



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

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.

- There are several National Certification exams that are available to students who successfully complete this program:
 - **CompTIA Security+ Certification (Exam SY0-501)**
 - **CompTIA Network+ Certification (Exam N10-007)**

Program Objectives

- Designing, implementing, configuring, managing, and maintaining networks and network devices
- Troubleshooting network problems
- Identifying strategies developed by cyber adversaries to attack networks and hosts and the countermeasures deployed to defend against them
- Applying the principles of organizational security and the elements of effective security policies
- Applying the technologies and uses of cryptographic standards and products
- Installing and configuring network- and host-based security technologies
- Enforcing wireless and remote access security
- Applying the standards and products used to enforce security on web and communications technologies
- Implementing strategies for ensuring business continuity, fault tolerance, and disaster recovery
- Identifying application and coding vulnerabilities and the development and deployment methods designed to mitigate them
- Communicating effectively and professionally

National Certification

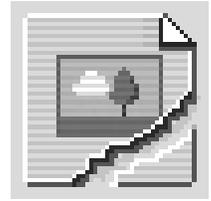
Students who complete the Tyler Junior College Computer Security Technician (CompTIA Security+ and Network+) program will be prepared to sit for the CompTIA Security+ Certification (Exam SY0-501) or CompTIA Network+ Certification (Exam N10-007) national certification exam(s). In order to work as a Computer 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 SY0-501) or CompTIA Network+ Certification (Exam N10-007) exam(s). Students who complete this program can and do sit for the CompTIA Security+ Certification (Exam SY0-501) or CompTIA Network+ Certification (Exam N10-007) 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 jbow@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:

TOPOLOGIES, THE OSI MODEL, AND ETHERNET

- Explain devices, applications, protocols, and services at their appropriate OSI layers
- Explain the concepts and characteristics of routing and switching
- Compare and contrast the characteristics of network topologies, types, and technologies
- Deploy the appropriate cabling solution

HUBS, BRIDGES, AND SWITCHES

- Explain the concepts and characteristics of routing and switching
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them
- Explain common mitigation techniques and their purposes

INFRASTRUCTURE AND DESIGN, POLICIES AND BEST PRACTICES

- Explain the concepts and characteristics of routing and switching
- Compare and contrast the characteristics of network topologies, types, and technologies
- Identify policies and best practices

INTERNET PROTOCOL AND IP ADDRESSING

- Explain the purposes and uses of ports and protocols
- Configure the appropriate IP addressing components
- Explain the concepts and characteristics of routing and switching

DHCP AND APIPA

- Explain the purposes and uses of ports and protocols
- Given a scenario, configure the appropriate IP addressing components
- Explain the functions of network services

ROUTING

- Explain the concepts and characteristics of routing and switching
- Configure the appropriate IP addressing components
- Determine the appropriate placement of networking devices on a network and install/configure them

TCP AND UDP

- Explain the purposes and uses of ports and protocols
- Explain common scanning, monitoring, and patching processes and summarize their expected outputs

NAME RESOLUTION

- Explain the purposes and uses of ports and protocols
- Explain the functions of network services

MONITORING, SCANNING, AND NETWORK TROUBLESHOOTING

- Explain the purposes and uses of ports and protocols
- Explain common scanning, monitoring, and patching processes and summarize their expected outputs
- Implement network device hardening
- Explain the network troubleshooting methodology
- Troubleshoot common wired connectivity and performance issues
- Troubleshoot common network service issues

APPLICATIONS AND SERVICES, VIRTUALIZATION, SAN, AND CLOUD SERVICES

- Explain the purposes and uses of ports and protocols
- Explain the concepts and characteristics of routing and switching
- Explain the functions of network services
- Determine the appropriate placement of networking devices on a network and install/configure them
- Explain the purposes and use cases for advanced networking devices
- Troubleshoot common wired connectivity and performance issues
- Troubleshoot common network service issues
- Summarize cloud concepts and their purposes
- Explain the purposes of virtualization and network storage technologies

NETWORK SECURITY DESIGN AND APPLIANCES

- Implement network device hardening
- Explain common mitigation techniques and their purposes
- Troubleshoot common wired connectivity and performance issues
- Explain the purposes and use cases for advanced networking devices
- Summarize common network attacks
- Troubleshoot common network service issues

AUTHENTICATION, ENDPOINT SECURITY, AND NETWORK SITE MANAGEMENT

- Explain the purposes and uses of ports and protocols
- Explain the purposes and use cases for advanced networking devices
- Explain authentication and access controls
- Summarize common networking attacks
- Explain common mitigation techniques and their purposes
- Deploy the appropriate cabling solution
- Use appropriate documentation and diagrams to manage the network
- Compare and contrast business continuity and disaster recovery concepts
- Summarize the purposes of physical security devices

INSTALLING CABLED NETWORKS

- Given a scenario, deploy the appropriate cabling solution
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them
- Troubleshoot common wired connectivity and performance issues

INSTALLING WIRELESS NETWORKS

- Compare and contrast the characteristics of network topologies, types, and technologies

- Given a scenario, implement the appropriate wireless technologies and configurations
- Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them
- Explain the purposes and use cases for advanced networking devices
- Given a scenario, secure a basic wireless network
- Summarize common networking attacks
- Troubleshoot common wireless connectivity and performance issues

INSTALLING WAN LINKS

- Explain the concepts and characteristics of routing and switching
- Compare and contrast the characteristics of network topologies, types, and technologies
- Implement the appropriate wireless technologies and configurations
- Determine the appropriate placement of networking devices on a network and install/configure them
- Compare and contrast WAN technologies

CONFIGURING REMOTE ACCESS

- Explain the purposes and uses of ports and protocols
- Explain the purposes and use cases for advanced networking devices
- Compare and contrast WAN technologies

INDICATORS OF COMPROMISE

- Analyze indicators of compromise and determine the type of malware
- Compare and contrast types of attacks
- Explain threat actor types and attributes
- Troubleshoot common security issues

CRITICAL SECURITY CONTROLS AND SECURITY POSTURE ASSESSMENT TOOLS

- Explain penetration testing concepts
- Explain vulnerability scanning concepts
- Use appropriate software tools to assess the security posture of an organization
- Explain use cases and purpose for frameworks, best practices, and secure configuration guides
- Explain risk management processes and concepts
- Compare and contrast various types of controls
- Use appropriate software tools to assess the security posture of an organization

INCIDENT RESPONSE

- Follow incident response procedure

CRYPTOGRAPHY

- Compare and contrast types of attacks
- Explain the impact associated with types of vulnerabilities
- Compare and contrast basic concepts of cryptography
- Explain cryptography algorithms and their basic characteristics

PUBLIC KEY INFRASTRUCTURE

- Explain the impact associated with types of vulnerabilities
- Install and configure network components, both hardware- and software-based, to support organizational security
- Explain cryptography algorithms and their basic characteristics
- Implement public key infrastructure

IDENTIFICATION AND AUTHENTICATION

- Compare and contrast types of attacks
- Given a scenario, use appropriate software tools to assess the security posture of an organization
- Troubleshoot common security issues
- Compare and contrast identity and access management concepts
- Install and configure identity and access services
- Implement identity and access management controls
- Compare and contrast basic concepts of cryptography
- Explain cryptography algorithms and their basic characteristics

IDENTITY AND ACCESS SERVICES AND ACCOUNT MANAGEMENT

- Implement secure protocols
- Compare and contrast identity and access management concepts
- Install and configure identity and access services
- Explain the impact associated with types of vulnerabilities
- Differentiate common account management practices

SECURE NETWORK DESIGN

- Compare and contrast types of attacks
- Explain the impact associated with types of vulnerabilities
- Install and configure network components, both hardware- and software-based, to support organizational security
- Implement secure network architecture concepts

FIREWALLS, LOAD BALANCERS, IDS, AND SIEM

- Analyze and interpret output from security technologies

SECURE WIRELESS ACCESS AND PHYSICAL SECURITY CONTROLS

- Install and configure network components, both hardware- and software-based, to support organizational security
- Troubleshoot common security issues
- Analyze and interpret output from security technologies
- Implement secure network architecture concepts
- Compare and contrast types of attacks
- Install and configure wireless security settings
- Explain the importance of physical security controls

SECURE PROTOCOLS, SERVICES, AND REMOTE ACCESS

- Compare and contrast types of attacks
- Explain the impact associated with types of vulnerabilities
- Install and configure network components, both hardware- and software-based, to support organizational security
- Implement secure protocols
- Implement secure network architecture concepts

SECURE SYSTEMS DESIGN

- Explain the impact associated with types of vulnerabilities
- Troubleshoot common security issues
- Analyze and interpret output from security technologies
- Given a scenario, implement secure systems design
- Explain the security implications of embedded systems

SECURE MOBILE DEVICE SERVICES, VIRTUALIZATION, AND CLOUD SERVICES

- Given a scenario, deploy mobile devices securely
- Explain the impact associated with types of vulnerabilities
- Summarize cloud and virtualization concepts

FORENSICS

- Summarize basic concepts of forensics

DISASTER RECOVERY, RESILIENCY, AND RISK MANAGEMENT

- Explain the impact associated with types of vulnerabilities
- Use appropriate software tools to assess the security posture of an organization
- Explain how resiliency and automation strategies reduce risk
- Explain disaster recovery and continuity of operation concepts
- Troubleshoot common security issues
- Summarize business impact analysis concepts
- Explain risk management processes and concepts

SECURE APPLICATION DEVELOPMENT AND ORGANIZATIONAL SECURITY

- Compare and contrast types of attacks
- Explain the impact associated with types of vulnerabilities
- Explain the importance of secure staging deployment concepts
- Summarize secure application development and deployment concepts
- Given a scenario, use appropriate software tools to assess the security posture of an organization
- Explain the importance of policies, plans, and procedures related to organizational security
- Carry out data security and privacy practices

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