EDUSUM

#1 Online Certification Guide

GIAC GEVA

GIAC Enterprise Vulnerability Assessor Certification Questions & Answers

Exam Summary – Syllabus –Questions

GEVA

GIAC Enterprise Vulnerability Assessor Certification (GEVA)

75 Questions Exam – 71% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GEVA Certification Well:

The GEVA is best suitable for candidates who want to gain knowledge in the GIAC Offensive Operations, Pen Testing, and Red Teaming. Before you start your GEVA preparation you may struggle to get all the crucial GIAC Enterprise Vulnerability Assessor materials like GEVA syllabus, sample questions, study guide.

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

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

GEVA GIAC Enterprise Vulnerability Assessor Certification Details:

Exam Name	GIAC Enterprise Vulnerability Assessor (GEVA)
Exam Code	GEVA
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	71%
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GEVA Sample Questions**
Practice Exam	**GIAC GEVA Certification Practice Exam**

GEVA Syllabus:

Topic	Details
Application and Configuration Discovery	- The candidate will demonstrate understanding of scanning and discovery techniques to find application and configuration vulnerabilities.
Authentication and Configuration Auditing	- The candidate will demonstrate understanding of validating vulnerabilities specific to authentication systems and host/service configurations.
Data Management and Collaboration Strategies	- The candidate will demonstrate understanding of vulnerability and configuration data management as well as team collaboration.
Intelligence and Threat Modeling	- The candidate will demonstrate understanding of performing and applying intelligence and threat modeling within a vulnerability assessment.
Network-based Discovery	- The candidate will demonstrate understanding of network-based scanning and discovery methods and techniques.
Reconnaissance, Scanning, and Vulnerability Fundamentals	- The candidate will demonstrate understanding of reconnaissance and scanning fundamentals.
Remediation Concepts and Vulnerability Assessment Reporting	- The candidate will demonstrate understanding of remediation concepts and vulnerability assessment reporting.
Validation and Risk Essentials	- The candidate will demonstrate understanding of essential risk methodologies and how these inform vulnerability validation.
Vulnerability Assessment Methodology	- The candidate will demonstrate understanding of the fundamental theories and process of planning and performing a vulnerability assessment.
Vulnerability Validation and Enumeration Fundamentals	- The candidate will demonstrate understanding of vulnerability validation techniques and value.

GIAC GEVA Sample Questions:

Question: 1

Which technique is most effective in the initial phase of vulnerability scanning?

a) Active network scanning
b) Passive network monitoring
c) Deep packet inspection
d) Log file analysis

Answer: a

Question: 2

During authentication auditing, which vulnerability is most crucial to identify?

a) SQL injection vulnerabilities
b) Weak encryption algorithms
c) Default credentials in use
d) Cross-site scripting vulnerabilities

Answer: c

Question: 3

How does threat modeling assist in the assessment of network vulnerabilities?

a) By providing a framework for incident response
b) Through identifying the most likely attack vectors
c) By determining the effectiveness of current security measures
d) Through assessing the physical security of network infrastructure

Answer: b

Question: 4

In a collaborative vulnerability assessment environment, what is the most significant advantage of using shared tools and platforms?

a) Reducing the overall cost of security tools
b) Ensuring uniformity in data analysis
c) Promoting faster decision-making processes
d) Enhancing the efficiency of team communication

Answer: d

Question: 5

In authentication auditing, what advanced technique is used to detect evasion of multi-factor authentication systems?

a) Behavioral biometrics analysis
b) Deep packet inspection
c) Encrypted traffic analysis
d) AI-based anomaly detection

Answer: d

Question: 6

In the context of data management and collaboration strategies during a vulnerability assessment, what is the primary benefit of using a centralized vulnerability database?

a) Reducing the need for manual data entry
b) Facilitating automated patch deployment
c) Enhancing communication and data sharing among team members
d) Allowing for real-time threat intelligence updates

Answer: c

Question: 7

What advanced technique in reconnaissance involves analyzing DNS records for historical data and potential vulnerabilities?

a) DNS footprinting
b) DNS tunneling
c) Reverse DNS lookup
d) DNS cache snooping

Answer: a

Question: 8

What complex risk assessment technique involves quantitative analysis to estimate potential losses from identified vulnerabilities?

a) Threat hunting
b) Monte Carlo simulations
c) Attack surface analysis
d) Advanced persistent threat modeling

Answer: b

Question: 9

Which of the following best describes the role of a 'Vulnerability Assessment Framework' in an enterprise environment?

a) To define the scope and frequency of vulnerability assessments
b) To provide a detailed list of known vulnerabilities
c) To outline the response plan for security breaches
d) To catalog software and hardware assets in the network

Answer: a

Question: 10

When discovering configuration vulnerabilities, which aspect is most crucial to check?

a) Network throughput and performance
b) Compliance with industry security standards
c) Frequency of software updates
d) End-user accessibility and usability

Answer: b

Study Guide to Crack GIAC Enterprise Vulnerability Assessor GEVA Exam:

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