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

Table of Contents

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.

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!

Questions

1. **Which command shows the Windows firewall settings, including all profiles?**

   A. netsh firewall show allprofiles

   B. netsh advfirewall show currentprofile

   C. netsh firewall show allprofiles

   D. netsh advfirewall show allprofiles

2. **Which practice improves PowerShell usability by shortening flags?**

   A. Command flag shortening

   B. Tab Autocomplete

   C. Profile scripts

   D. Verbose output

3. **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

4. **What does the related: directive show?**

   A. Pages that have similar content and links to the searched page

   B. Pages within the same directory

   C. Terms in the URL

   D. The site's robots.txt

5. **What should you verify with administrators about lockout during testing?**

   A. Whether account lockout is utilized on the target network.

   B. The color of their terminal wallpaper.

   C. The exact hardware vendor in use.

   D. The network's DNS primary server.

6. If a target machine sends back RESETs or ICMP Port Unreachable, what happens?

A. The results will be encrypted

B. The scan will be unable to proceed

C. The target is immune

D. The scan can occur more quickly because we don't have to wait for a timeout

7. Which force concerns how easily suppliers can influence prices, considering product uniqueness and supplier power?

A. Power Of Suppliers

B. Power Of Customers

C. Threats of New Entrants

D. Competitive Rivalry

8. Findings are typically categorized into which severity levels?

A. High/Medium/Low

B. Critical/High/Medium/Low

C. Very High/High/Low

D. Informational/Low/High

9. For NMAP OS fingerprinting, which networking field is commonly analyzed to help determine the target's OS in the 2nd Gen tests?

A. TTL value changes

B. Window size changes

C. SYN sequence patterns

D. IP ID value changes

10. Which command directs traffic from a target subnet through a Meterpreter session to another victim?

A. msf route

B. meterpreter route

C. pivot route

D. route

Answers

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

Explanations

1. Which command shows the Windows firewall settings, including all profiles?

A. netsh firewall show allprofiles

B. netsh advfirewall show currentprofile

C. netsh firewall show allprofiles

D. netsh advfirewall show allprofiles

To view Windows Firewall settings for every network profile, you need the Advanced Firewall context and request all profiles in one command. The correct command is netsh advfirewall show allprofiles. The advfirewall namespace is the modern interface for Windows Firewall with Advanced Security, and show allprofiles returns the settings for Domain, Private, and Public profiles in one view, giving a complete picture of how the firewall is configured across all contexts. The other options use older or incorrect syntax—netsh firewall is deprecated on newer Windows versions, and showing the current profile only returns just the active profile, not all of them.

2. Which practice improves PowerShell usability by shortening flags?

A. Command flag shortening

B. Tab Autocomplete

C. Profile scripts

D. Verbose output

PowerShell can accept shortened, unambiguous parameter names, so you can type a shorter flag instead of the full parameter name. This directly speeds how you specify options because the shell will bind to the intended parameter as long as the prefix you type uniquely identifies it. For example, if a cmdlet has a parameter named Recurse, you can often use Rec as long as no other parameter starts with Rec, and PowerShell will treat it as -Recurse. This reduces keystrokes and friction when building commands, which is exactly what shortening flags aims to achieve. Tab Autocomplete helps you type faster by filling in the rest after you start typing, but it's a broader usability aid rather than shortening the flag itself. Profile scripts and verbose output don't address shortening the flags you type.

3. 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.

4. What does the related: directive show?

A. Pages that have similar content and links to the searched page

B. Pages within the same directory

C. Terms in the URL

D. The site's robots.txt

The related: operator is a search tool that returns pages Google considers connected to a given page. It bases this on how similar the content is and how pages link to or from the target page. So it's about finding pages with similar topics and/or pages that are linked to the searched page, not about being in the same directory, nor about terms in the URL, nor about the site's robots.txt.

5. What should you verify with administrators about lockout during testing?

A. Whether account lockout is utilized on the target network.

B. The color of their terminal wallpaper.

C. The exact hardware vendor in use.

D. The network's DNS primary server.

Understanding whether account lockout is in place and how it works is essential when testing authentication. Verifying this with administrators helps you avoid unintentionally locking out real users and ensures you stay within authorized, safe boundaries. You want to know if the system enforces a lockout after a certain number of failed logins, the exact threshold, how long the lockout lasts, and how the counter resets. Also clarify any exemptions for privileged or service accounts, whether there are maintenance windows or special rules, and the approved procedure if a lockout occurs during testing. It's important to align on whether temporary disabling, targeted testing windows, or active monitoring is permitted, and to have written authorization in place. The other options listed aren't related to login security and wouldn't help you manage lockout risk.

6. If a target machine sends back RESETs or ICMP Port Unreachable, what happens?

A. The results will be encrypted

B. The scan will be unable to proceed

C. The target is immune

D. The scan can occur more quickly because we don't have to wait for a timeout

When probing ports, you rely on responses to determine state. A TCP reset means the port is closed, and an ICMP Port Unreachable from a UDP probe also indicates a closed port. These definitive replies tell you immediately that the port isn't open, so you don't have to wait for a timeout to conclude its state. That lets the scan move on faster, reducing overall time. The other options don't fit because a reset or ICMP unreachable doesn't encrypt results, doesn't make the scan unable to proceed, and doesn't imply immunity—just a closed port. The key benefit here is the ability to skip waiting for timeouts when a definitive negative response is received.

7. Which force concerns how easily suppliers can influence prices, considering product uniqueness and supplier power?

A. Power Of Suppliers

B. Power Of Customers

C. Threats of New Entrants

D. Competitive Rivalry

Power of suppliers focuses on how much leverage suppliers have to influence the price and terms for the inputs a company needs. When the inputs are unique or highly differentiated and there are few alternative sources, suppliers can command higher prices and more favorable terms because buyers can't easily switch. This situation directly describes why suppliers' ability to influence prices matters in this context. In contrast, buyer power looks at how much customers can push prices down, threats of new entrants deal with barriers to entry, and competitive rivalry covers pricing/struggle among existing firms. So the force described here is Power of Suppliers.

8. Findings are typically categorized into which severity levels?

A. High/Medium/Low

B. Critical/High/Medium/Low

C. Very High/High/Low

D. Informational/Low/High

Severity levels in findings are used to prioritize remediation by impact. In most pen test reporting, the standard triad is High, Medium, and Low. This three-level scale provides clear urgency without overcomplicating triage, matching how teams typically categorize and respond to issues. The option that uses High/Medium/Low fits this widely used scheme. The other options introduce an extra level such as Critical or Very High, which isn't part of the basic triage, or include Informational, which isn't a severity that drives remediation priority. Hence, High/Medium/Low is the best match.

9. For NMAP OS fingerprinting, which networking field is commonly analyzed to help determine the target's OS in the 2nd Gen tests?

A. TTL value changes

B. Window size changes

C. SYN sequence patterns

D. IP ID value changes

In second-generation OS fingerprinting, the pattern of how the IP identification field (IP ID) changes in responses is key. Different operating systems and their TCP/IP stacks generate IP IDs in characteristic ways—some increment them predictably, others use distinct sequences or patterns. By sending probes and observing how the IP ID value in replies evolves, Nmap can distinguish between OS families more reliably than with fields that are more easily altered by routers or network conditions. While TTL, window size, and SYN sequence patterns can also provide clues, they are more susceptible to path effects or kernel tuning, making IP ID behavior a particularly useful discriminator in these tests.

10. Which command directs traffic from a target subnet through a Meterpreter session to another victim?

A. msf route

B. meterpreter route

C. pivot route

D. route

Pivoting traffic through a compromised host relies on telling Metasploit which subnet should be reached via the existing Meterpreter session. The command you use to set that up is the msf route command in the console, which adds a routing entry that directs all traffic for the specified target network through the chosen Meterpreter session. Once this route is in place, modules and tools inside Metasploit will send packets for that subnet via the pivot, enabling you to reach additional hosts behind the compromised machine. This is how you extend access from one victim to others in the same network. The other options don't represent the standard way to configure this routing in Metasploit. They don't reflect the actual Metasploit command used to manage pivot routes, whereas the msf route command encapsulates this routing capability.

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!