EDUSUM

#1 Online Certification Guide

GIAC GDAT

GIAC Defending Advanced Threats Certification Questions & Answers

Exam Summary – Syllabus –Questions

GDAT

GIAC Defending Advanced Threats

75 Questions Exam – 70% Cut Score – Duration of 120 minutes

Table of Contents:

Know Your GDAT Certification Well:

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

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

Passing the GDAT exam makes you GIAC Defending Advanced Threats. Having the GIAC Defending Advanced Threats certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GDAT GIAC Defending Advanced Threats Certification Details:

Exam Name	GIAC Defending Advanced Threats (GDAT)
Exam Code	GDAT
Exam Price	$979 (USD)
Duration	120 mins
Number of Questions	75
Passing Score	70%
Books / Training	**SEC599: Defeating Advanced Adversaries - Purple Team Tactics & Kill Chain Defenses**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GDAT Sample Questions**
Practice Exam	**GIAC GDAT Certification Practice Exam**

GDAT Syllabus:

Topic	Details
Active Directory/Domains	- The candidate will demonstrate knowledge of the following domain topics as they relate to information security: Authentication basics, kerberos, common attacks against domains, and detecting attacks against domains.
Administrative Access	- The candidate will exhibit a proficiency in topics related to the impacts of privilege escalation, and the importance of concepts related to "least privelege" methodologies.
Adversary Emulation	- The candidate will demonstrate knowledge of the following adversary emulation topics: Basic concepts, common tools used, and Key technical controls to consider.
Application Exploitation	- The candidate will be able to summarize how; combining the sofwtare development lifecycle with threat modeling, employing proper patch management strategies, and other exploit mitigation techniques can improve the security of an organization against application exploitation.
Data Exfiltration	- The candidate will be able to compare and contrast common exfil strategies, summarize strategies for detecting C2 channels, and discuss pros and cons of performing deception teqniques as a possible attack target.
Installation	- The candidate will be able to compare and contrast common persistaence strategies and how organizations can be protected against them.
Lateral Movement	- The candidate will be able to appraise different lateral movement strategies, as well as strategies and controls for detecting and preventing the successful execution of malicious payloads.
Payload Delivery	- The candidate will be able to appraise different payload delivery strategies, as well as strategies and controls focused on minimizing the likelihood of the successful delivery of malicious payloads.
Payload Execution	- The candidate will be able to appraise different payload execution strategies, as well as strategies and controls for detecting and preventing the successful execution of malicious payloads.

Topic	Details
Reconnaissance, Threat Handling, and Incident Response	- The candidate will exhibit a proficiency in the following exploitation topics: fundamental reconnaisance, threat hunting strategies, and the incident response process.

GIAC GDAT Sample Questions:

Question: 1

Regarding Kerberos authentication, which of the following steps are involved in the process of obtaining a service ticket?

a) The client requests an authentication ticket (TGT) from the Key Distribution Center (KDC).
b) The client presents the TGT to the Ticket Granting Server (TGS) to request a service ticket.
c) The client uses the service ticket to authenticate directly to the Active Directory database.
d) The Ticket Granting Server (TGS) issues a service ticket after validating the TGT.

Answer: b, d

Question: 2

An effective adversary emulation plan should include detailed _____ to ensure that all actions are reversible and non-disruptive to daily operations.

a) escalation procedures
b) rollback procedures
c) deployment strategies
d) communication plans

Answer: b

Question: 3

Which phase of the software development lifecycle is most critical for implementing security patches?

a) Requirements gathering
b) Design
c) Implementation
d) Maintenance

Answer: d

Question: 4

In the context of lateral movement, what is the function of using pass-the-ticket (PtT) techniques?

a) To escalate privileges on the target system
b) To maintain persistence in the network
c) To impersonate legitimate users
d) To encrypt data being exfiltrated

Answer: c

Question: 5

Why is regular vulnerability scanning crucial for application security?

a) It aligns IT strategies with business objectives
b) It identifies weaknesses that could be exploited by attackers
c) It ensures compliance with international standards
d) It facilitates faster software release cycles

Answer: b

Question: 6

What is the primary benefit of employing encryption in data exfiltration techniques?

a) It reduces the amount of data needing exfiltration
b) It ensures faster transfer of data
c) It masks the content from network monitoring tools
d) It complies with international data protection laws

Answer: c

Question: 7

What role does sandboxing play in defending against payload delivery?

a) It isolates potentially malicious programs in a separate environment from the host system.
b) It filters incoming network traffic to prevent unauthorized access.
c) It encrypts sensitive information stored on the device.
d) It logs user activities for audit purposes.

Answer: a

Question: 8

Which strategies are effective in preventing privilege escalation attacks?

a) Conducting regular privilege audits
b) Implementing strong password policies
c) Using non-administrative accounts for daily operations
d) Encrypting sensitive data at rest

Answer: a, c

Question: 9

How does application whitelisting help prevent the execution of malicious payloads?

a) By only allowing pre-approved applications to run
b) By detecting zero-day exploits
c) By encrypting data transmitted over the network
d) By monitoring outbound traffic for anomalies

Answer: a

Question: 10

What are key indicators of an effective exploit mitigation strategy?

a) Quick identification of new vulnerabilities
b) Immediate deployment of software patches
c) No reported security incidents
d) Regular security training for developers

Answer: a, b, d

Study Guide to Crack GIAC Defending Advanced Threats GDAT Exam:

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