DSST® FUNDAMENTALS OF CYBERSECURITY

EXAM INFORMATION

This examination includes content related to major topics in cybersecurity including application and systems security, implementing authentication and authorization technologies, compliance, security pertaining to networks and physical environments, and vulnerability management.

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

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. Applications and Systems Security – 17%
- a. Best practices for bringing new services and applications in production
- b. Implementing and maintaining encryption
- c. Communicating security concerns throughout the system development life cycle (SDLC)

II. Authentication and Authorization – 13%
- a. Implementing authentication technologies
- b. Authorization

III. Compliance / Governance – 13%
- a. Security Architecture
- b. Identifying risks and threats
- c. Outsourced process governance

IV. Operational Security – 15%
- a. Securing and monitoring the environment
- b. Securing and monitoring cloud and virtualization

V. Network Security – 19%
- a. Protocols and services
- b. Analysis and management
- c. Infrastructure

VI. Physical and Environmental Security – 8%
- a. Physical access management
- b. Media management
- c. Environmental controls

VII. Vulnerability Management – 15%
- a. Testing the network
- b. Recognizing and mitigating threats

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:

Print References:

1. , Brad (2010). *Seven deadliest wireless technologies attacks.*
2. Harris & Shon. (2007). *CISSP Certification All-in-One Exam Guide.* 4th Ed.
3. Jernigan, Scott & Meyers, Michael (2011). *CompTIA Strata IT fundamentals all-in-one exam guide.*
4. Ligh, Michael Hale & Adair, Steven & Hartstein, Blake & Richard, Matthew. *Malware analyst's cookbook: tools and techniques for fighting malicious code*. (2011). ISBN:9780470613030
5. Orebaugh, A., & Pinkard, B. (2008). *Nmap In the Enterprise: Your Guide to Network Scanning*.
6. Shinder, Debra Littlejohn & Cross, Michael. *Scene of the Cybercrime.* 2nd Edition. Haines
7. Tipton, Harold F. (1997). Handbook of *Information Security Management.*
8. Vyncke, Eric & Paggen, Christopher. *Lan switch security: what hackers know about your switches: a practical guide to hardening layer 2 devices and stopping campus network attacks*., (2008). ISBN:9781587052569
9. Whitman, Michael E., Mattord, Herbert J., & Green, A., (2012). *Guide to firewalls and VPNs .* Boston, MA: Course Technology, 3rd Ed.

Online References:

1. http://csrc.nist.gov/groups/SNS/rbac/documents/design_implementation/Intro_role_based_access.htm

2. http://federalevidence.com/blog/2008/september/using-%E2%80%9Chash%E2%80%9D-values-handling-electronic-evidence

3. http://informationr.net/ir/7-3/paper129.html

4. http://searchsecurity.techtarget.com/definition/false-rejection

5. http://technet.microsoft.com/en-us/library/cc786041%28v=WS.10%29.aspx

6. http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_2/ccmsys/a02mla.html

7. http://www.giac.org/cissp-papers/2.pdf

8. http://www.itl.nist.gov/lab/bulletns/bltnaug04.htm

9. http://www.sans.org/critical-security-controls/control.php?id=12

10. https://www.owasp.org/index.php/Secure_Coding_Principles

11. https://www.us-cert.gov/sites/default/files/publications/TIP11-075-01.pdf

SAMPLE QUESTIONS

All test questions are in a multiple-choice format, with one correct answer and three incorrect options. These are samples of the types of questions that may appear on the exam. Other sample questions can be found in the form of practice exams by visiting our website at **www.getcollegecredit.com/testprep.**

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

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 recommendation

Area or Course Equivalent	Fundamentals of Cybersecurity
Level	Upper-level baccalaureate
Amount of Credit	Three (3) semester hours
Minimum Score	400
Source	American Council on Education – College Credit Recommendation Service

Answers to sample questions: 1-A; 2-A; 3-A; 4-B; 5-D