Cybersecurity Essentials 1.1 Release Notes

Last updated 22 August 2018

Purpose

The *Cybersecurity Essentials 1.1* course prepares students to continue their education in more advanced security courses. This exploratory course contains eight chapters that explain why cybersecurity is needed, the kinds of tools used to combat a cybersecurity threat, and the growing opportunities for careers in this exciting field.

Release Content

Table 1. Content included in the *Cybersecurity Essentials 1.1* Course Release

Component	Description
E-Learning Content	8 chapters
Labs	12 hands-on labs use a combination of security tools. Some labs include the use of a custom virtual machine (VM). Students should have access to a PC with the VM installed. Students can also download and install the VM on their own PC.
Packet Tracer Activities	10 Packet Tracer activities embedded in the curriculum (PT version 6.3 or higher is required)
Packet Tracer Skills Integration Challenge	1 capstone challenge at the end of the course
Additional Resources	Chapters include a variety of links out to external resources for further investigation
Chapter Quizzes	8 chapter quizzes
Final Quiz	Dynamically built final quiz that pulls from 8 pools of questions
Accessibility	8 chapters containing accessible text and media text
Certificate of Completion	The successful completion of the chapter modules and end-of-course survey are required to receive the Certificate of Completion.

Known Issues

Table 2. Known Issues for the *Cybersecurity Essentials 1.1*

Item	Description
English Spelling	American and British English spellings are interspersed in the text of the modules

Course Outline

Table 3. Course Outline for *Cybersecurity Essentials 1.1*

Chapter	Chapter Title
1	Cybersecurity - A World of Experts and Criminals
2	The Cybersecurity Cube
3	Cybersecurity Threats, Vulnerabilities, and Attacks
4	The Art of Protecting Secrets
5	The Art of Ensuring Integrity
6	The Five Nines Concept
7	Protecting a Cybersecurity Domain
8	Becoming a Cybersecurity Specialist

Certification Exam Alignment

The *Cybersecurity Essentials 1.1* course does not fully align with any certification. However, the content does support many of the objectives within the CompTIA Security+ certification objectives, as outlined in Table 4.

Table 4. Partial CompTIA Security+ SY0-401 Framework Alignment

Chapter	CompTIA Security+
1	**Cybersecurity - A World of Experts and Criminals**
	2.2: Summarize the security implications of integrating systems and data with third parties.
	2.6: Explain the importance of security related awareness and training
	2.7: Compare and contrast physical security and environmental controls.
	3.2: Summarize various types of attacks.
	3.4: Explain types of wireless attacks.
	3.7: Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
2	**The Cybersecurity Cube**
	2.9: Given a scenario, select the appropriate control to meet the goals of security.
3	**Cybersecurity Threats, Vulnerabilities, and Attacks**
	3.1: Explain types of malware.
	3.2: Summarize various types of attacks.
	3.3: Summarize social engineering attacks and the associated effectiveness with each attack.
	3.4: Explain types of wireless attacks.
	3.5: Explain types of application attacks.
4	**The Art of Protecting Secrets**
	5.2: Given a scenario, select the appropriate authentication, authorization or access control.
	6.1: Given a scenario, utilize general cryptography concepts.
	6.2: Given a scenario, use appropriate cryptographic methods.
5	**The Art of Ensuring Integrity**
	2.9: Given a scenario, select the appropriate control to meet the goals of security.
	6.1: Given a scenario, utilize general cryptography concepts.
	6.2: Given a scenario, use appropriate cryptographic methods.
	6.3: Given a scenario, use appropriate PKI, certificate management and associated components.
6	**The Five Nines Concept**
	2.1: Explain the importance of risk related concepts.
	2.5: Summarize common incident response procedures.
	2.8: Summarize risk management best practices.
	2.9: Given a scenario, select the appropriate control to meet the goals of security.

7	**Protecting a Cybersecurity Domain**
	1.1: Implement security configuration parameters on network devices and other technologies.
	1.4: Given a scenario, implement common protocols and services.
	2.4: Given a scenario, implement basic forensic procedures.
	2.7: Compare and contrast physical security and environmental controls.
	2.8: Summarize risk management best practices.
	2.9: Given a scenario, select the appropriate control to meet the goals of security.
	3.1: Explain types of malware.
	3.6: Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
	4.2: Summarize mobile security concepts and technologies.
	4.3: Given a scenario, select the appropriate solution to establish host security.
	4.4: Implement the appropriate controls to ensure data security.
	4.5: Compare and contrast alternative methods to mitigate security risks in static environments.
	5.2: Given a scenario, select the appropriate authentication, authorization or access control.
	5.3: Install and configure security controls when performing account management, based on best practices.
	6.2: Given a scenario, use appropriate cryptographic methods.
8	**Becoming a Cybersecurity Specialist**
	2.1: Explain the importance of risk related concepts.
	2.6: Explain the importance of security related awareness and training
	2.7: Compare and contrast physical security and environmental controls.
	3.2: Summarize various types of attacks.
	3.6: Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
	3.7: Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
	4.2: Summarize mobile security concepts and technologies.
	2.1: Explain the importance of risk related concepts.

The following CompTIA Security+ SY0-401 Objectives are not covered in *Cybersecurity Essentials 1.1*:

- 1.2: Given a scenario, use secure network administration principles.
- 1.3: Explain network design elements and components.
- 1.5: Given a scenario, troubleshoot security issues related to wireless networking.
- 2.3: Given a scenario, implement appropriate risk mitigation strategies.
- 3.8: Explain the proper use of penetration testing versus vulnerability scanning.
- 4.1: Explain the importance of application security controls and techniques.
- 5.1: Compare and contrast the function and purpose of authentication services.

For more information on the CompTIA Security+ certification visit the CompTIA website here:

https://certification.comptia.org/training/certmaster/security

Support

For general assistance with curriculum, classroom, or program issues, please contact the Networking Academy™ Support Desk by signing into www.netacad.com and clicking **Help** > **Contact Support** at the top of the page.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**