

Cyber Security

Lesson 1



Cyber Security

Preparation for CompTIA Security+ exam

+

Introduction to Certified Ethical Hacker exam by EC-Council

Cyber Security Role	Required/Recommended Certifications
Information Security Analyst	CompTIA Security+, CEH, CISSP
Security Consultant	CompTIA Security+, CISSP, CISM, CEH
Penetration Tester	OSCP, CEH, CompTIA PenTest+, GWAPT
Cybersecurity Engineer	CISSP, CompTIA Security+, CEH, GSEC
Security Architect	CISSP, CEH, SANS GIAC, CISM
IT Security Manager	CISSP, CISM, CompTIA Security+, GIAC GSEC
Chief Information Security Officer (CISO)	CISSP, CISM, CompTIA Security+, GSEC
Cybersecurity Analyst	CompTIA CySA+, CEH, CISSP, GIAC GSEC
Network Security Engineer	CompTIA Security+, Cisco CCNA, CISSP, GSEC
Systems Security Administrator	CompTIA Security+, SSCP, CISSP, CEH
Forensic Computer Analyst	GIAC Certified Forensic Analyst (GCFA), CCE, EnCE
Security Software Developer	CompTIA Secure Software Developer+, GIAC GWEB, CSSLP
Incident Responder	GIAC Certified Incident Handler (GCIH), CERT-CSIH, ECIH
Vulnerability Assessor	CEH, CompTIA Security+, OSCP, CVPA
Cryptographer	GIAC Defensible Security Architecture (GDSA), CompTIA Security+
Compliance Analyst	CISA, CRISC, CGEIT, CompTIA Security+
Security Awareness Trainer	EC-Council Certified Security Specialist (ECSS), CompTIA Security+

Trainer

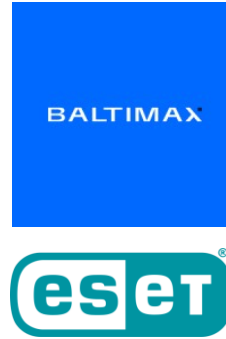
Lukas Apynis

Patirtis:

Dirbu nuo 2020 metų, IT srityje – 8+ metai

Darbo pobūdis:

- ESET ir kitų saugumo produktų implementacija
- Kibernetinių incidentų tyrimas
- Mokymai IT specialistams ir įmonių darbuotojams
- Pranešimų skaitymas konferencijose
- XDR/MDR/SOC



- Expectations for the course :
 - ✓ student preparation for CompTIA Security+ exam
 - ✓ introduction to Certified Ethical Hacker by EC-Council exam preparation




Students' introduction

- Name
- Job responsibility
- Computer/networking experience
- Expectations for the course

Security+ Test Overview

Number of questions	Maximum of 90
Time allowed	90 minutes
Minimum Passing Score	750 (83.33%)
Scale	100-900
Recommended Prerequisites	
Exam format	Conventional linear format Multiple-choice questions Performance-based questions

CompTIA Security+ Prices

<p>Security+ Voucher</p> <p>Exam SY0-701</p>  <p>INCLUDES:</p> <p>✓ 1 Exam Voucher</p> <p>Our Price: €364.00</p> <p>Details Add to Cart</p>	<p>Security+ Voucher + Retake</p> <p>Exam SY0-701</p>  <p>INCLUDES:</p> <p>✓ 1 Exam Voucher + Retake</p> <p>Our Price: €727.00</p> <p>Details Add to Cart</p>
--	---

Exam discount: <https://getcertified4less.com/CompTIA-Vouchers>

Recommended Prerequisites

- At least 2 years of work experience
 - In IT systems administration
 - With a focus on security or related field
- Hands-on technical information security experience
- Broad knowledge of security concepts

Security+ Test Overview

- Must recertify every three years
- Requires participation in continuing education program
 - Moving target
 - Check CompTIA site for current requirements

Security+ Domain Objectives

Domain	% of Examination
1.0 General Security Concepts	12%
2.0 Threats, Vulnerabilities and Mitigations	22%
3.0 Security Architecture	18%
4.0 Security Operations	28%
5.0 Security Program Management and Oversight	20%

- Test seeded with beta questions

General Security Concepts

Includes various types of security controls, fundamental security concepts, the importance of change management processes and using cryptographic solutions.



Understanding cybersecurity terminology and core concepts are essential to cybersecurity work and provides a common language of communication for cybersecurity industry workers.

Threats, Vulnerabilities and Mitigations

Includes threat actors and motivations, threat vectors and attack surfaces, types of vulnerabilities, mitigation techniques and indicators of malicious activity.



Cybersecurity professionals must be aware of the threats, attacks and vulnerabilities that may impact their networks in order to mitigate them (i.e., reduce the risk, lessen the harm). To prevent data breaches, malicious activity must be identified and analysed, and mitigation techniques implemented to secure the enterprise.

Security Architecture

Includes security implications of different architecture models, concepts and strategies to protect data, security principles to secure enterprise infrastructure and the importance of resilience and recovery in security architecture.



Cybersecurity professionals must be familiar with different types of security architectures because different techniques are needed to secure them, including on-premises, the cloud and hybrid (on-premises and cloud) networks.

Security Operations

Includes security techniques, security alerting and monitoring concepts and tools, vulnerability management activities, security implications of proper hardware, software and data asset management, identity and access management, as well as the importance of automation and orchestration and incident response activities.



Security operations includes the important day-to-day work that cybersecurity professionals do, such as monitoring systems, finding vulnerabilities, hardening systems and incident response. Incident response is a key function of cybersecurity professionals; skilled employees are needed to implement an effective incident response plan.

Security Program Management and Oversight

Includes elements of effective security governance, the risk management process (including third-party risk assessment and management), types and purposes of audits and assessments, security awareness practices and elements of effective security compliance.



Cybersecurity professionals are responsible for reporting and communicating their activities, such as security incident information, the types of threats, attacks and vulnerabilities found, trends they have encountered, etc.. Cybersecurity professionals must learn the latest trends of effective security governance, including third-party risk management concepts, to help with security compliance for an organization.

Course Materials

- Slides
- Labs
- Additional materials from various sources

Course Outline

- Ch 1: Mastering Security Basics
- Ch 2: Understanding Identity and Access Management
- Ch 3: Exploring Network Technologies and Tools
- Ch 4: Securing Your Network
- Ch 5: Securing Hosts and Data
- Ch 6: Comparing Threats, Vulnerabilities, and Common Attacks

Course Outline (Cont)

- Ch 7: Protecting Against Advanced Attacks
- Ch 8: Using Risk Management Tools
- Ch 9: Implementing Controls to Protect Assets and Business Continuity
- Ch 10: Understanding Cryptography and PKI
- Ch 11: Implementing Policies to Mitigate Risks

Recipe for Success

- Successfully complete class
- Practice, Practice, Practice
- Take exam within 30 days of class

Facilities

- Class hours
- Phones & Messages

Chapter 1

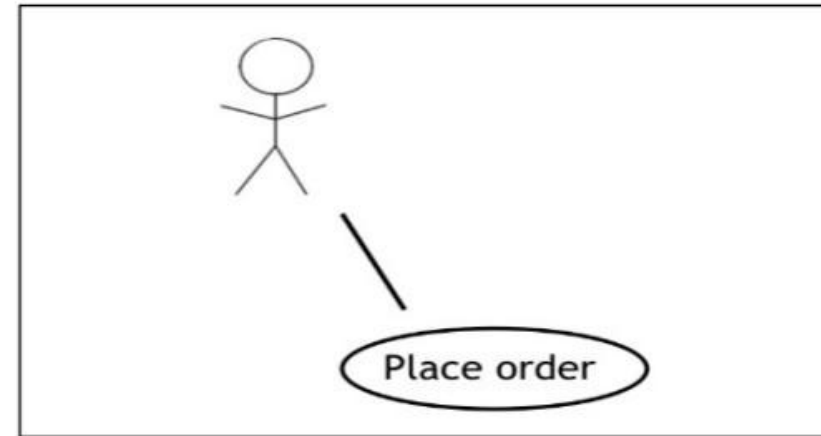
Mastering Security Basics

Introduction

- Understanding Core Security Goals
- Introducing Basic Risk Concepts
- Understanding Security Controls
- Using Command-Line Tools
- Understanding Logs

Understanding Core Security Goals

- Use Case
 - Describes a goal an organization wants to achieve
 - Elements
 - Actors
 - Precondition
 - Trigger
 - Postcondition
 - Normal flow
 - Alternate flow



Understanding Core Security Goals



Understanding Core Security Goals



Confidentiality

- Encryption
- Access controls
 - Identification
 - Authentication
 - Authorization



Understanding Core Security Goals



Availability

- Redundancy & Fault tolerance
- Scalability and Elasticity (scaling up and scaling out)

– Patching

– Resiliency



Understanding Core Security Goals



Integrity

— Protecting data from **unauthorized** :

➤ modification

➤ deletion

➤ addition

— digital signatures

— data hashing



Understanding Core Security Goals



- **Authenticity**
 - Protecting against impersonation, spoofing and other types of identity fraud :
 - Authentication
 - Digital certificates
 - Biometric identification
- **Non-repudiation**
 - Party cannot deny having sent or received a message or transaction :
 - Protecting against message tampering and replay attacks
 - Digital signatures
 - Timestamps

Understanding Core Security Goals





LABS 1.1

✓ Practice exam

13 Questions

self-assessment

At least 8 correct - OK

LABS 1.2

- Create virtual environment for labs – KALI Linux
- ✓ **Challenge** : Create KALI on Windows or MacOS virtual environment

