SANS560 GIAC PENETRATION TESTER (GPEN) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sans560gpen.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. **When the db_nmap command is used, Metasploit invokes which tool for scanning?**

   A. Nessus

   B. OpenVAS

   C. NMAP

   D. Nikto

2. **Which Meterpreter command lists compatible webcams on the target machine?**

   A. Webcam_list

   B. Webcam_snap

   C. Record_mic

   D. Ipconfig

3. **George Santayana quote 'Those who cannot remember the past are condemned to repeat it' is attributed to which author?**

   A. George Santayana

   B. Albert Einstein

   C. Thomas Jefferson

   D. Leonardo da Vinci

4. **After exploitation, what factors determine the choice of file transfer methods?**

   A. Outbound protocols, installed software, and the exploit used

   B. User credentials only

   C. OS version only

   D. Bandwidth only

5. **LANMAN C/R and NTLMv1 use the same padding, splitting, and encrypting steps. What is different between them?**

   A. Only the final hash differs; padding/splitting/encrypting steps are the same.

   B. Padding length differs.

   C. They use different encryption algorithms.

   D. NTLMv1 uses MD5.

SAMPLE

6. Which action helps avoid third-party malicious activity during testing?

A. Run tests on a live production network

B. Patch, harden, and shut off unnecessary services prior to testing

C. Use default credentials

D. Ignore updates

7. Which statement best describes Metasploit payloads that reside in memory and disappear on reboot?

A. They run as a separate process on the target.

B. They write a persistent loader to disk.

C. They load as a DLL into the target process memory.

D. They reside in memory and disappear after reboot.

8. What is the purpose of db_connect and db_status in Metasploit's database integration?

A. db_connect and db_status

B. db_export and db_disconnect

C. db_driver and db_status

D. hosts and services

9. In Metasploit, which module can perform pass-the-hash authentication by using an administrator's hash for SMB login?

A. psexec

B. hashdump

C. smb_login

D. windows/gather/credentials

10. Which tool is well known for sniffing NTLM credentials on a Windows network and can crack hashes?

A. Wireshark

B. Nmap

C. Cain & Abel

D. Burp Suite

SAMPLE

Answers

SAMPLE

1. C
2. A
3. A
4. A
5. A
6. B
7. D
8. A
9. A
10. C

SAMPLE

Explanations

SAMPLE

1. When the db_nmap command is used, Metasploit invokes which tool for scanning?

A. Nessus

B. OpenVAS

C. NMAP

D. Nikto

db_nmap uses the Nmap scanner and imports the results into Metasploit's database. This wrapper lets you perform port, service, and OS/version discovery with Nmap and then access the findings directly in msfconsole for further actions. The other options are different tools: Nessus and OpenVAS are vulnerability scanners, while Nikto is a web server scanner. NMAP is the tool Metasploit integrates for this scanning, making it the correct choice.

2. Which Meterpreter command lists compatible webcams on the target machine?

A. Webcam_list

B. Webcam_snap

C. Record_mic

D. Ipconfig

Understanding how Meterpreter exposes webcam functionality helps you see why this command is the one that lists webcams. On a target, Meterpreter can access video capture devices through a webcam extension. To know what webcams are available, you need to enumerate the devices first. The command that does this queries the system for all video capture devices and returns a list of the webcams you can use, including their identifiers. This is essential before attempting to capture images or video, because those actions require selecting a specific device from the enumerated list. The other options serve different purposes: one takes a snapshot from a chosen webcam, another records audio from the microphone, and the last shows the target's IP configuration. They operate after you've identified which webcam exists, not for discovery itself.

3. George Santayana quote 'Those who cannot remember the past are condemned to repeat it' is attributed to which author?

A. George Santayana

B. Albert Einstein

C. Thomas Jefferson

D. Leonardo da Vinci

The idea being tested here is identifying the correct author of a well-known historical quote. This line is attributed to George Santayana, a Spanish-born American philosopher and writer, who expressed this thought about memory and learning from history in The Life of Reason, Volume I, Reason in Common Sense. The essence is that neglecting the lessons of the past leads people to repeat the same mistakes, so recognizing Santayana as the source fits the quote's meaning and historical context. Other famous figures are known for many sayings, but they did not coin this exact line, and misattributions around Einstein and others are common.

SAMPLE

4. After exploitation, what factors determine the choice of file transfer methods?

A. Outbound protocols, installed software, and the exploit used

B. User credentials only

C. OS version only

D. Bandwidth only

After you have a foothold, the feasible file transfer method is governed by what can actually be used from the compromised host. The first factor is the outbound channels the host can reach and that the network permits; if only web traffic is allowed or if FTP/SMB ports are blocked, that shapes which transfer methods are workable and stealthy. The second factor is what tools are installed on the host; having native utilities like curl, wget, certutil, PowerShell, or an SSH client opens different transfer options and paths that avoid introducing new software. The third factor is the exploit payload and how it runs on the target—what privileges you have, what memory or disk access is available, and whether the payload already includes a built in exfiltration capability or relies on a particular transfer channel. These together explain why a method using common outbound protocols, supported by available tools on the host, and aligned with the exploit's capabilities is chosen. Merely having user credentials isn't sufficient because the transfer path still needs an active channel and usable tooling. OS version alone doesn't determine what is possible, since it doesn't account for available tools or network restrictions. Bandwidth matters, but without the right channel and tools, high bandwidth won't help.

5. LANMAN C/R and NTLMv1 use the same padding, splitting, and encrypting steps. What is different between them?

A. Only the final hash differs; padding/splitting/encrypting steps are the same.

B. Padding length differs.

C. They use different encryption algorithms.

D. NTLMv1 uses MD5.

The idea being tested is that LANMAN (LM) and NTLMv1 share the same DES-based challenge-response mechanism, but they differ in what value is fed into that mechanism, which changes the final output. In LM, you take the password, convert it to uppercase, pad or truncate it to 14 bytes, split that into two 7-byte pieces, turn each into a DES key, and DES-encrypt the server challenge with each key. The two 8-byte results are concatenated to form a 16-byte LM response. In NTLMv1, you first compute the NTLM hash by applying MD4 to the Unicode password, producing a 16-byte value. You then split this 16-byte hash into three 7-byte pieces (padding the last piece as needed), convert those into three DES keys, and DES-encrypt the server challenge with each key. The three results are concatenated to yield a 24-byte NTLMv1 response. So the same padding/splitting/encrypting steps are used, but the input material and thus the final hash differ, giving a different length and content. NTLMv1 relies on the MD4-hashed password, not MD5, and the final output is 24 bytes rather than 16.

SAMPLE

6. Which action helps avoid third-party malicious activity during testing?

A. Run tests on a live production network

B. Patch, harden, and shut off unnecessary services prior to testing

C. Use default credentials

D. Ignore updates

Hardening and patching before testing reduces the attack surface and minimizes the chance that a third party could exploit your activities. Patching closes known vulnerabilities, hardening removes or reduces unnecessary services and configurations, and shutting off services that aren't needed prevents extra entry points. Together, these steps make the testing environment more secure and less inviting for third-party malicious activity, while also reducing the risk of disrupting production or exposing data. Running tests on a live production network risks impacting users and leaking sensitive information if anything goes wrong. Using default credentials creates easily guessable access that malicious actors can exploit. Ignoring updates leaves known vulnerabilities unpatched, creating opportunities for misuse.

7. Which statement best describes Metasploit payloads that reside in memory and disappear on reboot?

A. They run as a separate process on the target.

B. They write a persistent loader to disk.

C. They load as a DLL into the target process memory.

D. They reside in memory and disappear after reboot.

Memory-resident, non-persistent payloads are loaded into the target's RAM and do not write artifacts to disk. Because nothing is stored on disk and memory is cleared on reboot, the payload vanishes after the system restarts. It may execute in memory as a separate process or be injected into another process, but its defining trait is that it does not persist across reboots. Options that imply writing to disk or creating a persistent loader would leave traces or survive reboot, which is not the behavior described.

8. What is the purpose of db_connect and db_status in Metasploit's database integration?

A. db_connect and db_status

B. db_export and db_disconnect

C. db_driver and db_status

D. hosts and services

Managing the database in Metasploit: db_connect sets up the connection between the Metasploit console and the backend database (the one used to store hosts, services, credentials, notes, etc.), enabling persistence of data across sessions. db_status then shows whether that connection is active and provides details about the connection (such as database type, host, port, database name, and user), helping you verify and troubleshoot the database integration. Other options listed either perform different actions (exporting data, disconnecting, selecting a driver, or listing data like hosts/services) and thus don't solve the same purpose as these two commands.

SAMPLE

9. In Metasploit, which module can perform pass-the-hash authentication by using an administrator's hash for SMB login?

A. psexec

B. hashdump

C. smb_login

D. windows/gather/credentials

Pass-the-hash authentication uses an NTLM hash to prove identity to Windows services (like SMB) without needing the plaintext password. For performing remote command execution over SMB using a hash in Metasploit, the module that fits this purpose is the psexec module. It connects to the target via SMB (often through the admin$ share) and runs the payload using the provided credentials, which can be an administrator's NTLM hash instead of a cleartext password. This makes it the best fit for logins authenticated with a hash and immediate remote execution. Hashdump is used after you have access to dump password hashes from the target; smb_login is for testing login viability against an SMB service and doesn't provide the remote execution flow with a hash; windows/gather/credentials collects credentials but isn't focused on performing pass-the-hash authentication for SMB login.

10. Which tool is well known for sniffing NTLM credentials on a Windows network and can crack hashes?

A. Wireshark

B. Nmap

C. Cain & Abel

D. Burp Suite

NTLM credentials on a Windows network can be captured and cracked using specialized tools; Cain & Abel stands out as it combines network sniffing of credentials with hash cracking capabilities. It can perform ARP poisoning to place itself on the same network segment and capture NTLM handshake traffic, which often includes NTLM hashes. Once captured, those hashes can be cracked using built-in password-cracking features, making it possible to recover plaintext passwords. This dual capability—intercepting credentials from traffic and then cracking the hashes—makes Cain & Abel particularly well known for this purpose. Wireshark, while excellent for capturing and analyzing network traffic, doesn't include hash cracking features; you'd need separate tools to crack anything you capture. Nmap is a network discovery and vulnerability scanning tool, not designed to sniff credentials or crack hashes. Burp Suite focuses on web application security testing and does not target Windows network NTLM sniffing or crack NTLM hashes.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://sans560gpen.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE