FUNDAMENTALS OF CYBERSECURITY

EXAM INFORMATION

This exam was developed to enable schools to award credit to students for knowledge equivalent to that learned by students taking the course. This exam covers topics such as disaster recovery, operational and network security, authentication, authorization, access controls, application and systems security.

The exam contains 100 questions to be answered in 2 hours.

Form Codes: SS013, ST013, SY013, SZ013

CREDIT RECOMMENDATIONS

The American Council on Education's College Credit Recommendation Service (ACE CREDIT) has evaluated the DSST test development process and content of this exam. It has made the following recommendations:

Area or Course Equivalent: Fundamentals of Cybersecurity
Level: Lower-level baccalaureate
Amount of Credit: 3 Semester Hours
Minimum Score: 400
Source: www.acenet.edu

EXAM CONTENT OUTLINE

The following is an outline of the content areas covered in the examination. The approximate percentage of the examination devoted to each content area is also noted.

I. **Application & Systems Security – 15%**
   a. Security Triad
   b. Accountability & non-repudiation
   c. Fundamentals of Cryptography
   d. Security development life cycle
   e. Best practices for migration from development environment to production
   f. Anti-virus protection and malware detection
   g. Software Development (Dev) and IT operations (Ops) and SecOps (Security + Operations)

II. **Authentication, Authorization, & Access Controls – 12%**
   a. Implementing authentication technologies
   b. Authorization
   c. Access controls
   d. Identity and Access Management

III. **Compliance, & Governance – 12%**
   a. Security architecture
   b. Audits and Risk Assessment
   c. Outsourcing
   d. Ethics and legal
   e. Governance Risk & Compliance

IV. **Operational Security – 10%**
   a. Securing and monitoring the production environment
   b. Policies, standards and procedures

V. Network Security – 16%

a. Protocols and services
b. Analysis tools and management
c. Infrastructure
d. Wireless i.e. 5G,Bluetooth,LTE

VI. Vulnerability Management – 17%

a. Penetration Testing
b. Recognizing and mitigating threats
c. Tools
d. Security Awareness Training i.e. Preventing Social Engineering, Phishing etc

VII. Physical & Environmental Security – 6%

a. Physical access controls and management
b. Logical Controls

VIII. Disaster Recovery & Business Continuity – 12%

a. Backup and Recovery, Retention, Offsite and Cloud Storage, Archiving
b. Business impact analysis
c. Disaster recovery planning
d. Business continuity planning
e. Plan testing and maintenance
f. Incident Response Planning

REFERENCES

Below is a list of reference publications that were either used as a reference to create the exam, or were used as textbooks in college courses of the same or similar title at the time the test was developed. You may reference either the current edition of these titles or textbooks currently used at a local college or university for the same class title. It is recommended that you reference more than one textbook on the topics outlined in this fact sheet.

You should begin by checking textbook content against the content outline provided before selecting textbooks that cover the test content from which to study.

Sources for study material are suggested but not limited to the following:

1. John Warsinske. (2019). Official (ISC)2 Guide to the CISSP CBK, 5th Edition. Auerbach Publications.
2. Pfleeger, Charles P; Pfleeger, Shari Lawrence; Maggulies, Jonathan. (2015). Security in Computing, 5th Edition. Prentice Hall PTG.
3. Conklin, Arthur Wm; White, Gregory (2018) CompTIA Security+ All-in-One Exam Guide (Exam SY0-501) 5th Edition. McGraw-Hill Education

SAMPLE QUESTIONS

All test questions are in a multiple-choice format, with one correct answer and three incorrect options. The following are samples of the types of questions that may appear on the exam.

1. A company needs to digitally sign all of the data sent to its customers. What should the administrator use to digitally sing the data?

a. Asymmetric Keys
b. Standard Keys
c. Symmetric Keys
d. Quantitative Keys

2. What standard does a Certificate Authority (CA) use to create a certificate?
   a. X.509
   b. X.802
   c. X.423
   d. X129

3. The concept of comparing the best practices and performance metrics of other companies with a similar process is known as
   a. Benchmarking
   b. Gap Analysis
   c. Baselining
   d. Quantifying

4. If an intrusion detection system wanted to only monitor web traffic, what would the rules filter on?
   a. IP Address
   b. Port
   c. User Name
   d. Destination Name

5. What security technique can be used to identify malicious HTTPS (Secure Hyper Text Transport Protocol) tunnels?
   a. Detection inspection
   b. Context inspection
   c. Plain HTTP inspection
   d. SSL inspection

Answers to sample questions:

1-A; 2-A; 3-A; 4-B; 5-D