CompTIA A+ 220-802

The CompTIA A+ 220-802 examination measures necessary competencies for an entry-level IT professional with the equivalent knowledge of at least 12 months of hands-on experience in the lab or field. Successful candidates will have the knowledge required to assemble components based on customer requirements, install, configure and maintain devices, PCs and software for end users, understand the basics of networking and security/forensics, properly and safely diagnose, resolve and document common hardware and software issues while applying troubleshooting skills. Successful candidates will also provide appropriate customer support; understand the basics of virtualization, desktop imaging, and deployment.

Course Outline

1.0 Operating Systems

1.1 Compare and contrast the features and requirements of various Microsoft Operating Systems.

- Windows XP Home, Windows XP Professional, Windows XP Media Center, Windows XP 64-bit Professional
- Windows Vista Home Basic, Windows Vista Home Premium, Windows Vista Business, Windows Vista Ultimate, Windows Vista Enterprise
- Windows 7 Starter, Windows 7 Home Premium, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise
- Features
- Upgrade paths - differences between in place upgrades, compatibility tools, Windows upgrade OS advisor

1.2 Given a scenario, install, and configure the operating system using the most appropriate method.

- Boot methods
- Type of installations
- Partitioning
- File system types/formatting
- Load alternate third party drivers when necessary
- Workgroup vs. Domain setup
- Time/date/region/language settings
- Driver installation, software and windows updates
- Factory recovery partition

1.3 Given a scenario, use appropriate command line tools.

- Networking
- OS
- Recovery console

1.4 Given a scenario, use appropriate operating system features and tools.

- Administrative
- MSCONFIG
- Task Manager
- Disk management
- Other
- Run line utilities

1.5 Given a scenario, use Control Panel utilities (the items are organized by "classic view/large icons" in Windows).

- Common to all Microsoft Operating Systems
- Unique to Windows XP
- Unique to Vista
- Unique to Windows 7

1.6 Setup and configure Windows networking on a client/desktop.

- HomeGroup, file/print sharing
- WorkGroup vs. domain setup
- Network shares/mapping drives
- Establish networking connections
- Proxy settings
- Remote desktop
- Home vs. Work vs. Public network settings
- Firewall settings
- Configuring an alternative IP address in Windows
- Network card properties

1.7 Perform preventive maintenance procedures using appropriate tools.

- Best practices
- Tools

1.8 Explain the differences among basic OS security settings.

- User and groups
- NTFS vs. Share permissions
- Shared files and folders
- System files and folders
- User authentication

1.9 Explain the basics of client-side virtualization.

- Purpose of virtual machines
- Resource requirements
- Emulator requirements
- Security requirements
- Network requirements
- Hypervisor

2.0 Security

2.1 Apply and use common prevention methods.

- Physical security
- Digital security
- User education
- Principle of least privilege

2.2 Compare and contrast common security threats.

- Social engineering
- Malware
- Rootkits
- Phishing
- Shoulder surfing
- Spyware
- Viruses

2.3 Implement security best practices to secure a workstation.

- Setting strong passwords
- Requiring passwords
- Restricting user permissions
- Changing default user names
- Disabling guest account
- Screensaver required password
- Disable autorun

2.4 Given a scenario, use the appropriate data destruction/disposal method.

- Low level format vs. standard format
- Hard drive sanitation and sanitation methods
- Physical destruction

2.5 Given a scenario, secure a SOHO wireless network.

- Change default user-names and passwords
- Changing SSID
- Setting encryption
- Disabling SSID broadcast
- Enable MAC filtering
- Antenna and access point placement
- Radio power levels
- Assign static IP addresses

2.6 Given a scenario, secure a SOHO wired network.

- Change default usernames and passwords
- Enable MAC filtering
- Assign static IP addresses
- Disabling ports
- Physical security

3.0 Mobile Devices

3.1 Explain the basic features of mobile operating systems.

- Android 4.0.x vs. iOS 5.x

3.2 Establish basic network connectivity and configure email.

- Wireless / cellular data network (enable/disable)
- Bluetooth
- Email configuration
- POP3
- IMAP
- Port and SSL settings

3.3 Compare and contrast methods for securing mobile devices.

- Passcode locks
- Remote wipes
- Locator applications
- Remote backup applications
- Failed login attempts restrictions
- Antivirus
- Patching/OS updates

3.4 Compare and contrast hardware differences in regards to tablets and laptops.

- No field serviceable parts
- Typically not upgradeable
- Touch interface
- Solid state drives

3.5 Execute and configure mobile device synchronization.

- Types of data to synchronize
- Software requirements to install the application on the PC
- Connection types to enable synchronization

4.0 Troubleshooting

4.1 Given a scenario, explain the troubleshooting theory.

- Identify the problem
- Establish a theory of probable cause (question the obvious)
- Test the theory to determine cause
- Establish a plan of action to resolve the problem and implement the solution
- Verify full system functionality and if applicable implement preventive measures
- Document findings, actions and outcomes

4.2 Given a scenario, troubleshoot common problems related to motherboards, RAM, CPU and power with appropriate tools.

- Common symptoms
- Tools

4.3 Given a scenario, troubleshoot hard drives and RAID arrays with appropriate tools.

- Common symptoms
- Tools

4.4 Given a scenario, troubleshoot common video and display issues.

- Common symptoms

4.5 Given a scenario, troubleshoot wired and wireless networks with appropriate tools.

- Common symptoms
- Tools

4.6 Given a scenario, troubleshoot operating system problems with appropriate tools.

- Common symptoms
- Tools

4.7 Given a scenario, troubleshoot common security issues with appropriate tools and best practices.

- Common symptoms
- Tools
- Best practices for malware removal

4.8 Given a scenario, troubleshoot, and repair common laptop issues while adhering to the appropriate procedures.

- Common symptoms
- Disassembling processes for proper re-assembly

4.9 Given a scenario, troubleshoot printers with appropriate tools

- Common symptoms

Tools