EDUSUM

#1 Online Certification Guide

GIAC GCED

GIAC Certified Enterprise Defender Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCED

GIAC Certified Enterprise Defender (GCED)

115 Questions Exam – 69% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GCED Certification Well:

The GCED is best suitable for candidates who want to gain knowledge in the GIAC Cybersecurity and IT Essentials. Before you start your GCED preparation you may struggle to get all the crucial GIAC Certified Enterprise Defender materials like GCED syllabus, sample questions, study guide.

But don't worry the GCED 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 GCED syllabus?
- How many questions are there in the GCED exam?
- Which Practice test would help me to pass the GCED exam at the first attempt?

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

GCED GIAC Certified Enterprise Defender Certification Details:

Exam Name	GIAC Certified Enterprise Defender (GCED)
Exam Code	GCED
Exam Price	$949 (USD)
Duration	180 mins
Number of Questions	115
Passing Score	69%
Books / Training	**SEC501: Advanced Security Essentials - Enterprise Defender**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCED Sample Questions**
Practice Exam	**GIAC GCED Certification Practice Exam**

GCED Syllabus:

Topic	Details
Defending Network Protocols	- The candidate will demonstrate an understanding of commonly-used network protocols and how to defend against protocol attacks. The candidate will demonstrate knowledge of audit techniques and the Center for Internet Security's benchmarks and Critical Security Controls.
Defensive Infrastructure and Tactics	- The candidate will demonstrate basic knowledge of network and cloud-based infrastructure defensive measures, including common detective and preventive controls.
Digital Forensics Concepts and Application	- The candidate will demonstrate an understanding of methods and practices of digital forensics. The candidate will demonstrate proficiency in identification of forensic artifacts.
Incident Response Concepts and Application	- The candidate will demonstrate an understanding of continuous incident response processes, and their relationship to threat intelligence practices and the Cyber Kill Chain.
Interactive and Manual Malware Analyses	- The candidate will demonstrate an understanding of interactive malware behavior analysis, knowledge of analysis tools, and ability to interpret the analysis results. The candidate will demonstrate an understanding of manual malware code reversal, disassembly and decompiling, and of code obfuscation techniques used by malware.
Intrusion Detection and Packet Analysis	- The candidate will demonstrate an understanding of intrusion prevention systems, their placement in the enterprise, and their configuration and tuning. The candidate will demonstrate proficiency in taking action in response to alerts.
Malware Analysis Concepts and Basic Analysis Techniques	- The candidate will demonstrate an understanding of the various types of malware, identify symptoms of infection, and methods to analyze malware safely. The candidate will demonstrate an understanding of the benefits and disadvantages of automated and static malware analysis techniques, and to interpret their results.
Network Forensics, Logging, and Event Management	- The candidate will demonstrate an understanding of using logs and flows in network forensics, the importance of logging and event management in security operations,

Topic	Details
	and the usage of a SIEM and Security Analytics.
Network Security Monitoring Concepts and Application	- The candidate will demonstrate knowledge of devices that are used in SOCs to monitor networks, their understanding of packet types, packet capture tools, the practice of continuous network monitoring, and advanced issues such as monitoring encrypted traffic.
Penetration Testing Application	- The candidate will demonstrate familiarity and proficiency using penetration testing tactics and tools against typical types of penetration test targets.
Penetration Testing Concepts	- The candidate will demonstrate knowledge of penetration testing scoping, rules of engagement, the tools and tactics used in penetration tests, and reporting test results to the intended audience.

GIAC GCED Sample Questions:

Question: 1

At the start of an investigation on a Windows system, the lead handler executes the following commands after inserting a USB drive. What is the purpose of this command?

C:\ >dir / s / a dhsra d: \ > a: \ IRCD.txt

a) To create a file on the USB drive that contains a listing of the C: drive
b) To show hidden and archived files on the C: drive and copy them to the USB drive
c) To copy a forensic image of the local C: drive onto the USB drive
d) To compare a list of known good hashes on the USB drive to files on the local C: drive

Answer: c

Question: 2

When analyzing network flows, a sudden and unexplained increase in the number of outgoing _____ connections might indicate a security breach.

a) Outbound
b) Intranet
c) Wireless
d) Peripheral

Answer: a

Question: 3

What is the primary goal of "containment" in incident response?

a) Eradicate the attacker from the network
b) Monitor the attacker's activities for future intelligence
c) Inform the public about the incident
d) Isolate the affected systems to prevent further damage

Answer: d

Question: 4

Why might an administrator not be able to delete a file using the Windows del command without specifying additional command line switches?

a) Because it has the read-only attribute set
b) Because it is encrypted
c) Because it has the nodel attribute set
d) Because it is an executable file

Answer: a

Question: 5

_____ logs provide information about system and application errors, which can be valuable for diagnosing issues or identifying security incidents.

a) System
b) Traffic
c) Billing
d) Access

Answer: a

Question: 6

Which of the following is a key advantage of disassembling malware code?

a) It helps to remove the malware from the system
b) It provides insights into the malware's behavior and functionality
c) It prevents the malware from executing
d) It encrypts the malware code

Answer: b

Question: 7

During interactive malware analysis, what is the purpose of a sandbox environment?

a) To remove the malware from the system
b) To execute the malware and observe its behavior in a controlled environment
c) To disassemble the malware code
d) To patch vulnerabilities in the malware

Answer: b

Question: 8

In penetration testing, what is the primary purpose of "pivoting"?

a) To infiltrate the target organization's management team
b) To move from one compromised system to others within the network
c) To report findings to the client
d) To perform vulnerability scanning

Answer: b

Question: 9

What does manual malware code reversal involve?

a) Executing malware in a sandbox environment
b) Running malware in a virtual machine
c) Analyzing malware behavior in real-time
d) Decompiling malware code to its original source code

Answer: d

Question: 10

In cloud-based infrastructure, what is the main responsibility of a Cloud Access Security Broker (CASB)?

a) Managing network traffic
b) Monitoring user activity
c) Securing cloud applications and data
d) Providing network connectivity

Answer: c

Study Guide to Crack GIAC Certified Enterprise Defender GCED Exam:

- Getting details of the GCED 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 GCED 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 GCED 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 GCED 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 GCED practice tests is must. Continuous practice will make you an expert in all syllabus areas.