EDUSUM

#1 Online Certification Guide

GIAC GSEC

GIAC GSEC Certification Questions & Answers

Exam Summary – Syllabus –Questions

GSEC

GIAC Security Essentials (GSEC)

180 Questions Exam – 73% Cut Score – Duration of 300 minutes

Table of Contents:

Know Your GSEC Certification Well:

The GSEC is best suitable for candidates who want to gain knowledge in the GIAC Cyber Defense. Before you start your GSEC preparation you may struggle to get all the crucial GSEC materials like GSEC syllabus, sample questions, study guide.

But don't worry the GSEC PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the GSEC syllabus?
- How many questions are there in the GSEC exam?
- Which Practice test would help me to pass the GSEC exam at the first attempt?

Passing the GSEC exam makes you GIAC Security Essentials (GSEC). Having the GSEC certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GIAC GSEC Certification Details:

Exam Name	GIAC Security Essentials (GSEC)
Exam Code	GSEC
Exam Price	$1999 (USD)
Duration	300 mins
Number of Questions	180
Passing Score	73%
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GSEC Sample Questions**
Practice Exam	**GIAC GSEC Certification Practice Exam**

GSEC Syllabus:

Topic	Details
Access Control & Password Management	- The candidate will understand the fundamental theory of access control and the role of passwords in managing access control.
Active Defense	- The candidate will demonstrate a high-level understanding of what Active Defense is and the tools, methods, and techniques needed to utilize it effectively.
Contingency Plans	- The candidate will understand the critical aspect of contingency planning with a business continuity plan and disaster recovery plan
Critical Controls	- The candidate will understand the purpose, implementation, and background of the Critical Security Controls
Cryptography	- The candidate will have a basic understanding of the concepts of cryptography, including a high-level understanding of the major types of cryptosystems and steganography.
Cryptography Algorithms & Deployment	- The candidate will have a basic understand of the mathematical concepts that contribute to cryptography and identify commonly used symmetric, asymmetric, and hashing cryptosystems.
Cryptography Application	- The candidate will have a high-level understanding of the use, functionality, and operation of VPNs, GPG, and PKI
Defense in Depth	- The candidate will understand what defense in depth is and an identify the key areas of security and demonstrate the different strategies for implementing effective security within an organization.
Defensible Network Architecture	- The candidate will demonstrate how to architect a network to be monitored and controlled to resist intrusion.
Endpoint Security	- The candidate will demonstrate a basic understanding of the function and uses of endpoint security devices, such as endpoint firewalls, HIDS, and HIPS
Enforcing Windows Security Policy	- The candidate will have a high-level understanding of the features of Group Policy and working with INF security templates
Incident Handling & Response	- The candidate will understand the concepts of incident handling and the processes pertaining to incident handling.
IT Risk Management	- The candidate will understand the terminology and approaches to cyber security risk management including

Topic	Details
	identification of the steps of the Threat Assessment process
Linux Security: Structure, Permissions and Access	- The candidate will demonstrate understanding of a variety of Linux operating systems, including mobile systems, to better understand how to configure and secure Linux.
Linux Services: Hardening and Securing	- The candidate will demonstrate an ability to gain visibility into a Linux system to be able to secure and harden the system.
Linux: Monitoring and Attack Detection	- The candidate will demonstrate an understanding of the use of system baselines, log files, and other tools common to Linux operating systems in order to better monitor systems for signs of attack.
Linux: Security Utilities	- The candidate will demonstrate an understanding of how to use key security utilities and tools that are available for Linux systems to enhance system security.
Log Management & SIEM	- The candidate will demonstrate a high-level understanding of the importance of logging, the setup and configuration of logging, and log analysis with the assistance of SIEMs
Malicious Code & Exploit Mitigation	- The candidate will understand important attack methods and basic defensive strategies to mitigate those threats.
Network Device Security	- The candidate will have a basic understanding of the risks of network devices and how to secure them.
Network Security Devices	- The candidate will demonstrate a basic understanding of the function and uses of network security devices, such as, firewalls, NIDS, and NIPS
Networking & Protocols	- The candidate will demonstrate an understanding of the properties and functions of network protocols and network protocol stacks.
Securing Windows Network Services	- The candidate will know how to take basic measures in securing Windows network services such as IPSec, IIS, and Remote Desktop Services
Security Policy	- The candidate will understand the purpose and components of policy.
Virtualization and Cloud Security	- The candidate will have a basic understanding of the risks of virtualization and cloud services and how to secure them.
Vulnerability Scanning and Penetration Testing	- The candidate will demonstrate an understanding of the concepts and relationship behind reconnaissance, resource protection, risks, threats, and vulnerabilities including

Topic	Details
	preliminary abilities to create network maps and perform penetration testing techniques
Web Communication Security	- The candidate will demonstrate an understanding of web application security and common vulnerabilities including CGI, cookies, SSL and active content.
Windows Access Controls	- The candidate will understand how permissions are applied in the Windows NT File System, Shared Folders, Printers, Registry Keys, and Active Directory, and how Privileges are applied
Windows as a Service	- The candidate will understand how to manage updates for a network of Windows hosts.
Windows Automation, Auditing, and Forensics	- The candidate will be introduced to the techniques and technologies used to audit Windows hosts.
Windows Security Infrastructure	- The candidate will identify the differences between types of Windows OSes and how Windows manages groups and accounts, locally and with Active Directory and Group Policy
Wireless Network Security	- The candidate will have a basic understanding of the misconceptions and risks of wireless networks and how to secure them.

GIAC GSEC Sample Questions:

Question: 1

With regard to defense-in-depth, which of the following statements about network design principles is correct?

a) A secure network design requires that systems that have access to the Internet should not be accessible from the Internet and that systems accessible from the Internet should not have access to the Internet.
b) A secure network design requires that networks utilize VLAN (Virtual LAN) implementations to insure that private and semi-public systems are unable to reach each other without going through a firewall.
c) A secure network design will seek to provide an effective administrative structure by providing a single choke-point for the network from which all security controls and restrictions will be enforced.
d) A secure network design will seek to separate resources by providing a security boundary between systems that have different network security requirements.

Answer: d

Question: 2

There are three key factors in selecting a biometric mechanism. What are they?

a) Reliability, encryption strength, and cost
b) Encryption strength, authorization method, and cost
c) Reliability, user acceptance, and cost
d) User acceptance, encryption strength, and cost

Answer: c

Question: 3

Which of the following is an advantage of an Intrusion Detection System?

a) It is a mature technology.
b) It is the best network security.
c) It never needs patching.
d) It is a firewall replacement.

Answer: a

Question: 4

How many bytes does it take to represent the hexadecimal value OxFEDCBA?

a) 12
b) 2
c) 3
d) 6

Answer: c

Question: 5

Which of the following is an advantage of private circuits versus VPNs?

a) Flexibility
b) Performance guarantees
c) Cost
d) Time required to implement

Answer: b

Question: 6

At what point in the Incident Handling process should an organization determine its approach to notifying law enforcement?

a) When performing analysis
b) When preparing policy
c) When recovering from the incident
d) When reacting to an incident

Answer: b

Question: 7

In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

a) Discrete
b) Reporting
c) Promiscuous
d) Alert

Answer: c

Question: 8

What is the maximum passphrase length in Windows 2000/XP/2003?

a) 255 characters
b) 127 characters
c) 95 characters
d) 63 characters

Answer: b

Question: 9

Regarding the UDP header below, what is the length in bytes of the UDP datagrarm?

04 1a 00 a1 00 55 db 51

a) 161
b) 81
c) 219
d) 85

Answer: d

Question: 10

Which type of risk assessment results are typically categorized as low, medium, or high-risk events?

a) Technical
b) Qualitative
c) Management
d) Quantitative

Answer: b

Study Guide to Crack GIAC GSEC Exam:

- Getting details of the GSEC syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GSEC exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GSEC exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GSEC sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GSEC practice tests is must. Continuous practice will make you an expert in all syllabus areas.