- Processors
- System Memory
- Expansion Bus
- System Cooling
- Exercises / Specifying PC Systems

Environment and Power

- ESD Precautions
- Device Placement
- Power Supply Units
- Energy Efficiency
- Power Protection
- Safe Disposal and Recycling
- Exercises / Adjusting Power Options

Module 3 – Networks & Security

Setting Up a Network
- Network Components
- TCP/IP
- Setting up a Local Network
- Setting Up a Wireless Network
- Exercises / Network Settings

Sharing and Storage
- Windows Client Software
- Local Sharing and Storage
- Hosted Sharing and Storage
- Backups
- Exercises / Homegroups and File Sharing

Mobile Devices
- Using a Mobile Device
- Mobile Applications and App Stores
- Network Connectivity
- Email Configuration
- Synchronization and Data Transfer
- Bluetooth and NFC

Basic Security Threats
- Computer Security Basics
- Malware
- Preventing Malware Infections
- Patch Management
- Exercises / Using Windows Defender and Windows Update

Security Best Practices
- Spam
- Social Engineering
- Hardware Theft and Device Hardening
- Managing User Authentication
- User Education

Web Browsing Best Practices
- Using Free / Open Networks
- Configuring Web Browser Security
- Managing Plug-ins
- Digital Certificates and Anti-phishing
- Managing Cookies and PII
- Enabling a Firewall
- Exercises / Web Security / Installing a Plug-in

Exam Details

This course is recommended as preparation for the following exam:

- FC0-U61 - CompTIA ITF+ Exam.

CompTIA Network +

Course Code CPNET
Duration 5 days

Overview

This course will teach you the fundamental principles of installing, configuring, and troubleshooting network technologies and help you to progress a career in network administration. It will prepare you to take the CompTIA Network+ exam by providing 100% coverage of the objectives and content examples listed on the syllabus. Study of the course can act as groundwork for more advanced training.

The CompTIA Network+ credential proves knowledge of networking features and functions and is the leading vendor-neutral certification for networking professionals. Worldwide nearly 500,000 individuals are CompTIA Network+ certified and 91% of hiring managers indicate CompTIA certifications are valuable in validating IT employee skills and expertise. Dell, HP, Sharp, Xerox and Ricoh are among the companies that employ Network+ certified staff and it is supported by top organizations, such as Apple, Best Buy, Canon, Cisco, Intel and U.S. Navy.

Audience

CompTIA Network+ is aimed at IT professionals with job roles such as network administrator, network technician, network installer, help desk technician and IT cable installer.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Describe the features of different network protocols and products for LANS, WANS and wireless networks.
- Understand the functions and features of TCP/IP addressing and protocols.
- Identify threats to network resources and appropriate security countermeasures.
- Install and configure network cabling and appliances.
- Manage, monitor and troubleshoot networks.

Pre-Requisites

Attendees should be able to:

- Configure and support PC, laptop, mobile (smartphone / tablet), and print devices.
- Know basic network terminology and functions (such as Ethernet, TCP/IP, switches, routers).
- Configure and manage users, groups, and shared resources in a simple SOHO network.
- Understand the use of basic access control measures, such as authentication, security policy, encryption, and firewalls

Course Contents

Module 1: Topologies and Infrastructure

- Topologies and the OSI Model
- Ethernet
- Hubs, Bridges, and Switches
- Infrastructure and Design

Module 2: Addressing and Routing

- Internet Protocol
- IPv4 Addressing
- DHCP and APIPA
- IPv6 Addressing
- Routing

Module 3: Troubleshooting and Management

- Transport Protocols
- Name Resolution
- Troubleshooting
- Applications and Services
- Management and Monitoring
- Cloud and Virtualization

Module 4: Installation

- Network Sites
- Installing Cable
- Installing Wireless Networks
- WAN Technologies
- Remote Access

Module 5: Security

- Vulnerabilities and Threats
- Security Appliances
- Authentication
- Incident Response
- Change and Configuration Management

Exam Details

This course is recommended as preparation for the following exam:

- CompTIA Network+ exam

CompTIA Pentest +

Course Code CPPENT
Duration 5 days

Overview

As organisations scramble to protect themselves and their customers against privacy or security breaches, the ability to conduct penetration testing is an emerging skill set that is becoming ever more valuable to the organisations seeking protection, and ever more lucrative for those who possess these skills. In this course, you will be introduced to general concepts and methodologies related to pen testing, and you will work your way through a simulated pen test for a fictitious company.

The CompTIA PenTest+ certification requires a candidate to demonstrate the hands-on ability and knowledge to test devices in new environments such as the cloud and mobile, in addition to traditional desktops and servers.
CompTIA PenTest+ joins CompTIA Cybersecurity Analyst (CySA+) at the intermediate-skills level of the cybersecurity career pathway as shown below. Depending on your course of study, PenTest+ and CySA+ can be taken in any order but typically follows the skills learned in Security+. While CySA+ focuses on defense through incident detection and response, PenTest+ focuses on offense through penetration testing and vulnerability assessment.

Although the two exams teach opposing skills, they are dependent on one another. The most qualified cybersecurity professionals have both offensive and defensive skills. Earn the PenTest+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

Audience

Cybersecurity professionals involved in hands-on penetration testing to identify, exploit, report, and manage vulnerabilities on a network.

Learning Objectives

By actively participating in this course, you will learn about the following:

- Explain the importance of planning and key aspects of compliance-based assessments.
- Conduct information gathering exercises with various tools and analyse output and basic scripts (limited to: Bash, Python, Ruby, PowerShell).
- Gather information to prepare for exploitation then perform a vulnerability scan and analyse results.
- Utilise report writing and handling best practices explaining recommended mitigation strategies for discovered vulnerabilities.
- Exploit network, wireless, application, and RF-based vulnerabilities, summarize physical security attacks, and perform post-exploitation techniques.

Pre-Requisites

Attendees should meet the following prerequisites:

- Intermediate knowledge of information security concepts, including but not limited to identity and access management (IAM), cryptographic concepts and implementations, computer networking concepts and implementations, and common security technologies.
- Practical experience in securing various computing environments, including small to medium businesses, as well as enterprise environments.
- CompTIA Network + or CompTIA Security + or equivalent knowledge
- Hands-on information security experience

Recommended prerequisites:

- CPNET – CompTIA Network +
- CPSEC – CompTIA Security +

Course Contents

Planning and Scoping Penetration Tests

- Introduction to Penetration Testing Concepts
- Plan a Pen Test Engagement
- Scope and Negotiate a Pen Test Engagement
- Prepare for a Pen Test Engagement

Conducting Passive Reconnaissance

- Gather Background Information
- Prepare Background Findings for Next Steps

Performing Non-Technical Tests

- Perform Social Engineering Tests
- Perform Physical Security Tests on Facilities

Conducting Active Reconnaissance

- Scan Networks
- Enumerate Targets
- Scan for Vulnerabilities
- Analyse Basic Scripts

Analysing Vulnerabilities

- Analyse Vulnerability Scan Results
- Leverage Information to Prepare for Exploitation

Penetrating Networks

- Exploit Network-Based Vulnerabilities
- Exploit Wireless and RF-Based Vulnerabilities
- Exploit Specialized Systems

Exploiting Host-Based Vulnerabilities

- Exploit Windows-Based Vulnerabilities
- Exploit *Nix-Based Vulnerabilities

Testing Applications

- Exploit Web Application Vulnerabilities
- Test Source Code and Compiled Apps

Completing Post-Exploit Tasks

- Use Lateral Movement Techniques
- Use Persistence Techniques
- Use Anti-Forensics Techniques

Analysing and Reporting Pen Test Results

- Analyse Pen Test Data
- Develop Recommendations for Mitigation Strategies
- Write and Handle Reports
- Conduct Post-Report-Delivery Activities

Appendix A: Mapping Course Content to CompTIA PenTest+ (Exam PT0-001) Solutions Glossary Index

Exam Details

This course is recommended as preparation for the following exam:

- PT0-001 - CompTIA Pentest+ Certification

CompTIA Security +

Course Code CPSEC
Duration 5 days

Overview

The *Security+ Certification Prep Course* provides the basic knowledge needed to plan, implement, and maintain information security in a vendor-neutral format. This includes risk management, host and network security, authentication and access control systems, cryptography, and organizational security. This course maps to the CompTIA Security+ certification exam (SY0-501). Objective coverage is marked throughout the course.
Our Security+ courseware has received the CompTIA Approved Quality Content (CAQC) validation, assuring that all test objectives are covered in the training material.
What is Security+ Certification?

The Security+ certification is considered to be the minimum level of certification for all IT security positions beyond entry-level. This course delivers the core knowledge required to pass the exam and the skills necessary to advance to an intermediate-level security job.

Audience

- Network Administrators
- Cybersecurity Associates
- IT Personnel interested in pursuing a career in cybersecurity

Learning Objectives

By actively participating in this course, you will learn about the following:

- Proactively implement sound security protocols to mitigate security rises.
- Quickly respond to security issues.
- Retroactively identify where security breaches may have occurred.
- Design a network, on-site or in the cloud, with security in mind.

Pre-Requisites

This course assumes basic knowledge of using and maintaining individual workstations.

Attendees should be CompTIA A+ certified (or have equivalent experience) and CompTIA Network+ certified (or have equivalent experience) with 2-3 years networking experience.

Course Contents

Exam Details

This course is recommended as preparation for the following exam:

- SYO-501: CompTIA Security+