



School of Continuing Studies

Tyler Junior College
1530 SSW LOOP 323, Tyler, Texas 75701
www.tjc.edu/continuingstudies/mycaa
Contact: Judie Bower | (800) 298-5226 | jbower@tjc.edu

Education & Training Plan

Computer Security Technician (CompTIA Security+ and Network+) Certification Program with Externship

Student Full Name: _____

Start Date: _____ End Date: _____

Program includes National Certification & an Externship Opportunity
Mentor Supported

Tyler Junior College Program with Externship

Course Code:	TJC-IT-CSTSN
Program Duration:	6 Months
Course Contact Hours:	375
Student Tuition:	\$3,999.00

Computer Security Technician (CompTIA Security+ and Network+)

The Computer Security Technician CompTIA Security+ program is designed to prepare students to function as computer professionals in multiple technical, business, and healthcare settings. Sec+ technicians serve many technical support and IT operation roles with job titles such Systems Administrator, Security Administrator, Junior IT/Auditor, Penetration Tester, and Security Consultant as well as Network Field Technician, Help Desk Technician, and Network Support Specialist.

Computer Security Technician (CompTIA Security+ and Network+) Program

The Computer Security Technician CompTIA Security+ Program is to prepare students to support the IT infrastructure through installing and configuring systems to secure applications, networks, and devices as well as perform threat analysis and respond with appropriate mitigation techniques. It also prepares students to learn to manage, maintain, troubleshoot, install, operate, and configure basic network infrastructure as well as describe networking technologies, understand basic design principles, adhere to wiring standards, and use testing tools.

Education and National Certifications

- Students should have or be pursuing a high school diploma or GED.

- Students who complete this program can sit for the following exams:
 - **CompTIA Security+ Certification (Exam SY0-601)**
 - **CompTIA Network+ Certification (Exam N10-008)**

Program Objectives

- Fundamental networking concepts, such as protocol reference models, network devices and theory, network topologies, and network services
- WAN technologies including ISDN, Frame Relay, PPP, MPLS, Metro-Ethernet, and more
- How to work with different network cables and connectors
- Network design considerations
- Switch and wireless LAN configuration
- IPv4 and IPv6 addressing
- Routing fundamentals including RIP, OSPF, IS-IS, and BGP routing protocols; HSRP and VRRP; route aggregation; and routing metrics
- Unified communications, Voice over IP (VoIP), video, and QoS
- Virtualized devices, storage area network technologies (SAN), and cloud technologies
- Network security attacks, vulnerabilities, policies, defenses, and counter-measures
- Network monitoring tools and analysis, configuration management, and best practices
- Network troubleshooting
- Detect various types of compromise and have an understanding of penetration testing and vulnerability scanning concepts
- Install, configure, and deploy network components while assessing and troubleshooting issues to support organizational security
- Implement secure network architecture concepts and systems design
- Install and configure identity and access services, as well as management controls
- Implement and summarize risk management best practices and the business impact
- Install and configure wireless security settings and implement public key infrastructure
- Be familiar with every objective on the CompTIA Security+ Exam
- Employ tips to prepare for and pass the exam

National Certification

Students who complete the Tyler Junior College Computer Security Technician (CompTIA Security+ and Network+) program will be prepared to sit for the CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-008) national certification exam(s). In order to work as a Computer Security Technician (CompTIA Security+ and Network+), many states nationwide are requiring that learners achieve national certification prior to working in that state. Students who complete this program are encouraged to complete the practical/clinical externship option with their program. This comprehensive program is designed to prepare students to sit for CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-008) exam(s). Students who complete this program can and do sit for the CompTIA Security+ Certification (Exam SY0-601) and CompTIA Network+ Certification (Exam N10-008) national certification exam(s) and are qualified, eligible and prepared to do so.

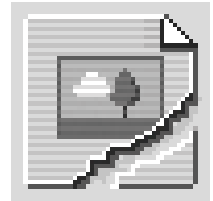
Externship / Hands on Training / Practicum

Although not a requirement, once students complete the program, they have the ability to participate in an externship and/or hands on practicum so as to practice the skills necessary to perform the job requirements of

a professional in this field. Students will be assisted with completing a resume and/or other requirements necessary to work in this field. All students who complete this program are eligible to participate in an externship and will be placed with a participating organization near their location. The institution works with national organizations and has the ability to place students in externship opportunities nationwide.

Tyler Junior College contact: If students have any questions regarding this program including national certification and externships , **they should call Judie Bower of Tyler Junior College at | (800) 298-5226 or via email at jbower@tjc.edu**

Note : No refunds can be issued after the start date published in your Financial Award document.



About Tyler Junior College!

Welcome to Tyler Junior College! One of the oldest junior colleges in Texas, the College was established in 1926 with a mission of providing the finest academic education for freshmen and sophomore students. Tyler Junior College remains committed to that goal while also recognizing the changing role of community colleges and the need to provide quality training for technical fields. There are several unique aspects of the healthcare career programs available to students through the School of Continuing Studies at Tyler Junior College (TJC). In addition to enrollment of over 32,000 students annually, Tyler Junior College (TJC) has been the Texas leader in healthcare technician training and education programs for over 12 years. Over the last 12 years, approximately 13,000 students have successfully completed TJC's Pharmacy Technician, Dental Assisting, Medical Billing & Coding, Clinical Medical Assistant and other healthcare programs.

www.tjc.edu/continuingstudies/mycaa



Tyler Junior College and Pearson Education

Tyler Junior College's eLearning programs were developed in partnership with Pearson Education to produce the highest quality, best-in-class content and delivery necessary to enhance the overall student learning experience, boost understanding and ensure retention. Pearson Education is the premier content and learning company in North America offering solutions to the higher education and career training divisions of colleges and universities across the country aimed at driving quality education programs to ensure student success. Please visit us at www.pearson.com.

About Pearson Education

Welcome to Pearson. We have a simple mission: to help people make more of their lives through learning. We are the world's leading learning company, with 40,000 employees in more than 80 countries helping people of all ages to make measurable progress in their lives. We provide a range of education products and services to institutions, governments and direct to individual learners, that help people everywhere aim higher and fulfil their true potential. Our commitment to them requires a holistic approach to education. It begins by using research to understand what sort of learning works best, it continues by bringing together people and organizations to develop ideas, and it comes back round by measuring the outcomes of our products.

Computer Security Technician (CompTIA Security+ and Network+) Program Detailed Student Objectives:

COMPTIA NETWORK+ MODULE

The OSI Model and Encapsulation

- The Purpose of Reference Models
- The OSI Model
- The TCP/IP Stack
- Real-World Case Study

Network Topologies and Types

- Defining a Network
- Network Types and Characteristics
- Networks Defined Based on Resource Location
- Networks Defined by Topology
- Virtual Network Concepts
- Provider Links
- Real-World Case Study

Network Media Types

- Copper and Fiber Media and Connectors
- Unshielded Twisted Pair
- Plenum Versus Nonplenum Cable
- Multiplexing in Fiber-Optic Networks
- Cable Management
- Real-World Case Study

IP Addressing

- Binary Numbering
- IPv4 Addressing
- Assigning IPv4 Addresses
- Subnetting
- Address Translation
- IP Version 6
- Real-World Case Study

Common Ports and Protocols

- Ports and Protocols
- IP Protocol Types

Network Services

- DHCP
- DNS
- NTP

Corporate and Datacenter Architectures

- The Three-Tiered Network Architecture
- Software-Defined Networking
- Storage Area Networks
- Deciding on an Architecture

Cloud Concepts

- Deployment Models
- Service Models
- Key Cloud Concepts

Various Network Devices

- Networking Devices
- Networked Devices

Routing Technologies and Bandwidth Management

- Routing
- Sources of Routing Information
- Routing Protocol Characteristics
- Routing Protocol Examples
- Bandwidth Management

Ethernet Switching

- Principles of Ethernet
- Ethernet Switch Features

Wireless Standards

- Introducing Wireless LANs
- Deploying Wireless LANs
- Securing Wireless LANs

Ensure Network Availability

- Monitoring Tools
- Additional Monitoring Topics

Organizational Documents and Policies

- Plans and Policies
- Hardening and Security Policies
- Common Documentation

High Availability and Disaster Recovery

- High Availability
- Real-World Case Study: SOHO Network Design

Common Security Concepts

- Core Security Concepts
- Authentication Methods
- Risk Management and SIEM

Common Types of Attacks

- Technology-Based Attacks
- Human and Environmental Attacks
- Other Miscellaneous Attacks

Network Hardening Techniques

- Best Practices
- Wireless Security and IoT Considerations

Remote Access Methods

- Virtual Private Networks (VPNs)
- Other Remote Access Technologies
- Authentication and Authorization Considerations
- In-Band vs. Out-of-Band Management

Physical Security

- Detection Methods
- Prevention Methods
- Asset Disposal

A Network Troubleshooting Methodology

- Troubleshooting Basics

Troubleshoot Common Cabling Problems

- Specifications and Limitations
- Cable Considerations and Applications
- Common Issues
- Common Tools

Network Software Tools and Commands

- Software Tools
- Command Line Tools
- Basic Network Platform Commands

Troubleshoot Common Wireless Issues

- Specifications and Limitations
- Considerations
- Common Issues
- Wireless Network Troubleshooting

Troubleshoot General Network Issues

- Considerations for General Network Troubleshooting
- Common Issues

COMPTIA SECURITY+ MODULE

COMPARING SECURITY ROLES AND SECURITY CONTROLS

- Compare and Contrast Information Security Roles
- Compare and Contrast Security Control and Framework Types

EXPLAINING THREAT ACTORS AND THREAT INTELLIGENCE

- Explain Threat Actor Types and Attack Vectors
- Explain Threat Intelligence Sources

PERFORMING SECURITY ASSESSMENTS

- Assess Organizational Security with Network Reconnaissance Tools
- Explain Security Concerns with General Vulnerability Types
- Summarize Vulnerability Scanning Techniques
- Explain Penetration Testing Concepts

IDENTIFYING SOCIAL ENGINEERING AND MALWARE

- Compare and Contrast Social Engineering Techniques
- Analyze Indicators of Malware-Based Attacks

SUMMARIZING BASIC CRYPTOGRAPHIC CONCEPTS

- Compare and Contrast Cryptographic Cipher
- Summarize Cryptographic Modes of Operation
- Summarize Cryptographic Use Cases and Weaknesses
- Summarize Other Cryptographic Technologies

IMPLEMENTING PUBLIC KEY INFRASTRUCTURE

- Implement Certificates and Certificate Authorities
- Implement PKI Management

IMPLEMENTING AUTHENTICATION CONTROLS

- Summarize Authentication Design Concepts
- Implement Knowledge-Based Authentication
- Implement Authentication Technologies
- Summarize Biometrics Authentication Concepts

IMPLEMENTING IDENTITY AND ACCOUNT MANAGEMENT CONTROLS

- Implement Identity and Account Types
- Implement Account Policies
- Implement Authorization Solutions
- Explain the Importance of Personnel Policies

IMPLEMENTING SECURE NETWORK DESIGNS

- Implement Secure Network Designs
- Implement Secure Switching and Routing
- Implement Secure Wireless Infrastructure
- Implement Load Balancers

IMPLEMENTING NETWORK SECURITY APPLIANCES

- Implement Firewalls and Proxy Servers
- Implement Network Security Monitoring
- Summarize the Use of SIEM

IMPLEMENTING SECURE NETWORK PROTOCOLS

- Implement Secure Network Operations Protocols
- Implement Secure Application Protocols
- Implement Secure Remote Access Protocols

IMPLEMENTING HOST SECURITY SOLUTIONS

- Implement Secure Firmware
- Implement Endpoint Security
- Explain Embedded System Security Implications

IMPLEMENTING SECURE MOBILE SOLUTIONS

- Implement Mobile Device Management
- Implement Secure Mobile Device Connections

SUMMARIZING SECURE APPLICATION CONCEPTS

- Analyze Indicators of Application Attacks
- Analyze Indicators of Web Application Attacks
- Summarize Secure Coding Practices
- Implement Secure Script Environments
- Summarize Deployment and Automation Concepts

IMPLEMENTING SECURE CLOUD SOLUTIONS

- Summarize Secure Cloud and Virtualization Services
- Apply Cloud Security Solutions
- Summarize Infrastructure as Code Concepts

EXPLAINING DATA PRIVACY AND PROTECTION CONCEPTS

- Explain Privacy and Data Sensitivity Concepts
- Explain Privacy and Data Protection Controls

PERFORMING INCIDENT RESPONSE

- Summarize Incident Response Procedures
- Utilize Appropriate Data Sources for Incident Response
- Apply Mitigation Controls

EXPLAINING DIGITAL FORENSICS

- Explain Key Aspects of Digital Forensics Documentation
- Explain Key Aspects of Digital Forensics Evidence Acquisition

SUMMARIZING RISK MANAGEMENT CONCEPTS

- Explain Risk Management Processes and Concepts
- Explain Business Impact Analysis Concepts

IMPLEMENTING CYBERSECURITY RESILIENCE

- Implement Redundancy Strategies
- Implement Backup Strategies
- Implement Cybersecurity Resiliency Strategies

EXPLAINING PHYSICAL SECURITY

- Explain the Importance of Physical Site Security Controls
- Explain the Importance of Physical Host Security Controls

ACING YOUR EXAM

- Understanding the Security+ Exam Structure
- Test Taking Strategies
- The Week Leading Up to Your Exam
- What to Expect at the Testing Center
- Attaining and Maintaining Your Security+ Certification

Note: This program can be completed in 6 months. However, students will have online access to this program for a 24-month period.

MICROSOFT OFFICE

- Module Use an integrated software package, specifically the applications included in the Microsoft Office suite
- Demonstrate marketable skills for enhanced employment opportunities
- Describe proper computer techniques for designing and producing various types of documents
- Demonstrate the common commands & techniques used in Windows desktop
- List the meaning of basic PC acronyms like MHz, MB, KB, HD and RAM
- Use WordPad and MSWord to create various types of documents
- Create headings and titles with Word Art
- Create and format spreadsheets, including the use of mathematical formulas
- Demonstrate a working knowledge of computer database functions, including putting, processing, querying and outputting data
- Define computer terminology in definition matching quizzes
- Use the Windows Paint program to alter graphics
- Use a presentation application to create a presentation with both text and graphics
- Copy data from one MS Office application to another application in the suite
- Use e-mail and the Internet to send Word and Excel file attachments
- Demonstrate how to use the Windows Taskbar and Windows Tooltips
- Explain how copyright laws pertain to data and graphics posted on the Internet
- Take the college computer competency test after course completion
- Follow oral and written directions and complete assignments when working under time limitations

Note: Although the Microsoft Office Module is not required to successfully complete this program, students interested in pursuing free Microsoft MOS certification may want to consider completing this Microsoft Office Module at no additional cost.

System Requirements:

Windows Users:

- Windows 8, 7, XP or Vista
- 56K modem or higher
- Soundcard & Speakers
- Firefox, Chrome or Microsoft Internet Explorer

Mac OS User:

- Mac OS X or higher (in classic mode)
- 56K modem or higher
- Soundcard & Speakers
- Apple Safari

iPad Users:

- Due to Flash limitations, eLearning programs are NOT compatible with iPads

Screen Resolution:

- We recommend setting your screen resolution to 1024 x 768 pixels.

Browser Requirements:

- System will support the two latest releases of each browser. When using older versions of a browser, users risk running into problems with the course software.
- Windows Users: Mozilla Firefox, Google Chrome, Microsoft Internet Explorer
- Mac OS Users: Safari, Google Chrome, Mozilla Firefox

Suggested Plug-ins:

- Flash Player
- Real Player
- Adobe Reader
- Java