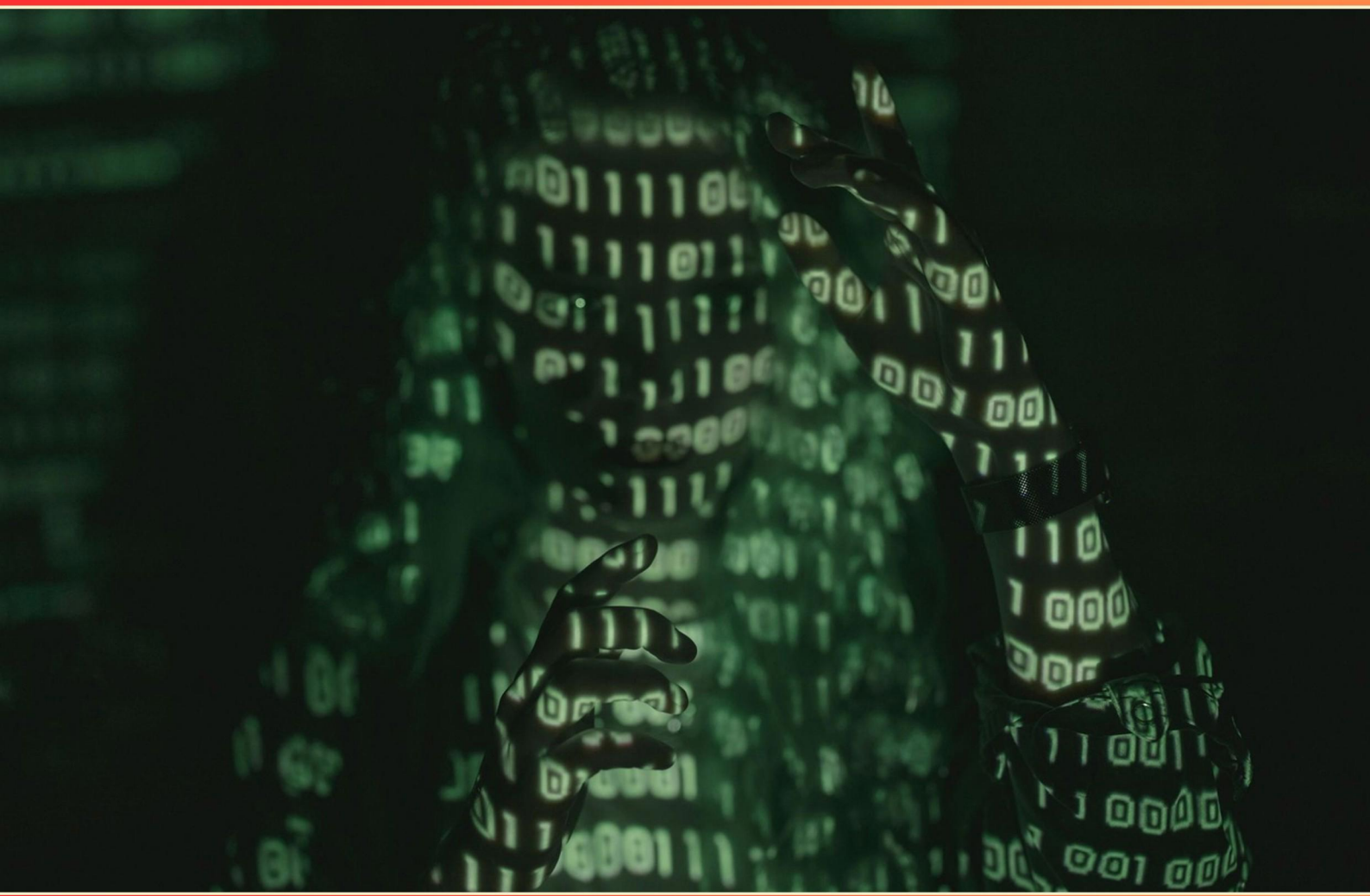
NMAP/ZENMAP SWITCHES PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://nmapzenmapswitches.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. What is the effect of --min-rate and --max-rate on scan throughput, and why would you adjust them?

A. They only affect output formatting.

B. They set timing templates.

C. They limit the number of hosts in a session.

D. They constrain the probe rate; --min-rate enforces minimum packets/second, --max-rate caps the rate; adjust to balance speed, reliability, and stealth.

2. Which timing template corresponds to Paranoid (0) IDS evasion?

A. -T3

B. -T1

C. -T0

D. -oX

3. Which option allows Nmap to read targets from a file to scan?

A. -iL

B. --exclude

C. --traceroute

D. --open

4. Which option enables operating system detection in Nmap?

A. -S enables OS detection.

B. -O enables OS detection.

C. -6 enables OS detection.

D. -p enables OS detection.

5. Which of the following is a typical drawback of OS detection with -O?

A. It may require privileged access.

B. It may be unreliable behind firewalls, NAT, or IDS.

C. It always produces perfect results.

D. It requires physical access to the device.

SAMPLE

6. DNS Scan aka List Scan: Which scan is used to list IPs for all listed subnets on the command line?

A. -sN

B. -sI

C. -sA

D. -sL

7. What is the initial action of a UDP port scan?

A. Sent UDP Packet to every port

B. -sU

C. Open Response: A service responds with a UDP packet

D. Close Response: ICMP port unreachable

8. Which syntax scans ports that are in the nmap-services list below a threshold?

A. -p 1-1024

B. -p [1024]

C. -p [-1024]

D. -p 0-1024

9. Which of the following correctly pairs an NSE script category with a typical use?

A. Discovery: host discovery; Safe: non-intrusive checks like http-title; Intrusive: vulnerability checks; Brute-force is another category used for credential guessing.

B. Brute-force is another NSE script category used for credential guessing.

C. Discovery: host discovery; Safe: vulnerability checks; Intrusive: OS fingerprinting; Brute-force: port scanning

D. Discovery: DNS resolution; Safe: port scanning; Intrusive: banner grabbing; Brute-force

10. Which option performs a TCP connect scan?

A. -sN

B. -sL

C. -sX

D. -sT

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the effect of --min-rate and --max-rate on scan throughput, and why would you adjust them?

A. They only affect output formatting.

B. They set timing templates.

C. They limit the number of hosts in a session.

D. They constrain the probe rate; --min-rate enforces minimum packets/second, --max-rate caps the rate; adjust to balance speed, reliability, and stealth.

The main idea here is how you control scan throughput by limiting how fast probes are sent. The switches --min-rate and --max-rate actually bound the probe rate during a scan. The minimum rate sets a floor, ensuring Nmap keeps sending probes at or above a certain packets-per-second level, which can help keep progress steady in noisy or slow networks. The maximum rate sets a ceiling, preventing the scan from overwhelming the network, flooding targets, or triggering defensive systems, which improves reliability and stealth. Because of that balance, you adjust them to trade speed for reliability and stealth. In a controlled, fast network you might push the max rate higher to finish quickly; in congested networks or when you want to be gentler on the target or less conspicuous, you lower the max rate. The min rate is useful to avoid scans that stall or become unreasonably slow in environments that drop or delay packets. These options don't affect how output is formatted, they don't set timing templates, and they don't limit how many hosts are included in a session. They are all about controlling how aggressively probes are sent to achieve a usable balance of speed, reliability, and stealth.

2. Which timing template corresponds to Paranoid (0) IDS evasion?

A. -T3

B. -T1

C. -T0

D. -oX

Timing templates in Nmap control how fast probes are sent and how much stealth is built into the scan. Paranoid is the slowest setting, designed to evade IDS by inserting long delays between probes and making traffic look like background noise. That's why Paranoid (0) IDS evasion uses the option -T0. The other templates map to faster or less stealthy modes: -T3 is the normal/default speed, -T1 is a sneaky but still slower-than-default mode, and -oX is not a timing template at all but an XML output option.

3. Which option allows Nmap to read targets from a file to scan?

A. -iL

B. --exclude

C. --traceroute

D. --open

Target lists from a file are read using the -iL option. This tells Nmap to take its targets from the specified file, with one host or range per line, which is especially useful when scanning many targets. For example: nmap -iL targets.txt. The other options serve different purposes: --exclude omits specified targets from the scan; --traceroute performs a traceroute to map the route to hosts; and --open filters results to show only hosts with open ports. None of these change how targets are read from input.

SAMPLE

4. Which option enables operating system detection in Nmap?

A. -S enables OS detection.

B. -O enables OS detection.

C. -6 enables OS detection.

D. -p enables OS detection.

OS detection in Nmap is activated by the -O option. This flag tells Nmap to perform fingerprinting of the target's operating system by sending a set of probes and analyzing the responses against its OS database. That direct enablement is why it's the best choice. The other flags don't turn on OS detection: -S sets the source address (useful for spoofing), -6 switches to IPv6 mode, and -p selects which ports to scan. For broader reconnaissance, OS detection can be combined with other checks (for example, -sV for version detection or -A for an aggressive scan that includes OS and version detection).

5. Which of the following is a typical drawback of OS detection with -O?

A. It may require privileged access.

B. It may be unreliable behind firewalls, NAT, or IDS.

C. It always produces perfect results.

D. It requires physical access to the device.

OS detection with -O works by sending a variety of probes and comparing the host's replies to a fingerprint database. The typical drawback is that network devices in the path—firewalls, NATs, and IDSs—can interfere with those probes, block or alter responses, and mask the true characteristics of the target's TCP/IP stack. This can make fingerprints unreliable, leading to incorrect OS guesses or no result at all. Other options aren't the main issue in practice: while privileged access is often required to send raw packets, that's a setup constraint rather than a reliability problem; OS detection isn't guaranteed to be perfect in all cases, but saying it always is ignores real-world noise; and you don't need physical access to perform remote OS detection.

6. DNS Scan aka List Scan: Which scan is used to list IPs for all listed subnets on the command line?

A. -sN

B. -sI

C. -sA

D. -sL

List Scan is the mode that expands every target you specify into individual IP addresses and prints them without sending any packets. That's why it's used to list all the IPs within the subnets you provide on the command line. It effectively reveals what would be scanned, without performing any probing. You can opt to show hostnames by enabling DNS resolution (for example with reverse DNS) or keep just the IPs by disabling resolution. In contrast, the other scan types actually send probes to discover open ports or map firewall rules, rather than just listing targets. For example, one of them sends a TCP packet with no flags, another uses a zombie host to perform probing, and another checks firewall behavior by sending ACK packets. So the option that lists every target address from the given subnets without scanning is the List Scan.

SAMPLE

7. What is the initial action of a UDP port scan?

A. Sent UDP Packet to every port

B. -sU

C. Open Response: A service responds with a UDP packet

D. Close Response: ICMP port unreachable

UDP scans start by sending a UDP datagram to each target port. Since UDP is connectionless, there's no handshake to establish first. What you get next depends on the port: an ICMP Port Unreachable may come back if a port is closed, a UDP reply might come from an open service, or you may get no reply at all if the port is filtered or the service doesn't respond. The option to use UDP scan mode is a way to perform this type of probing, but the actual initial action is sending UDP packets to the ports.

8. Which syntax scans ports that are in the nmap-services list below a threshold?

A. -p 1-1024

B. -p [1024]

C. -p [-1024]

D. -p 0-1024

Understanding port range notation in Nmap helps you target ports by numeric criteria. The question asks for the syntax that scans ports in the nmap-services list that are below a certain threshold. In this context, the form that signals "less than" a value is used. Using a dash before the threshold within brackets communicates that you want all ports below that limit, so -p [-1024] selects ports strictly under 1024. The other options describe ranges that end at 1024, start at 0, or span a consecutive block up to 1024, which don't express the "below" condition as cleanly.

9. Which of the following correctly pairs an NSE script category with a typical use?

A. Discovery: host discovery; Safe: non-intrusive checks like http-title; Intrusive: vulnerability checks; Brute-force is another category used for credential guessing.

B. Brute-force is another NSE script category used for credential guessing.

C. Discovery: host discovery; Safe: vulnerability checks; Intrusive: OS fingerprinting; Brute-force: port scanning

D. Discovery: DNS resolution; Safe: port scanning; Intrusive: banner grabbing; Brute-force

In NSE, scripts are grouped by their intent, and the brute-force category is specifically designed for trying many username/password combinations to test or gain access, which is credential guessing. That makes the statement about brute-force being a category used for credential guessing the correct pairing: it directly reflects what those scripts do and why they exist. Understanding this helps when you see other NSE scripts labeled as discovery, safe, or intrusive. Discovery scripts focus on finding hosts and services, safe scripts aim to perform non-destructive checks, and intrusive scripts cover more riskier probing like vulnerability checks. Brute-force scripts sit apart because their purpose is to test credentials, which can affect access controls and is inherently more aggressive than typical discovery or passive checks.

SAMPLE

10. Which option performs a TCP connect scan?

A. -sN

B. -sL

C. -sX

D. -sT

The method tests port state by using the operating system's normal TCP connection process to complete a full handshake with the target. This is a TCP connect scan, where the scanner attempts to establish a real TCP connection to each port via the system's connect() call. If the port is open, the handshake finishes and the scanner immediately closes the connection, marking the port as open. If the port is closed, the connect attempt fails quickly with a connection refusal, marking it as closed. If filtering or a firewall blocks the attempt, there may be no response, leading to a timeout or other filtering indication. This contrasts with the other techniques, which don't establish a full connection: those send packets with unusual flag combinations or no flags to infer state without completing a handshake, or simply list targets without scanning ports.

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://nmapzenmapswitches.examzify.com

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

SAMPLE