CompTIA A+ Core 2 (220-1202) V15 Training (16 Hours)

Course Description

The CompTIA A+ Core 2 (220-1202) V15 course delves into the software, security, and service layers essential for a technician's toolkit. Covering areas such as operating systems, security, software troubleshooting, and operational procedures, the class provides comprehensive training. You will explore the installation and management of Windows, macOS, Linux, and mobile systems, alongside the use of command-line tools. Security concepts are integrated into everyday tasks, focusing on threat mitigation and system hardening. Troubleshooting guidance addresses crashes, malware, and performance issues across various platforms, while operational practices emphasize documentation, change management, backups, safety protocols, scripting, and professional communication. Successfully passing this 90-question exam with a score of 700 out of 900, along with the Core 1 exam, earns the complete CompTIA A+ certification, demonstrating your capability to secure, maintain, and support systems in real-world scenarios.

Audience Profile

This course is appropriate for computer technicians, IT support staff, and help desk professionals with 6 to 12 months of hands-on experience. It will also help prepare professionals seeking CompTIA A+ certification (220-1201/220-1202).

Prerequisites

- Basic end-user skills with Windows-based PCs
- Basic knowledge of computing concepts
- Completion of the CompTIA A+ Core 1 (220-1201) V15 course or equivalent knowledge

Course Outline

Operating Systems

Common operating system types and their purposes
OS installations and upgrades in diverse environments
Microsoft Windows editions features
Microsoft Windows operating system features and tools
Microsoft command-line tools
Microsoft Windows settings configuration
Microsoft Windows networking features on client/desktop
macOS/desktop operating system features and tools
Linux client/desktop operating system features and tools
Application installation according to requirements
Cloud-based productivity tools installation and configuration

Security

- Security measures and purposes
- Microsoft Windows OS security settings configuration
- Wireless security protocols and authentication methods
- Malware types and detection, removal, and prevention tools/methods
- Social engineering attacks, threats, and vulnerabilities
- SOHO malware removal procedures
- Workstation security options and hardening techniques
- Mobile device security methods
- Data destruction and disposal methods
- SOHO wireless and wired network security settings
- Browser security settings configuration

Software Troubleshooting

- Windows OS issues troubleshooting
- Mobile OS and application issues troubleshooting
- Mobile OS and application security issues troubleshooting
- Personal computer security issues troubleshooting

Operational Procedures

- Documentation and support systems information management best practices
- Change management procedures
- Workstation backup and recovery methods
- Common safety procedures
- Environmental impacts and local environment controls
- Prohibited content/activity and privacy, licensing, and policy concepts
- Communication techniques and professionalism
- Scripting basics
- Remote access technologies
- Artificial intelligence basic concepts