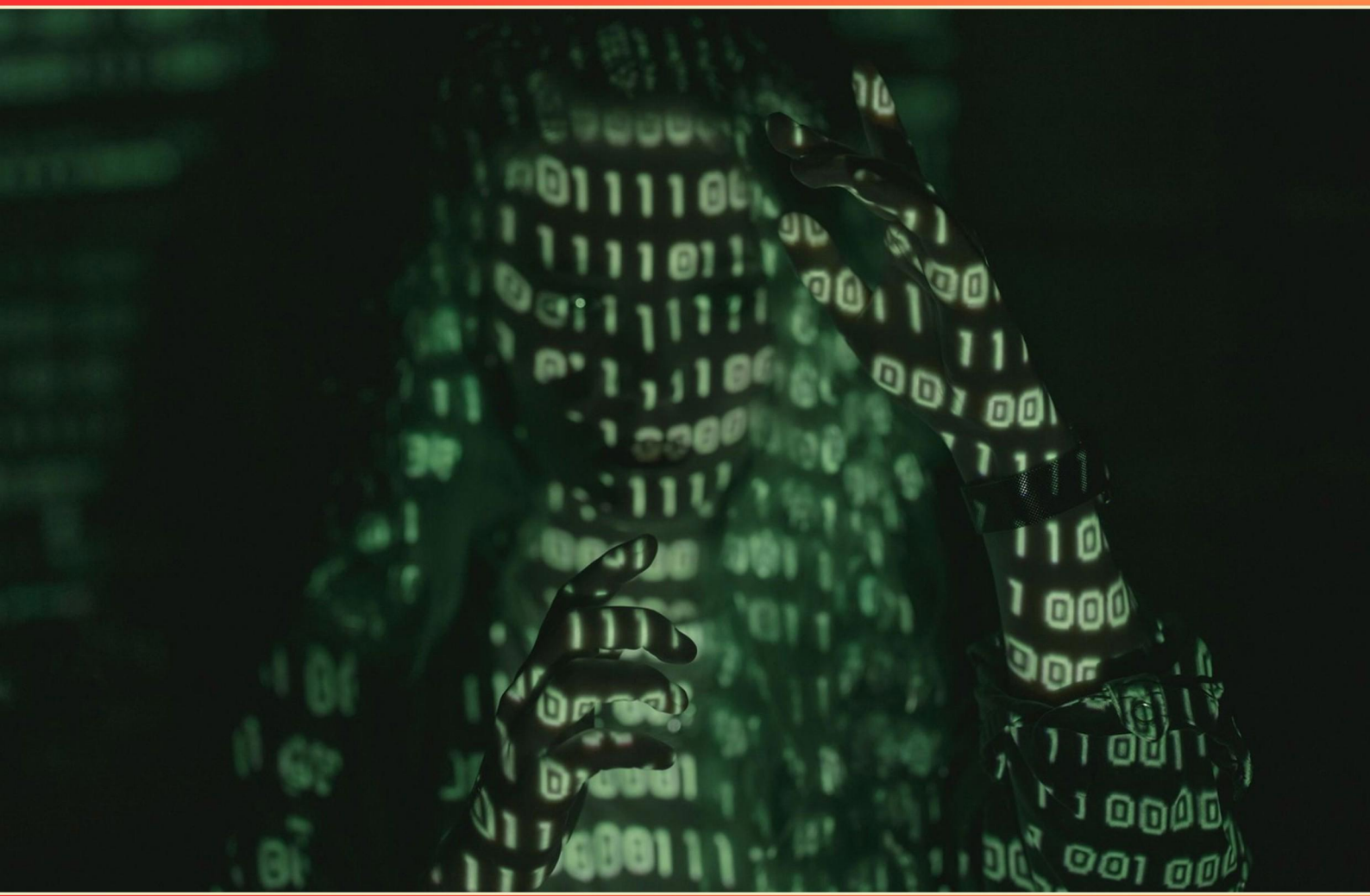
# NMAP/ZENMAP SWITCHES PRACTICE TEST (SAMPLE)

## STUDY GUIDE



## SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

**VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE**

https://nmapzenmapswitches.examzify.com

# 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 option would you use to perform a UDP scan?**

A. -sS

B. -sT

C. -sU

D. -sA

**2. What is the purpose of the -sA option and what does an ACK scan reveal about firewall behavior?**

A. It performs a TCP FIN scan to shut down services.

B. It performs a SYN scan to discover open ports.

C. It enables version detection with OS fingerprinting.

D. It performs a TCP ACK scan to map firewall rules; It reveals stateless vs stateful filtering and doesn't indicate open ports.

**3. What does the --reason option do and why would you enable it?**

A. --reason prints the reason a port is in its stated state; helps interpret results, especially when states are ambiguous.

B. --reason enables real-time network kinematics.

C. --reason filters out ports by reason codes.

D. --reason toggles verbose output.

**4. Which statement best describes idle scans in Nmap?**

A. They rely on a zombie host and IPID timing and are often less reliable.

B. They are simpler and more reliable than standard scans.

C. They do not require any extra legality considerations.

D. They always provide guaranteed covert access.

**5. How do you scan a specific port range in Nmap, for example ports 80, 443, and 1024-1050?**

A. -p 80,443,1024-1050.

B. -p 80-443,1024-1050.

C. -p 80 443 1024-1050

D. -ports 80,443,1024-1050

**6. If Nmap reports a host's port state as open, what does that imply, and how would you interpret closed and filtered states?**

A. Open ports accept connections and have services; closed ports are reachable but have no service; filtered indicates firewall or filtering.

B. Open ports mean the port is closed to all traffic.

C. Closed ports always respond with ICMP unreachable.

D. Filtered means the port is open but noisy.

**7. Distinguish between safe and intrusive NSE scripts and give an example usage scenario for each.**

A. Safe NSE scripts are non-disruptive and focus on non-intrusive checks like http-title.

B. Safe NSE scripts always require root privileges.

C. Intrusive NSE scripts probe vulnerabilities or misconfigurations and may disrupt service; use in controlled environments.

D. All NSE scripts are intrusive by design.

**8. Which flag is used to run Nmap Scripting Engine (NSE) scripts?**

A. --script

B. -S

C. -v

D. -e

**9. Which statement best describes an intrusive NSE script?**

A. Safe NSE scripts are harmless and only collect banners.

B. NSE scripts cannot cause disruption.

C. Intrusive NSE scripts probe vulnerabilities or misconfigurations and may disrupt service; use in controlled environments.

D. All NSE scripts are intrusive by design.

**10. Which scan uses FIN, PSH, and URG flags for probing and is known as a Fin scan?**

A. -sF

B. -sX

C. -sA

D. -sI

# Answers

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

# Explanations

## 1. Which option would you use to perform a UDP scan?

A. -sS

B. -sT

C. -sU

D. -sA

*UDP scanning probes UDP ports because UDP is a connectionless protocol with no handshake. When you use the UDP scan switch, Nmap sends UDP packets to target ports and waits for responses. If a port replies with a UDP payload, it's likely open. If you receive an ICMP Port Unreachable message, the port is closed. If there is no reply, the port is usually considered open|filtered, since a firewall or filtering device might be dropping the packets. This approach tends to be slower and noisier than TCP scans, and many hosts filter or rate-limit UDP traffic. Other common scanning methods target TCP behavior: one uses a SYN packet to elicit a half-open handshake, another attempts a full TCP connect, and another analyzes responses to ACK probes to infer firewall rules. The UDP switch is the appropriate choice when you specifically need to assess UDP ports.*

## 2. What is the purpose of the -sA option and what does an ACK scan reveal about firewall behavior?

A. It performs a TCP FIN scan to shut down services.

B. It performs a SYN scan to discover open ports.

C. It enables version detection with OS fingerprinting.

D. It performs a TCP ACK scan to map firewall rules; It reveals stateless vs stateful filtering and doesn't indicate open ports.

*The main idea here is how an ACK scan works and what it can reveal about a firewall. The -sA option performs a TCP ACK scan, sending ACK packets to each port. Because ACKs aren't used to open a connection, the target's responses (or lack thereof) depend on the firewall's rules rather than on whether a port is actually open. If a firewall is stateful, it tends to filter unsolicited ACKs and may drop them, producing no response for filtered ports; if a firewall is stateless, you'll see different, predictable responses for allowed versus blocked paths. By observing which ports elicit a RST or no response, you can map the firewall's rule set and determine whether filtering is stateful or stateless. This doesn't indicate open ports, which is why this scan is specifically about firewall behavior rather than port openness.*

## 3. What does the --reason option do and why would you enable it?

A. --reason prints the reason a port is in its stated state; helps interpret results, especially when states are ambiguous.

B. --reason enables real-time network kinematics.

C. --reason filters out ports by reason codes.

D. --reason toggles verbose output.

*The option is about showing why Nmap classified a port in a particular state. Enabling it adds a reason for each port's state, so you can see the underlying cause—like a firewall filter or a specific type of response—that led to labels such as open, closed, or open|filtered. This makes results much easier to interpret, especially when the state is ambiguous or influenced by intermediate devices. It's not about kinematics, filtering by reason codes, or simply increasing verbosity, which is why those other ideas don't fit.*

## 4. Which statement best describes idle scans in Nmap?

A. They rely on a zombie host and IPID timing and are often less reliable.

B. They are simpler and more reliable than standard scans.

C. They do not require any extra legality considerations.

D. They always provide guaranteed covert access.

*Idle scans rely on a zombie host and IPID timing to infer the target's port state, offering a covert probing method rather than directly from the scanner. The zombie is used to generate traffic toward the target, with the scan manipulating IP spoofing so the target's responses appear to come from the zombie. By watching how the zombie's IPID—the identification value in IP headers—changes between probes, Nmap can deduce whether the target port is open or closed based on the observed timing patterns. This approach is appealing for stealth, since the true source appears to be the zombie, but it's often less reliable because it hinges on the zombie's IPID behavior being predictable. Some operating systems randomize IPID or behave inconsistently under load, and network factors like NAT, firewalls, packet loss, or traffic elsewhere on the path can disrupt the timing measurements, leading to unclear results or failures to detect states accurately.*

## 5. How do you scan a specific port range in Nmap, for example ports 80, 443, and 1024-1050?

A. -p 80,443,1024-1050.

B. -p 80-443,1024-1050.

C. -p 80 443 1024-1050

D. -ports 80,443,1024-1050

*In Nmap, the -p option controls which ports are scanned. You can mix individual ports with port ranges by listing them separated with commas. For your target of ports 80, 443, and the range 1024-1050, the correct syntax is -p 80,443,1024-1050. This exactly specifies the two single ports plus the block from 1024 through 1050. This works because -p accepts a comma-separated list of ports and ranges, and the range 1024-1050 includes every port from 1024 to 1050 inclusive. Using a range like 80-443 would scan every port between 80 and 443, which isn't the same as scanning only 80 and 443. And using spaces or a non-existent flag like -ports would not be parsed correctly by Nmap.*

## 6. If Nmap reports a host's port state as open, what does that imply, and how would you interpret closed and filtered states?

A. Open ports accept connections and have services; closed ports are reachable but have no service; filtered indicates firewall or filtering.

B. Open ports mean the port is closed to all traffic.

C. Closed ports always respond with ICMP unreachable.

D. Filtered means the port is open but noisy.

*Port state shows what Nmap can infer about a port based on its probes. When a port is open, a service is listening there and can accept connections, so the port will respond to connection attempts. A closed port is reachable but has no service listening on it, typically replying to probes with a reset on TCP or with an ICMP unreachable in some UDP cases. Filtered means a firewall or filtering device blocks the probes, so Nmap can't determine whether the port is open or closed. This is why the described interpretation—open ports hosting services, closed ports being reachable but without a service, and filtered ports being blocked by filtering—best matches how Nmap reports port states.*

## 7. Distinguish between safe and intrusive NSE scripts and give an example usage scenario for each.

A. Safe NSE scripts are non-disruptive and focus on non-intrusive checks like http-title.

B. Safe NSE scripts always require root privileges.

C. Intrusive NSE scripts probe vulnerabilities or misconfigurations and may disrupt service; use in controlled environments.

D. All NSE scripts are intrusive by design.

*NSE scripts differ in how much they might affect the target. Some are designed to be safe and non-disruptive, simply gathering information or verifying things without touching the service beyond reading data. Intrusive scripts go further: they probe for vulnerabilities or misconfigurations and can disrupt or destabilize a service, so they should only be used where you have explicit permission and in controlled environments. That distinction is why the statement about intrusive scripts is the most accurate: they probe vulnerabilities or misconfigurations and may disrupt service, so they're appropriate only in a lab or other controlled, authorized testing scenario. An example of a safe usage is running a script that reads the HTTP title to confirm what service is listening on a port, which provides information without affecting the service. An example of an intrusive usage is running a vulnerability-focused script in a test network to detect known flaws—procedures like this carry a risk of disruption and must be done with consent and proper safeguards. Other points to note: not all safe scripts require root privileges, and not all NSE scripts are intrusive; some are explicitly designed to be non-disruptive.*

## 8. Which flag is used to run Nmap Scripting Engine (NSE) scripts?

A. --script

B. -S

C. -v

D. -e

*NSE scripts are invoked with the --script flag. This option tells Nmap to load and run the Nmap Scripting Engine scripts, either a specific script by name, a category, or multiple scripts at once. You can also pass arguments to scripts with --script-args and combine scripting with port scanning or other options. The other flags don't engage the NSE: -S sets a spoofed source address, -v only increases verbosity, and -e selects the network interface, so none of them run NSE scripts.*

## 9. Which statement best describes an intrusive NSE script?

A. Safe NSE scripts are harmless and only collect banners.

B. NSE scripts cannot cause disruption.

C. Intrusive NSE scripts probe vulnerabilities or misconfigurations and may disrupt service; use in controlled environments.

D. All NSE scripts are intrusive by design.

*Intrusive NSE scripts are the ones that go beyond simple information gathering and actively probe for vulnerabilities or misconfigurations in services. Because they perform actions that can affect a target's behavior or stability—such as attempting credential checks, configuration flaws, or vulnerability tests—they can disrupt or degrade service. That's why they're recommended only in controlled environments or with explicit authorization, so any potential impact is anticipated and managed. That's why this choice is the best: it correctly notes the probing nature of intrusive scripts and their potential to disrupt, while also advising use in a controlled setting. In contrast, safe NSE scripts are designed to minimize impact and are intended for non-destructive information collection, but they aren't restricted to just banners, and saying they're entirely harmless or limited to banners isn't an accurate or complete description. The idea that NSE scripts cannot cause disruption is false, since intrusive ones can; and the claim that all NSE scripts are intrusive by design is incorrect, as many scripts are categorized as safe or non-intrusive.*

## 10. Which scan uses FIN, PSH, and URG flags for probing and is known as a Fin scan?

A. -sF

B. -sX

C. -sA

D. -sI

*A Fin scan is all about probing ports by sending a packet with the FIN flag set and no others. In TCP, open ports typically don't respond to a FIN probe, while closed ports reply with a RST, so you can infer port state without completing a connection. That's why this scanning method is labeled as a Fin scan in Nmap, corresponding to the option that performs a FIN-flag probe. The combination of FIN, PSH, and URG flags describes a different technique known as an Xmas scan, which is a separate probe method used for fingerprinting and evasion. Other scans, like those using different flag sets for ACK or idle scanning, follow their own probing rules and don't match the Fin scan behavior.*

# 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!