HYBRID TECHNOLOGY TRAINING
PRINCE GEORGES COMMUNITY COLLEGE

Prince George's Community College (PGCC)

Security+ Course

CompTIA SY0-401
Security+ Pro Certifications Exams

STUDENT WORKBOOK

Prince George's Community College Mission Statement

Prince George's Community College transforms students' lives. The colleges exist to educate, train, and serve our diverse populations through accessible, affordable and rigorous learning experiences.

Information Technology Entry Program Objective

The Hybrid Technology Training Program (HTT) is a comprehensive multi-phase program of Prince George's Community College that develops the skills needed to enter the demanding world of IT Support. Upon successful completion of the program, the student will be able to demonstrate practical knowledge and application of their skills, exceeding that of an Entry Level Desktop and Network IT Support Technician or Tier I Help Desk Support.

Through our comprehensive approach, the material is combined into an interconnected program, allowing the instructor and student adequate time on a specific subject such as: TCP/IP, DNS, DHCP, Wireless, IPv6 or troubleshooting.

Each student is treated and trained as an information technology support professional from day one. The student will design, build, administer and maintain a live network during the program. We can do this through the delivery method of the combined and interconnected nature of this dynamic multi-phase program.

Upon completion of the Information Technology Entry Program, and with adequate preparation in addition to the contact hours, the student should have developed the skills needed to sit for the following exams: CompTIA A+ SYS-401 and Security+ Pro certifications.

CompTIA Security + Objective

In this course students will be given knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.

The CompTIA Security+ Certification course is to provide students with the most comprehensive accelerated learning environment for the Security+ (SY0-401) exam. Our instructors have a total commitment to the exam objectives of the Security+, and will teach you vital tips and tricks needed to pass the exam. The Security+ teaches you information security theory, as well as reinforces theory with hands-on exercises that help you "learn by doing". It provides an excellent foundation for IT professionals whether they want to find a job in network security, or train for more advanced security certifications such as CISSP.

HOW TO USE THIS INSTRUCTOR GUIDE

The instructor's guide provides instructors with an overview of the topic that should be covered for a student to successfully complete and pass CompTIA Security+ SY0-401 and Security+ Pro Certifications.

The Instructor's Guide is intended to be used in conjunction with the Course Syllabus and Course Schedule documents. All electronic copies of all three documents are posted in the "Syllabus & Schedule" area of the Blackboard course site for this course.

Throughout this course, instructors should gauge student success and adjust accordingly.

The Table of Contents below provides links to all of the pertinent information found in this document.

Let's get started!

TABLE OF CONTENTS

SECTION 1: COURSE INFORMATION

Course Description

In this course students will be given knowledge and skills required to identify risk, to participate in risk mitigation activities, and to provide infrastructure, application, information, and operational security. In addition, the successful candidate will apply security controls to maintain confidentiality, integrity, and availability, identify appropriate technologies and products, troubleshoot security events and incidents, and operate with an awareness of applicable policies, laws, and regulations.

Required Textbook **Book:**

CompTIA Security+ Certification, 3th Edition (Exam SY0-401)
ISBN 978-0-07-178922-7
Publisher: Pearson
Authors: Kirk Hausman, Martin Weiss, Diane Barrett

Other Required Course Materials **Online Labs:**

An introductory course in a Windows operating system and TCPIP, or equivalent skills and knowledge, is required. Such as: *Windows 7* or Windows 8.1
CompTIA Network+ certifications, or the equivalent skills and knowledge,

Online Labs:

NetLab
Testout Lab Simulations

Required Technology Accounts

To be successful in this course, students must have access to the following technology accounts:

- Owl Mail Email Account
- Blackboard Account
- Testout Account
- NetLab Account
- Testout Account
- eLearning Account

Details on how to setup and access the technology accounts for this course can be found in the Course Technology Setup section of this document.

Prerequisites

The prerequisites for this course are: CompTIA A+ Certification, Strong Fundamental Network Foundation.

Course Meeting Schedule

This course will meet on the PGCC Largo campus Monday through Friday. The class meeting times and room location for this course can be found on the Course Syllabus document found in the Syllabus & Schedule area of the Blackboard course site.

Course Length
This course meets for 9 days.

Course Contact Hours
The total number of contact hours for this course is: 72 Hours

Course Structure
This course is designed to provide a hybrid experience, including a blend of face-to-face and online activities.

Face-to-face sessions will be held on the Largo campus (location TBD). Face-to-face activities will consist of Lecture and online labs.

Online sessions will be a blend of self-paced and group activities using Blackboard, Testout, and NetLab. The instructor may add supplemental online activities as needed.

Technology Requirements
Computer/internet access and mastery of basic computer skills are considered to be the student's responsibility. To be successful in this course, students must have access to:

- Blackboard
- NetLab (http://netlab5.pgcc.edu/)
  - Students must have Java Installed.
  - a Pentium-class or Mac computer with at least 256 MB RAM
  - Broadband (DSL, Cable, FIOS) is highly recommended
  - An Internet Service Provider (ISP)
  - Your PGCC Owl Mail student email address
  - Firefox version 22 (or higher), Chrome version 30 (or higher), or Internet Explorer 8 (or higher)
  - Microsoft Word (word processing software)
  - Video player and speakers for multimedia content

SECTION 2: COURSE OBJECTIVES

The below outcomes are the CompTIA Security+ exam objectives.
Source: http://certification.comptia.org/getCertified/certifications/security.aspx

Students, upon completion of this course, should be able to show proficiency and /or knowledge in the following areas:

Security+

Network Security

- Implement security configuration parameters on network devices and other technologies
- Given a scenario, use secure network administration principles
- Explain network design elements and components
- Given a scenario, implement common protocols and services
- Given a scenario, troubleshoot security issues related to wireless networking

Compliance and Operational Security

- Explain the importance of risk related concepts
- Summarize the security implications of integrating systems and data with third parties
- Given a scenario, implement appropriate risk mitigation strategies
- Given a scenario, implement basic forensic procedures
- Summarize common incident response procedures
- Explain the importance of security related awareness and training
- Compare and contrast physical security and environmental controls
- Summarize risk management best practices
- Given a scenario, select the appropriate control to meet the goals of security

Threats and Vulnerabilities

- Explain types of malware
- Summarize various types of attacks
- Summarize social engineering attacks and the associated effectiveness with each attack
- Explain types of wireless attacks
- Explain types of application attacks
- Analyze a scenario and select the appropriate type of mitigation and deterrent techniques
- Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
- Explain the proper use of penetration testing versus vulnerability

Application, Data and Host Security

- Explain the importance of application security controls and techniques
- Summarize mobile security concepts and technologies
- Given a scenario, select the appropriate solution to establish host security
- Implement the appropriate controls to ensure data security

- Compare and contrast alternative methods to mitigate security risks in static environments.

Access Control and Identity Management

- Compare and contrast the function and purpose of authentication services
- Given a scenario, select the appropriate authentication, authorization or access control
- Install and configure security controls when performing account management, based on best practices

Cryptography

- Given a scenario, utilize general cryptography concepts
- Given a scenario, use appropriate cryptographic methods
- Given a scenario, use appropriate PKI, certificate management and associated components

SECTION 3: COURSE SCHEDULE

Module	Module Name	Course Objective(s) Covered	# Hours
Day 1			
1.1	Implement security configuration parameters on network devices and other technologies.	Network Security	1.5 hours
1.2	Given a scenario, use secure network administration principles.	Network Security	1.5 hours
1.3	Explain network design elements and components.	Network Security	1.5 hours
1.4	Given a scenario, implement common protocols and services.	Network Security	2 hours
Day 2			
1.5	Given a scenario, troubleshoot security issues related to wireless networking.	Network Security	1.5 hours
2.1	Explain the importance of risk related concepts.	Compliance and Operational Security	2 hours
2.2	Summarize the security implications of integrating systems and data with third parties.	Compliance and Operational Security	1.5 hours
2.3	Given a scenario, implement appropriate risk mitigation strategies.	Compliance and Operational Security	2.5 hours
Day 3			
2.4	Given a scenario, implement basic forensic procedures.	Compliance and Operational Security	1.5 hours
2.5	Summarize common incident response procedures.	Compliance and Operational Security	2 hours
2.6	Explain the importance of security related awareness and training.	Compliance and Operational Security	2 hours
2.7	Compare and contrast physical security and environmental controls.	Compliance and Operational Security	2 hours
Day 4			
2.8	Summarize risk management best practices.	Compliance and Operational Security	1 hours

2.9	Given a scenario, select the appropriate control to meet the goals of security.	Compliance and Operational Security	2 hours
3.1	Explain types of malware.	Threats and Vulnerabilities	1 hours
3.2	Summarize various types of attacks.	Threats and Vulnerabilities	2.5 hours

Day 5			
3.3	**S**ummarize social engineering attacks and the associated effectiveness with each attack.	Threats and Vulnerabilities	2 hours
3.4	Explain types of wireless attacks.	Threats and Vulnerabilities	1.5 hours
3.5	Explain types of application attacks.	Threats and Vulnerabilities	1.5 hours
3.6	Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.	Network Media and Topologies	2.5 hours
Day 6			
3.7	Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.	Network Security	1.5 hours
3.8	Explain the proper use of penetration testing versus vulnerability scanning.	Network Security	2 hours
4.1	Explain the importance of application security controls and techniques.	Application, Data and Host Security	1 hours
4.2	Summarize mobile security concepts and technologies.	Application, Data and Host Security	1.5 hours
4.3	Given a scenario, select the appropriate solution to establish host security.	Application, Data and Host Security	1hours
4.4	Implement the appropriate controls to ensure data security.	Application, Data and Host Security	1 hours
4.5	Compare and contrast alternative methods to mitigate security risks in static environments.	Application, Data and Host Security	2 hours
5.1	Compare and contrast the function and purpose of authentication services.	Access Control and Identity Management	1 hours

5.2	Given a scenario, select the appropriate authentication, authorization or access control.	Access Control and Identity Management	2 hours
5.3	Install and configure security controls when performing account management, based on best practices.	Access Control and Identity Management	1.5 hours
Day 8			
6.1	Given a scenario, utilize general cryptography concepts.	Cryptography	1.5 hours
6.2	Given a scenario, use appropriate cryptographic methods.	Cryptography	1.5 hours
6.3	Given a scenario, use appropriate PKI, certificate management and associated components.	Cryptography	1.5 hours

Note: There are 6 Exam objectives for Network+. Instructors may have to add or remove material based on students understanding or need. Ultimately, the schedule is at the discretion of the instructor based on assessing student learning.

SECTION 4: COURSE MODULES

Date:	Topic:	Reading Assignment:	TestOut Module
Day 1	Implement security configuration parameters on network devices and other technologies.	Chapters 1	1.5,
	Given a scenario, use secure network administration principles.	Chapters 1	1.5, 3.1, 3.2, 3.3, 9.5,
	Explain network design elements and components.	Chapters 1	1.4, 3.1, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7,
	Given a scenario, implement common protocols and services.	Chapters 2	3.2, 3.3, 5.4, 8.4, 9.4, 9.5
Day 2	Given a scenario, troubleshoot security issues related to wireless networking.	Chapters 2	4.6, 5.1, 5.2-6, 5.8
	Explain the importance of risk related concepts.	Chapters 3	1.3, 3.1, 5.2, 5.3, 5.7, 5.8, 8.6, 1.6, 9.3, 10.1
	Summarize the security implications of integrating systems and data with third parties.	Chapters 2	5.3,
	Given a scenario, implement appropriate risk mitigation strategies.	Chapters 3	3.2, 10.1, 10.2,
Day 3	Given a scenario, implement basic forensic procedures.	Chapters 4	5.9
	Summarize common incident response procedures.	Chapters 4	3.2, 3.3, 4.1, 5.4, 5.5, 5.8, 8.4, 9.4, 9.5,
	Explain the importance of security related awareness and training.	Chapters 4	6.1, 6.2, 6.3, 6.4
	Compare and contrast physical security and environmental controls.	Chapters 6	4.1, 5.2,
Day 4	Summarize risk management best practices.	Chapters 3	10.8
	Given a scenario, select the appropriate control to meet the goals of security.	Chapters 5	10.2, 10.3, 10.4, 10.5, 10.6, 10.7
	Explain types of malware.	Chapters 5	2.1, 2.2, 2.4, 3.1,

			3.2, 3.3, 4.1, 4.2, 4.3, 5.1, 5.2, 7.2, 7.3
	Summarize various types of attacks.	Chapters 5	2.1, 2.2, 2.3, 2.4, 4.3,
Day 5	**S**ummarize social engineering attacks and the associated effectiveness with each attack.	Chapters 5	2.1, 2.2, 2.3, 2.4, 4.3
	Explain types of wireless attacks.	Chapters 5	6.2,
	Explain types of application attacks.	Chapters 5	7.1, 7.2
	Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.	Chapters 6	1.1, 7.1
Day 6	Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.	Chapters 6, 7,	10.3
	Explain the proper use of penetration testing versus vulnerability scanning.	Chapters 6	4.1, 4.2, 6.1, 9.5,
	Explain the importance of application security controls and techniques.	Chapters 7	2.4, 7.1, 10.3,
	Summarize mobile security concepts and technologies.	Chapters 1	8.2, 8.2, 9.5,
	Given a scenario, select the appropriate solution to establish host security.	Chapters 6,20	2.4, 10.3
Day 7	Implement the appropriate controls to ensure data security.	Chapters 8	7.1, 9.4, 10.1, 10.4, 10.5, 10.7
	Compare and contrast alternative methods to mitigate security risks in static environments.	Chapters 3,6	8.6, 9.4,
	Compare and contrast the function and purpose of authentication services.	Chapters 10	7.5, 9.1
	Given a scenario, select the appropriate authentication, authorization or access control.	Chapters 10,11	9.5
	Install and configure security controls when performing account management, based on best practices.	Chapters 7,10,11	6.2, 6.3, 10.8
Day 8	Given a scenario, utilize general cryptography concepts.	Chapter 12	2.4, 7.3, 8.2, 8.6, 9.3
	Given a scenario, use appropriate cryptographic methods.	Chapters 12,13	2.2, 7.3, 8.5
	Given a scenario, use appropriate PKI, certificate management and associated components.	Chapters 13,	6.4, 8.1,

Classroom Lecture:

	Lab Name	Complete (Y/N)	Comment
Day 1	Network Security: Security Configuration Parameters on Network Devices		
	Network Security: Using Secure Network Administration Principles		
Day 2	Network Security: Implementing Common Protocols and Services and Troubleshooting Security Issues Related to Wireless Networking.		
Day 3	Compliance and Operation Security: Risk Related Concepts		
	Compliance and Operation Security: The Importance of Security Related Awareness and Training		
Day 4	Threats and Vulnerabilities: Risk Related Concepts		
	Threats and Vulnerabilities: Types of Wireless and Application Attacks and the Types of Mitigation		
Day 5	Application Data and Host Security: Application Security Controls and Techniques		
Day 6	Access Control and Identity Management: Authentication Services		
	Application Data and Host Security: Host Security and Data Security		
Day 7	Cryptography: Cryptography Concepts and Methods		

Class Discussion:

	Lab Name	Complete (Y/N)	Comment
Day 2	Network Security: Summary and Review		
Day 3	Compliance and Operation Security: Security Implications of Integrating Systems and Data with Third Parties		
	Compliance and Operation Security: Summary and Review		
Day 5	Threats and Vulnerabilities: Security Threats and Vulnerabilities		
	Threats and Vulnerabilities: Summary and Review		
Day 6	Application Data and Host Security: Summary and Review		
Day 7	Access Control and Identity Management: Summary and Review		
Day 8	Cryptography: Cryptography Concepts		

NetLabs:

	Lab Name	Complete (Y/N)	Comments
Day 6	Application Data and Host Security: Importance of Data Security and Data Theft		
Day 7	Access Control and Identity Management: Authentication, Authorization, and Access Control		
Day 8	Cryptography: Importance of Data Security and General Cryptography Concepts		

TestOut:

	Lab Name	Complete (Y/N)	Comment
Day 1	Network Security: Networking Review		
	Network Security: Security Appliances		
	Network Security: Firewalls		
	Network Security: Virtual Private Networks (VPN)		
	Network Security: Web Threat Protection		
	Network Security: Network Devices		
Day 2	Network Security: Wireless Defenses		
	Network Security: Configure a Wireless Profile		
Day 3	Compliance and Operation Security: Implement Physical Security		
Day 4	Threats and Vulnerabilities: Vulnerability Scan 3		
Day 5	Application Data and Host Security: Mobile		
Day 6	Application Data and Host Security: Manage Services with Group Policy		
Day 7	Access Control and Identity Management: Authentication		
	Access Control and Identity Management: Authorization		
	Access Control and Identity Management: Access Control Best Practices		
Day 8	Cryptography: Cryptography		
	Cryptography: Hashing		
	Cryptography: Symmetric Encryption		
	Cryptography: Asymmetric Encryption		
	Cryptography: Public Key Infrastructure (PKI)		

Blackboard eLearning:

	eLearning Unit	Complete (Y/N)	Comment
Day 2	Network Security: Building a Secure Network		
Day 3	Compliance and Operation Security: Compliance and Operation Security		
Day 5	Threats and Vulnerabilities: Threats and Vulnerabilities		
Day 6	Application Data and Host Security: Application, Data, and Host Security		
Day 8	Cryptography: Cryptography		

SECTION 5: COURSE TECHNOLOGY SETUP

Below are instructions to setup and access the technology tools used in this course.

Owl Mail (http://mail.students.pgcc.edu)

Owl Mail is the college's student email system. Your instructor will use Owl Mail *[ADD details here].* To be successful in this course, you should check your Owl Mail account regularly.

To activate your Owl Mail account, follow the directions at http://live.pgcc.edu/.

If you already have an active Owl Mail account, you may access your Owl Mail account at http://mail.students.pgcc.edu.

Blackboard (http://pgcconline.blackboard.com)

Blackboard is a web based program that serves as the college's online classroom. In this course, you will use Blackboard to access the eModules.

Instructions to login to Blackboard:

- Go to the Prince George's Community College Blackboard web site, which is located at http://pgcconline.blackboard.com. NOTE: There is no "www" in the Blackboard address.
- ALL STUDENTS must log in to Blackboard using their ***Owl Link*** account (this includes students who have used Blackboard in the past).
- If you do not have a ***Owl Link*** account,
    1. Go to Owl Link Website (http://www.pgcc.edu --> click "Quicklinks" --> select "Owl Link"
    2. Look up your ***Owl Link*** username (Under User Accounts, select "What's My User ID")
    3. Reset your ***Owl Link*** password (Under User Accounts, select "What's My Password")

    Note: You MUST use your student PGCC student email address in ALL communication with faculty and staff at PGCC.

- Once you have your ***Owl Link*** account information, type it in the Blackboard login box at the http://pgcconline.blackboard.com.
- If your login is successful, you will see the Blackboard "Welcome" screen. In the box labeled "My Courses", you will see the course or a list of courses in which you are enrolled. Click on the course name to enter your Blackboard course.

TestOut (http://testout.com)

TestOut provides online labs for academia and IT professionals. With LabSim, students get a broad range of hands-on experience in a safe, simulated environment.

NetLab(http://netlab5.pgcc.edu/)

NETLAB+ enables organizations to host real IT equipment, virtual machines, and lab content on the Internet to support IT training. NETLAB+ includes all the software needed to provide an environment through which students may schedule and complete lab exercises for Information Technology courses.

SECTION 6: TECHNOLOGY QUICKLINKS

Below are URL links to the technology tools used in this course:

Owl Mail	**http://mail.students.pgcc.edu**
Blackboard	**http://pgcconline.blackboard.com**
TestOut	**http://www.testout.com**
NetLabs	**https://moac.microsoftlabsonline.com**

SECTION 7: STUDENT SUPPORT

HTT Program Support Contact
Contact:
Title:
Email:

Technical Support
For technical support in this course, your first point of contact should be your instructor.

1. Blackboard: Please look to the following site:
   http://www.pgcconline.com/technicalSupport.html

Disability Support Services
Students requesting academic accommodations are required to contact the College's Disability Support Services Office (B-124) or call (301) 546-0838 (voice) or (301) 546-0122 (TTY) to establish eligibility for services and accommodations. Students with documented disabilities should discuss the matter privately with their instructors at the beginning of the semester and provide a copy of the completed Student/Faculty Accommodation Form.