Cyber Security Specialist

CompTIA A+, Network+ and Security+ Certification Program

147 Hours

Course Description

Break into the high pay, high demand field of Information and Network Security with our Cyber Security Specialist. This hands-on bundle covers the fundamentals of operating systems, hardware and networking and prepares the student to take the CompTIA A+ Essentials, CompTIA A+ Practical Application, CompTIA Network+ exam, and the CompTIA Security+ certification exam.

A+ Essentials
This course will prepare students for the one of the two exams that makes up the IT Technician certification: CompTIA A+ Essentials. 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+ Practical Application
The CompTIA A+ Practical Application 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. This course will prepare you for the second exam that makes up the IT Technician certification: CompTIA A+. 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 as a student path for entering into networking, and the logical stepping-stone to follow 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+ Essentials</strong></td>
<td></td>
</tr>
</tbody>
</table>
| 1: Working with Electricity and Power Systems | - Electricity and electronics  
- Static electricity  
- Power supplies  
- Power conditioning and management |
| 2: Working with CPUs and Motherboards | - Central processing units  
- Packaging, slots, and cooling techniques  
- Motherboards and system cases |
| 3: Working with Basic I/O System | - BIOS and CMOS  
- The POST process  
- Firmware updates |
| 4: Working with Memory Systems | - Memory  
- Memory packaging  
- RAM Installation |
| 5: Working with Bus Structures | - Buses  
- Host system interaction  
- The PCI bus  
- Video buses |
| 6: Working with Expansion Cards | - Drive adapters  
- Video cards  
- Sound cards  
- Internal modems  
- Legacy device installation |
| 7: Understanding Ports, Connectors, and Cables | - Serial and parallel ports, cables, and connectors  
- Keyboards, mice, and pointing devices  
- USB ports, cables, and connectors  
- FireWire ports, cables, and connectors  
- Infrared and Bluetooth wireless ports  
- Multimedia ports, cables, and connectors |
| 8: Understanding Data Storage Devices | - Hard drives  
- Optical drives  
- Removable storage devices  
- Tape drives and backup systems |
| 9: Working with Video and Multimedia I/O Devices | - Cathode ray terminals  
- LCDs and other video technologies  
- Sound input and output devices  
- Scanners and cameras |
| 10: Understanding Printers | - Dot matrix printers  
- Inkjet and related printer technologies  
- Laser printers  
- Other types of printers |
| 11: Understanding Portable Computers and Devices | - Notebook computers  
- Component replacement  
- Handheld computers  
- Portable computer problems |
| 12: Working with Operating System Management | - Directory and file management  
- System management  
- The Registry |

---

Towson University Continuing and Professional Studies  
www.continuingeducation.towson.edu
<table>
<thead>
<tr>
<th>1: Networking Computers</th>
<th>• Addressing</th>
<th>• Client configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>2: Network Troubleshooting</td>
<td>• Troubleshooting basics</td>
<td>• Troubleshooting the network</td>
</tr>
<tr>
<td>3: Portable Computers</td>
<td>• Notebook computers</td>
<td>• Component replacement</td>
</tr>
<tr>
<td></td>
<td>• Configuration</td>
<td>• Notebook issues</td>
</tr>
<tr>
<td>4: Windows Management</td>
<td>• System management</td>
<td>• Resource management</td>
</tr>
<tr>
<td></td>
<td>• Task Scheduler</td>
<td>• Remote management</td>
</tr>
<tr>
<td>5: Windows Monitoring</td>
<td>• Monitoring</td>
<td>• Backup and restore</td>
</tr>
<tr>
<td></td>
<td>• System performance</td>
<td></td>
</tr>
<tr>
<td>6: Operating System Troubleshooting</td>
<td>• Windows startup</td>
<td>• System troubleshooting</td>
</tr>
<tr>
<td>7: Security</td>
<td>• Operating system security</td>
<td>• Common Security threats</td>
</tr>
<tr>
<td></td>
<td>• Windows Encrypted File System</td>
<td>• The human aspects of security</td>
</tr>
<tr>
<td></td>
<td>• Security hardware</td>
<td></td>
</tr>
<tr>
<td>8: Windows Installation and Upgrades</td>
<td>• Windows installation</td>
<td>• Upgrades</td>
</tr>
<tr>
<td>9: Safety and Maintenance</td>
<td>• Safety and hazards</td>
<td>• Safe work practices</td>
</tr>
<tr>
<td></td>
<td>• Computer maintenance</td>
<td>• Disposing of computer equipment</td>
</tr>
</tbody>
</table>

**Network +**

<table>
<thead>
<tr>
<th>1: Network Basics</th>
<th>• Network concepts</th>
<th>• The OSI model</th>
</tr>
</thead>
<tbody>
<tr>
<td>2: Wired Computer to Computer Connections</td>
<td>• Wired network connections</td>
<td>• Network interface cards and modems</td>
</tr>
<tr>
<td>3: Network-to-Network Connections</td>
<td>• Network-to-network connection components</td>
<td>• LAN wiring tests</td>
</tr>
<tr>
<td></td>
<td>• LAN wiring</td>
<td></td>
</tr>
<tr>
<td>4: Wired Internetworking Devices</td>
<td>• Basic internetworking devices</td>
<td>• Specialized internetworking devices</td>
</tr>
<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>
| 1: Risk, Infrastructure, and Connectivity | • Risk Assessment  
• Developing Policies, Standards, and Guidelines  
• Risks Associated with Cloud Computing  
• Understanding Control Types  
• Incident Management | • Infrastructure and Connectivity  
• Mastering TCP/IP  
• Distinguishing Between Security Topologies  
• IPv4 vs. IPv6  
• Understanding Remote Access |
|---|---|---|
| 2: Network Security | • Protecting Networks  
• Monitoring and Diagnosing Networks  
• Intrusion Detection Systems  
• Protocol Analyzers  
• Securing Workstations | • Threats and Vulnerabilities  
• Software Exploitation  
• Surviving Malicious Code  
• Calculating Attack Strategies  
• Recognizing Common Attacks |
| 3: Access Control and Protecting the User | • Access Control Basics  
• Identity Management  
• Remote Access Connectivity  
• Authentication Services  
• Educating and Protecting the User Security Awareness Training | • Classifying Information  
• Complying with Privacy and Security Regulations  
• Social Engineering  
• Types of Social Attacks |
| 4: Application, Cryptography, and Host Security | • Operating Systems and Application Security  
• Hardening the Operating System  
• Working with Data Repositories  
• Host Security  
• Mobile Devices  
• Cryptography Basics | • Cryptography Algorithms  
• Cryptographic Systems  
• Cryptography Implementations  
• Public Key Infrastructure Page 6 of 6  
• Preparing for Cryptographic Attacks  
• Key Life Cycle |
| 5: Physical Security and Network Vulnerabilities | • Physical and Hardware-Based Security  
• Implementing Access Control  
• Maintaining Environmental and Power Controls  
• Fire Suppression  
• Security and Vulnerability in the Network  
• Security Threats | • Secure Network Administration Principals  
• Mitigation and Deterrant Techniques  
• Wireless Networking Security  
• Understanding Mobile Devices  
• Wireless Vulnerabilities |
| 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 |