This course supports the assessment for Security I. The course covers 6 competencies and represents 6 competency units, and prepares for the CompTIA Security + (SY0-401) certification exam.

Introduction

Overview

How long do you think your business or organization would survive if your data was not secure? Computers can house social security numbers, financial data, educational records, health information, and even programs that control military weapons.

Long gone are the times when you only ensured that applications and systems were built to meet functional requirements. Security requirements are equally important, and existing systems are often overhauled to implement security measures. IT technology is constantly changing and so is the technology used by hackers and criminals. Security is a growing concern, and not just among IT professionals. Customers now consider how well an organization will protect their data when deciding with whom they will conduct business.

As an IT security professional, you are expected to implement techniques that secure networks and computers. Security attacks are on the rise and continue to be a concern for organizations worldwide. As a result, competent security professionals are in high demand. A career as an IT security professional will undoubtedly provide you with many opportunities in a variety of industries and organizational environments.

To be a competent security professional, you should know how to recognize and prevent security attacks, identify security needs for your organization, and understand encryption techniques. You should be able to effectively evaluate security risks and know how to leverage various access control models.

Note: To use LabSim (i.e., the primary learning resource for this course), your computer must

- be running Microsoft Windows XP/Vista/7, and
- meet the minimum hardware and software system requirements provided on the LabSim website.

Watch the following video for an introduction to this course:

Note: View the video in full screen at 720p for best results.

Competencies

This course provides guidance to help you demonstrate the following 6 competencies:

- Competency 419.2.1: Basic Security Concepts
The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.

- **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.

- **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.

- **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.

- **Competency 419.2.5: Security for Organizational Operations**
  The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.

- **Competency 419.2.6: Security Assessments & Audits**
  The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

**Course Instructor Assistance**

As you prepare to successfully demonstrate competency in this subject, remember that course instructors stand ready to help you reach your educational goals. As subject matter experts, mentors enjoy and take pride in helping students become reflective learners, problem solvers, and critical thinkers. Course instructors are excited to hear from you and eager to work with you.

Successful students report that working with a course instructor is the key to their success. Course instructors are able to share tips on approaches, tools, and skills that can help you apply the content you’re studying. They also provide guidance in assessment preparation strategies and troubleshoot areas of deficiency. Even if things don’t work out on your first try, course instructors act as a support system to guide you through the revision process. You should expect to work with course instructors for the duration of your coursework, so you are welcome to contact them as soon as you begin. Course instructors are fully committed to your success!

**Preparing for Success**

The information in this section is provided to detail the resources available for you to use as you complete this course.

**Learning Resources**

The learning resources listed in this section are required to complete the activities in this course. For many resources, WGU has provided automatic access through the course. However, you may need to manually enroll in or independently acquire other resources. Read the full instructions provided to ensure that you have access to all of your resources in a timely manner.

*Note: If you decide to use other learning resources, particularly those found online, make certain that none qualify as a brain-dump. Using them can result in academic sanctions and loss of your certification.*
Note: Please see the full CompTIA Candidate Agreement.

Automatically Enrolled Resources

You will be automatically enrolled at the activity level for the following learning resources. Simply click on the links provided in the activities to access the learning materials.

LabSim
You will access the following resource at the activity level within this course:

- LabSim by TestOut, Security+ (2014)

To use LabSim your computer must

- be running either Microsoft Windows XP, Vista, or 7 and
- meet the minimum hardware and software system requirements provided on the System Requirements page.

SkillSoft and Books 24x7

You will access SkillSoft items at the activity level within this course. For more information on accessing SkillSoft items, please see the “Accessing SkillSoft Learning Resources” page.

The following Books24x7 e-texts will be used in this course:


*Note: These e-texts are available to you as part of your program tuition and fees, but you may purchase hard copies at your own expense through a retailer of your choice. If you choose to do so, please use the ISBN listed to ensure that you receive the correct edition.*

Pacing Guide

The pacing guide suggests a weekly structure to pace your completion of learning activities. It is provided as a suggestion and does not represent a mandatory schedule. Follow the pacing guide carefully to complete the course in the suggested timeframe.

- Pacing Guide: Network and Security - Applications

*Note: This pacing guide does not replace the course. Please continue to refer to the course for a comprehensive list of the resources and activities.*
LabSim Information

The following information pertains to LabSim and what will be covered in this course. Sections referenced correspond directly to the section in LabSim where the information is covered.

LabSim

The LabSim learning resource (Security+ 2014) for this course contains the following:

- Videos: 139 (19:42)
- Demonstrations: 117 (16:26)
- Simulations: 74
- Written Lessons: 122
- Exam Questions: 1037
- Section Quizzes: 82
- Practice Exams: 25

The LabSim modules are constructed in a manner to build off previous lessons, so it is not recommended that you complete the sections out of order. Each module has

- videos,
- lecture/fact sheets, and
- lab simulations.

It is essential to read the materials prior to attempting the simulations to ensure you have a full and applicable understanding of the concepts and competencies required for successful completion of the practice exams.

Note: It is strongly recommended that you continue to attempt lab simulations until you can easily complete the tasks scoring 100% and pass practice exams with no less than 90% to maximize your chances of successfully passing the actual examination associated with this course.

This topic addresses the following competencies:

- **Competency 419.2.1: Basic Security Concepts**
  The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.

- **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.

- **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.

- **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.
• **Competency 419.2.5: Security for Organizational Operations**
  The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.

• **Competency 419.2.6: Security Assessments & Audits**
  The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

**The Preassessment**

The preassessment assesses your knowledge of the content covered in this course. Your performance on this assessment will help guide you to the areas on which you need to focus the most attention.

Complete the LabSim "Practice Exam" within the LabSim learning resource before beginning the course.

If needed, use the [LabSim Preassessment Instructions](#).

When you take this preassessment, you should avoid

- studying for it in advance,
- looking up answers while taking it, and
- guessing at the correct answer (instead of simply "knowing" it).

Review the results of your preassessment with your mentor.

**LabSim Modules**

Direct your attention to the CompTIA Security+ exam objective(s) associated with each chapter. This will help you pinpoint those chapters that require special attention based on the results of your preassessment.

*Note: Because you are to complete the activities for this course within the LabSim learning resource, the following list of modules has been provided to*

- *orient you as you begin the course, and*
  *provide an overview of the content you will be studying.*

Access the following LabSim resource:

• **Security+ (2014) (SY0-401)**

Complete all of the modules within the following sections:

- 1.0 Introduction
- 2.0 Access Control and Identity Management
- 3.0 Cryptography
- 4.0 Policies, Procedures, and Awareness
• 5.0 Physical Security
• 6.0 Perimeter Defenses
• 7.0 Network Defenses
• 8.0 Host Defenses
• 9.0 Application Defenses
• 10.0 Data Defenses
• 11.0 Assessments and Audits
• Practice Exams

Please remember to proceed through the activities in the specified order.

**E-Text Reading**

Read the sections of the following text as they correspond to LabSim:

• *CompTIA Security+ Study Guide: SYO-401*

Each of the LabSim sections corresponds to a part of the CompTIA Security+ Study Guide: SYO-401. See the following page for the details on how these two resources work together:

• *LabSim Security+ Courseware Mapping*

**Transcender Practice Exam**

The Transcender practice exam will help you gauge how prepared you are for the CompTIA Security+ exam.

**Transcender Practice Exam**

Take the Transcender practice exam to determine your readiness for the CompTIA Security+ exam.

This topic addresses the following competencies:

• **Competency 419.2.1: Basic Security Concepts**
  The graduate identifies and discusses basic concepts of security and security threats, and recommends security procedures.

• **Competency 419.2.2: Access Control & Authentication Methods**
  The graduate recommends appropriate methods for controlling accessing data and information and for authenticating users and groups in gaining that access.

• **Competency 419.2.3: Security for Network Infrastructure**
  The graduate identifies security needs and recommends appropriate security practices for network infrastructure.

• **Competency 419.2.4: Encryption**
  The graduate identifies and explains the role of encryption in network security.
• **Competency 419.2.5: Security for Organizational Operations**  
The graduate explains and makes recommendations for appropriate security strategies and procedures for organizational operations.

• **Competency 419.2.6: Security Assessments & Audits**  
The graduate evaluates risks associated with network security and recommends monitoring strategies and methods.

**Transcender Practice Exam**

Use the Transcender practice exams to help you determine your readiness for the CompTIA Security+ exam:

- [CompTIA Practice Exam for SY0-401 CompCert: Security+](#)

**Final Steps**

Congratulations on completing the activities in this course! This course has prepared you to complete the assessment associated with this course. If you have not already been directed to complete the assessment, schedule and complete your assessment now.

**LabSim Practice Exam**

Take the "Practice Exam" at the end of the course. This will provide you with valuable feedback about

- your readiness to take the Certification Exam, and
- more specifically, questions you miss and what section you can refer back to in order to complete additional study.

It is recommended that you take and pass the Practice Exam at least twice with a score of 90% or higher before considering yourself ready for the assessment.

**First Attempt Checklist**

One of the many things that makes WGU unique is its competency based education model. If you know the material, all you have to do is prove it by passing the exam. If you can do this, you can accelerate the receipt of your degree.

To make sure you have the best chance possible to pass the exam on your first attempt, the following should be completed before you refer to take it:

1. Go through the course in its entirety. Mark as complete as you progress.
2. Complete Labsim in its entirety. Make sure each section is completed in order and that all videos and demonstrations are watched fully.

3. Pass the 6 Security+ Domains at the end of Labsim with an 80% or above. Please be sure to select, "Security+ Practice Exams," as this LabSim course also prepares for the Security Pro and SSCP certifications.

4. Pass the Practice Certification Exam in Labsim scoring a 95% or above.

5. Read and review the *CompTIA Security+ Study Guide: SYO-401* and take notes as appropriate. This book should be read in its entirety and used to help build competency after Labsim is completed.

6. Spend at least 8–10 weeks studying.

After completing the above sections and passing, please speak to your program mentor to have your voucher emailed to you.

This course of study supports the CompTIA Security+ 401 exam. Your voucher gives you access to several different exams. Please ensure you register for the correct version of the Security+ 401 exam. If you are unsure of how to register for the correct exam, please contact your mentor.

If the first attempt is failed, you will be required to get in contact with the course instructor to see what went wrong and how you can prepare to make sure your second attempt is a success. Once the course instructor feels you are ready to refer for the second attempt of the exam, he or she will approve your second exam referral.

**Outside Vendor Assessment**

You will complete the CompTIA Security+, 2014 Edition Exam:

- Exam ID: CompTIA Security+ 2014 Objectives (SY0-401 or educational code JK0-022) exam
- Number of Items: 90
- Passing score: at least 750 out of 900 points to be considered "passed."
- Time Limit: 90 minutes

*Note: Your voucher will show JK0-022, which is how CompTIA codes vouchers from educational institutions. The exam is the same as the SY0-401.*

*Note: Please note that CompTIA exams are no longer available at Prometric testing centers. Please see the CompTIA KnowledgeBase if you have questions.*

For directions on how to receive access to outside vendor assessments, see the “Accessing Objective and Outside Vendor Assessments” page.

**Submitting Outside Vendor Assessment Scores**

After completing an outside vendor assessment, follow the directions for submitting a score report on the “Following Outside Vendor Assessments” page.