
Security Essentials 1.0

(Exam code 020-100)

Overview:

IT security is absolutely crucial for individuals and organizations in today's digital world. The general ability to protect data, devices and networks is a fundamental skill for the responsible use of information technology. Obtaining the Linux Professional Institute Security Essentials certificate is a fantastic way to learn how to protect yourself and to demonstrate your knowledge and expertise in the field to potential employers and clients.

The Security Essentials exam covers preliminary knowledge in all important fields of IT security. The certificate is intended for students who had their first course in IT security, for all members and staff of organizations that want to improve their IT security as well as for individuals who want to attain a basic competence in the secure use of information technology.

Prerequisites

There are no prerequisites for this certificate

Requirements:

Pass the Security Essentials 020 exam

To receive the certificate the candidate must:

- Have a basic understanding of common security threats of using computers, networks, connected devices, and IT services on premises and in the cloud;
- Understand common ways to prevent and mitigate attacks against their personal devices and data;
- Be able to use encryption to secure data transferred through a network and stored on storage devices and in the cloud;
- Be able to apply common security best practices, protect private information, and secure their identity; and
- Able to securely use IT services and to take responsibility for securing their personal computing devices, applications, accounts, and online profiles.

Objectives

1. Security Concepts

- 1.1 021.1 Goals, Roles and Actors (weight: 1)
- 1.2 021.2 Risk Assessment and Management (weight: 2)
- 1.3 021.3 Ethical Behavior (weight: 2)

2. Encryption

- 2.1 022.1 Cryptography and Public Key Infrastructure (weight: 3)
- 2.2 022.2 Web Encryption (weight: 2)
- 2.3 022.3 Email Encryption (weight: 2)
- 2.4 022.4 Data Storage Encryption (weight: 2)

3. Device and Storage Security

- 3.1 023.1 Hardware Security (weight: 2)
- 3.2 023.2 Application Security (weight: 2)
- 3.3 023.3 Malware (weight: 3)
- 3.4 023.4 Data Availability (weight: 2)

4. Network and Service Security

- 4.1 024.1 Networks, Network Services and the Internet (weight: 4)
- 4.2 024.2 Network and Internet Security (weight: 3)
- 4.3 024.3 Network Encryption and Anonymity (weight: 3)

5. Identity and Privacy

- 5.1 025.1 Identity and Authentication (weight: 3)
- 5.2 025.2 Information Confidentiality and Secure Communication (weight: 2)
- 5.5.3 025.3 Privacy Protection (weight: 2)