CompTIA A+, Network+, and Security+ Course

144 Hours

Course Description
Break into the high pay, high demand field of Information and Network Security with our CompTIA A+, Network+, and Security+ Course. This hands-on bundle is ideal for career changes or those with no experience in IT. The course covers the fundamentals of hardware, software, troubleshooting, operating systems, networking, and security. It prepares the student to take the CompTIA A+ Core 1, A+ Core 2, Network+, and Security+ certification exams.

A+ Core 1
This course will prepare students for the first of the two exams that makes up the CompTIA A+ Core Series. Students will gain the skills and knowledge necessary to perform the following tasks on personal computer hardware and operating systems: installation, PC building, system upgrades, repair, and system configuration.

A+ Core 2
This course will prepare students for the second of the two exams that makes up the CompTIA A+ Core Series. The Core 2 examination is targeted for individuals who work or intend to work in environments where client interaction, client training, operating system, and connectivity issues are emphasized. You will gain the skills and knowledge necessary to perform the following tasks on personal computer hardware and operating systems: system configuration, troubleshooting, problem diagnosis, and preventative maintenance.

Network+
This part of the program is designed as a complete package to prepare students for Network and to provide a strong foundation in PC-based network software and hardware components. Network+ is intended for a student entering into networking, and the logical pathway from A+ Certification.

Security+
CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest-growing fields in IT. CompTIA Security+ is an international, vendor-neutral certification that demonstrates competency in Network Security, Compliance and Operational Security, Threats and Vulnerabilities, Application, Data and Host Security, Access Control and Identity Management Cryptography. This course prepares for the Security+ certification exam SY0-501. Many corporations recommend or require the Security+ certification for their IT employees. Companies like Sun, IBM/Tivoli Software Group, Symantec, Motorola and Olympus Security Group know the value of a Security+ certification and recommend or require it of their IT employees.
## Prerequisites
Basic knowledge of operating systems as in Windows or Linux, computer systems and should be comfortable working with Office applications.

## Course Outline

<table>
<thead>
<tr>
<th>MODULE</th>
<th>TOPICS COVERED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A+ Core 1</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 1: PC Components | • Use Appropriate Safety Procedures  
• PC Components  
• Common Connection Interfaces  
• Install Peripheral Devices  
• Troubleshooting Methodology |
| 2: Display and Multimedia Devices | • Install and Configure Display Devices  
• Troubleshoot Display Devices  
• Install and Configure Multimedia Devices  
• Install and Configure Removable Storage  
• Configure RAID  
• Troubleshoot Storage Devices |
| 3: Storage Devices | • Install System Memory  
• Install and Configure Mass Storage Devices  
• Troubleshoot Internal System Components  
• Configure a Custom PC |
| 4: Internal System Components | • Install and Upgrade CPUs  
• Configure and Update BIOS/UEFI  
• Install Power Supplies  
• Internet Connection Types  
• Network Configuration Concepts  
• Network Services  
• Configure Remote Access  
• Troubleshoot Network Connections  
• Install and Configure IoT Devices  
• Cloud Computing Concepts  
• Troubleshoot Common Laptop Issues  
• Configure Mobile Device Network Connectivity  
• Support Mobile Apps  
• Troubleshoot Print Device Issues  
• Install and Configure Imaging Devices |
| 5: Network Infrastructure Concepts | • Wired Networks  
• Network Hardware Devices  
• Wireless Networks  
• Configure Network Connection Settings  
• Install and Configure SOHO Networks  
• Configure SOHO Network Security |
| 6: Configuring and Troubleshooting Networks | • Configure Client-Side Virtualization  
• Use Laptop Features  
• Install and Configure Laptop Hardware  
• Mobile Device Types  
• Connect and Configure Mobile Device Accessories  
• Maintain Laser Printers  
• Maintain Inkjet Printers  
• Maintain Impact, Thermal, and 3D Printers  
• Install and Configure Printers |
| 7: Client Virtualization and Cloud Computing | • Configure Client-Side Virtualization  
• Use Laptop Features  
• Install and Configure Laptop Hardware  
• Mobile Device Types  
• Connect and Configure Mobile Device Accessories  
• Maintain Laser Printers  
• Maintain Inkjet Printers  
• Maintain Impact, Thermal, and 3D Printers  
• Install and Configure Printers |
| 8: Laptops | • Wired Networks  
• Network Hardware Devices  
• Wireless Networks  
• Configure Network Connection Settings  
• Install and Configure SOHO Networks  
• Configure SOHO Network Security  
• Internet Connection Types  
• Network Configuration Concepts  
• Network Services  
• Configure Remote Access  
• Troubleshoot Network Connections  
• Install and Configure IoT Devices  
• Cloud Computing Concepts  
• Troubleshoot Common Laptop Issues  
• Configure Mobile Device Network Connectivity  
• Support Mobile Apps  
• Troubleshoot Print Device Issues  
• Install and Configure Imaging Devices |
| 9: Mobile Devices | • Wired Networks  
• Network Hardware Devices  
• Wireless Networks  
• Configure Network Connection Settings  
• Install and Configure SOHO Networks  
• Configure SOHO Network Security  
• Internet Connection Types  
• Network Configuration Concepts  
• Network Services  
• Configure Remote Access  
• Troubleshoot Network Connections  
• Install and Configure IoTDevices  
• Cloud Computing Concepts  
• Troubleshoot Common Laptop Issues  
• Configure Mobile Device Network Connectivity  
• Support Mobile Apps  
• Troubleshoot Print Device Issues  
• Install and Configure Imaging Devices |
| 10: Print Devices | • Wired Networks  
• Network Hardware Devices  
• Wireless Networks  
• Configure Network Connection Settings  
• Install and Configure SOHO Networks  
• Configure SOHO Network Security  
• Internet Connection Types  
• Network Configuration Concepts  
• Network Services  
• Configure Remote Access  
• Troubleshoot Network Connections  
• Install and Configure IoT Devices  
• Cloud Computing Concepts  
• Troubleshoot Common Laptop Issues  
• Configure Mobile Device Network Connectivity  
• Support Mobile Apps  
• Troubleshoot Print Device Issues  
• Install and Configure Imaging Devices |
| 1: Supporting Operating Systems | • Identify Common Operating Systems  
• Use Windows Features and Tools  
• Manage Files in Windows  
• Manage Disks in Windows  
• Manage Devices in Windows |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2: Operating Systems          | • Configure and Use Linux  
• Configure and Use macOS  
• Install and Upgrade Operating Systems  
• Maintain OSs |
| 3: Microsoft Windows          | • Install and Manage Windows Applications  
• Manage Windows Performance  
• Troubleshoot Windows |
| 4: Configuring and Troubleshooting Networks | • Configure Network Connection Settings  
• Install and Configure SOHO Networks  
• Configure SOHO Network Security  
• Configure Remote Access  
• Troubleshoot Network Connections |
| 5: Managing Users, Workstations, and Shared Resources | • Manage Users  
• Configure Shared Resources  
• Configure Active Directory Accounts and Policies |
| 6: Security Concepts          | • Logical Security Concepts  
• Threats and Vulnerabilities  
• Physical Security Measures |
| 7: Securing Workstations and Data | • Implement Security Best Practices  
• Implement Data Protection Policies  
• Protect Data During Incident Response |
| 8: Workstation Security Issues | • Detect, Remove, and Prevent Malware  
• Troubleshoot Common Workstation Security Issues  
• Troubleshoot Mobile Device Issues |
| 9: Mobile Devices             | • Secure Mobile Devices |
| 10: Implementing Operational Procedures | • Use Appropriate Safety 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 |

**Network +**

| 1: Network Basics | • Network concepts  
• Network architectures  
• The OSI model |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 2: Wired Computer to Computer Connections | • Wired network connections  
• Network interface cards and modems |
| 3: Network-to-Network Connections | • Network-to-network connection components  
• LAN wiring  
• LAN wiring tests |
<table>
<thead>
<tr>
<th>4: Wired Internetworking Devices</th>
<th>• Basic internetworking devices</th>
<th>• Specialized internetworking devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>5: Wired Communication Standards</td>
<td>• The TCP/IP protocol suite</td>
<td>• DHCP servers</td>
</tr>
<tr>
<td></td>
<td>• TCP/IP</td>
<td></td>
</tr>
<tr>
<td>6: Wireless Networking</td>
<td>• Wireless network devices</td>
<td>• Wireless configuration</td>
</tr>
<tr>
<td></td>
<td>• Wireless networking standards</td>
<td></td>
</tr>
<tr>
<td>7: Security Threats and Mitigation</td>
<td>• Security threats</td>
<td>• Threat mitigation</td>
</tr>
<tr>
<td>8: Security Practices</td>
<td>• Operating systems</td>
<td>• Devices</td>
</tr>
<tr>
<td>9: Network Access Control</td>
<td>• Authentication</td>
<td>• Remote access</td>
</tr>
<tr>
<td></td>
<td>• Public key cryptography</td>
<td>• Wireless security</td>
</tr>
<tr>
<td>10: Monitoring</td>
<td>• Monitoring resources</td>
<td>• Event viewer</td>
</tr>
<tr>
<td>11: Troubleshooting</td>
<td>• Troubleshooting basics</td>
<td>• Troubleshooting scenarios</td>
</tr>
<tr>
<td></td>
<td>• Troubleshooting the network</td>
<td></td>
</tr>
</tbody>
</table>

### Security+

| 1: Risk, Infrastructure, and Connectivity | • Risk Assessment | • Infrastructure and Connectivity |
|                                          | • Developing Policies, Standards, and Guidelines | • Mastering TCP/IP |
|                                          | • Risks Associated with Cloud Computing | • Distinguishing Between Security Topologies |
|                                          | • Understanding Control Types | • IPv4 vs. IPv6 |
|                                          | • Incident Management | • Understanding Remote Access |
| 2: Network Security | • Protecting Networks | • Threats and Vulnerabilities |
|                  | • Monitoring and Diagnosing Networks | • Software Exploitation |
|                  | • Intrusion Detection Systems | • Surviving Malicious Code |
|                  | • Protocol Analyzers | • Calculating Attack Strategies |
|                  | • Securing Workstations | • Recognizing Common Attacks |
| 3: Access Control and Protecting the User | • Access Control Basics | • Classifying Information |
|                                          | • Identity Management | • Complying with Privacy and Security Regulations |
|                                          | • Remote Access Connectivity | • Social Engineering |
|                                          | • Authentication Services | • Types of Social Attacks |
|                                          | • Educating and Protecting the User | |
|                                          | • Security Awareness Training | |
| 4: Application, Cryptography, and Host Security | • Operating Systems and Application Security | • Cryptography Algorithms |
|                                        | • Hardening the Operating System | • Cryptographic Systems |
|                                        | • Working with Data Repositories | • Cryptography Implementations |
|                                        | • Host Security | • Public Key Infrastructure Page 6 of 6 |
|                                        | • Mobile Devices | • Preparing for Cryptographic Attacks |
|                                        | • Cryptography Basics | • Key Life Cycle |
| 5: Physical Security and Network Vulnerabilities | • Physical and Hardware-Based Security | • Secure Network Administration Principals |
|                                         | • Implementing Access Control' | • Mitigation and Deterrent Techniques |
| 6: Data Recovery and Administration | Disaster Recovery and Incident Response  
|                                 | Understanding Business Continuity  
|                                 | Impact Analysis  
|                                 | Reinforcing Vendor Support  
|                                 | Security-Related Policies and Procedures  
|                                 | Security Administration  
|                                 | Administrator’s Troubleshooting Guide  
|                                 | Access Control Issues  
|                                 | Auditing  
|                                 | Authentication Schemes  
|                                 | Back-Up Management  
|                                 | File Sharing Basics  
|                                 | Preventing Common Malicious Events  
| Maintenance and Power Controls  
| Fire Suppression  
| Security and Vulnerability in the Network  
| Security Threats  
| Wireless Networking Security  
| Understanding Mobile Devices  
| Wireless Vulnerabilities |