Nmap/ZenMap Switches Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. How would you run a script-based vulnerability check on a target using NSE's vuln category, and what considerations apply?

A. nmap --script vuln <target>; Consider limitations: not a substitute for full auditing, possible false positives, and safety concerns.

B. nmap --script vuln <target>; It guarantees detection of all vulnerabilities.

C. nmap --script vuln --safe <target>; There are no safety concerns.

D. nmap --scan vuln <target>; It automatically fixes vulnerabilities.

2. What is the purpose of the -e option and the -S/--source-address options, and when would you use them?

A. -e selects the interface.

B. -e selects the interface; -S sets the source IP address for probes or spoofing; use to control path or evade simple filters.

C. -S enables stealth scanning.

D. -S sets the source port for outbound probes.

3. Which timing template corresponds to Sneaky (1) IDS evasion?

A. -T0

B. -T2

C. -T3

D. -T1

4. Which statement about idle (s0) scan is true?

A. Probes are sent directly to the target

B. Probes are sent via the zombie rather than directly to the target

C. It requires DNS resolution of the zombie

D. It bypasses IPID correlation

5. Which timing template corresponds to the Polite (2) setting that slows the scan to use less bandwidth and resources?

A. -T2

B. -T0

C. -T1

D. -T3

6. Slower scans are less detectable?

A. Faster scans are less detectable

B. Slower scans are more detectable

C. Slower scans are less detectable

D. Timing templates do not affect detectability

7. How does IPv6 scanning interact with the -6 option and what should you be aware of when scanning IPv6 networks?

A. -6 enables IPv6; ensure targets support IPv6 and adjust assumptions about network structure and firewalls.

B. -6 disables IPv6.

C. IPv6 scanning ignores firewalls.

D. You should always use IPv4; -6 is deprecated.

8. Which scan type establishes a full three-way handshake (TCP Connect Scan)?

A. -sT

B. -sO

C. -sP

D. -sR

9. Which timing template corresponds to the Sneaky (1) IDS evasion level?

A. -T0

B. -T2

C. -T3

D. -T1

10. What does the -sV option do in Nmap?

A. It performs an initial ping sweep.

B. It enables service/version detection to identify running software.

C. It enables script scanning.

D. It increases the retry count.

Answers

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

Explanations

1. How would you run a script-based vulnerability check on a target using NSE's vuln category, and what considerations apply?

A. nmap --script vuln <target>; Consider limitations: not a substitute for full auditing, possible false positives, and safety concerns.

B. nmap --script vuln <target>; It guarantees detection of all vulnerabilities.

C. nmap --script vuln --safe <target>; There are no safety concerns.

D. nmap --scan vuln <target>; It automatically fixes vulnerabilities.

Running NSE vulnerability checks means using Nmap's scripting engine to probe services for known issues. The command to use is nmap --script vuln <target>, which runs all scripts in the vulnerability category against the target's open ports and reports what they find. This approach provides a quick, broad view of potential exposure, but it's not a complete security audit. Vulnerability checks can produce false positives, and some issues may not be detected depending on the target's configuration, patch level, or the environment. Some vulnerability scripts can be intrusive or disruptive, so safety considerations matter: use appropriate authorization, be mindful of the impact on production services, and consider running in a controlled or staged environment. To improve reliability, you might also gather version information (for context) and tune scan options (such as port selection, timing, or timeouts) to balance depth and practicality. Remember that findings point to possible exposures, not definitive fixes, so follow up with targeted verification and remediation as part of a fuller assessment.

2. What is the purpose of the -e option and the -S/--source-address options, and when would you use them?

A. -e selects the interface.

B. -e selects the interface; -S sets the source IP address for probes or spoofing; use to control path or evade simple filters.

C. -S enables stealth scanning.

D. -S sets the source port for outbound probes.

This probes your ability to control how the scan leaves your machine and what source address it uses. The -e option binds Nmap to a specific network interface. This is essential when a host has multiple interfaces (for example, a wired and a wireless card, or a VPN tunnel) and you need the scan to go out through the correct path or reach a target on a particular network. The -S or --source-address option sets the source IP address that appears in the probes. This lets you influence the network path (some networks route or filter traffic based on the source address) and test how filters behave with different sources. It can even be used to simulate traffic from a given IP. Because replies go to the source address, you won't see responses on your scanner unless the route returns to you, so use this when you specifically want to test path or filter behavior rather than to get direct test results back. In short, these switches give you precise control over which interface is used and what source IP the probes appear to come from, which is why you'd use them in multi-homed setups or when testing routing and filtering policies.

3. Which timing template corresponds to Sneaky (1) IDS evasion?

A. -T0

B. -T2

C. -T3

D. -T1

Timing templates control how fast or stealthy Nmap runs. The Sneaky (1) IDS evasion option uses the -T1 template. It intentionally slows down the scan and spaces probes to reduce the chance that IDS/IPS systems will flag or log the activity. This makes it slower than the default, but not as slow as the paranoid setting, giving a practical balance between stealth and speed. The other templates push speed in various directions—paranoid being very slow and stealthy, polite and normal offering moderate speed, and aggressive/insane being fast but more likely to trigger detections.

4. Which statement about idle (s0) scan is true?

A. Probes are sent directly to the target

B. Probes are sent via the zombie rather than directly to the target

C. It requires DNS resolution of the zombie

D. It bypasses IPID correlation

Idle (s0) scanning uses a zombie host to carry out the probe traffic to the target, rather than sending probes directly from the scanner. The attacker leverages a zombie with a predictable IPID sequence and a covert side channel: by forcing the zombie to provoke responses from the target and by observing how the zombie's IPID values change, the scanner can infer whether a port on the target is open, closed, or filtered. In short, the probes travel through the zombie, not directly from the scanner, which is why this option is the correct description. DNS resolution of the zombie isn't required for the technique, and the method specifically relies on IPID behavior, so it doesn't bypass IPID correlation.

5. Which timing template corresponds to the Polite (2) setting that slows the scan to use less bandwidth and resources?

A. -T2

B. -T0

C. -T1

D. -T3

Timing templates control how aggressively Nmap probes targets, affecting speed, bandwidth, and resource use. Polite is the middle timing profile: it slows the scan to use less bandwidth and resources by increasing inter-packet delays and reducing concurrency. This makes the scan gentler on the network and less noticeable, at the cost of longer run time. It sits between the slower, more stealthy templates (paranoid and sneaky) and the default-to-faster ones (normal, aggressive, insane). So the Polite setting corresponds to the middle timing template, which is why it matches the described behavior.

6. Slower scans are less detectable?

A. Faster scans are less detectable

B. Slower scans are more detectable

C. Slower scans are less detectable

D. Timing templates do not affect detectability

Slower scans are less detectable because sending fewer packets per second makes the probing activity blend more with normal network traffic. Security systems, rate limits, and IDS/IPS heuristics often flag rapid, high-volume scans, so dialing down the scan speed reduces the chances of triggering alarms. Nmap's timing templates let you trade speed for stealth, with slower settings producing quieter probes. That's why the statement is correct: slower scans tend to be less detectable. In contrast, faster scans generate more traffic and are more likely to be noticed, and timing templates definitely affect detectability.

7. How does IPv6 scanning interact with the -6 option and what should you be aware of when scanning IPv6 networks?

A. -6 enables IPv6; ensure targets support IPv6 and adjust assumptions about network structure and firewalls.

B. -6 disables IPv6.

C. IPv6 scanning ignores firewalls.

D. You should always use IPv4; -6 is deprecated.

IPv6 scanning is activated by the -6 switch, which tells Nmap to use IPv6 addresses and protocols instead of IPv4. Because you're working in the IPv6 space, you must verify that the targets actually have IPv6 addresses and reachable paths; many networks or devices may be IPv6-enabled in some parts but not others, or may require different discovery methods. Firewalls and filtering also behave differently in IPv6, so you shouldn't assume the same reachability as with IPv4. The network topology, access controls, and even how hosts respond to probes can differ, so you'll need to adjust your expectations about what's visible and reachable. Also, IPv6 lacks broadcast like IPv4, so host discovery and scanning strategies might rely more on targeted addresses, DNS results, or neighbor discovery behavior. In short, -6 enables IPv6 scanning; ensure targets support IPv6 and be prepared to rethink network structure assumptions and firewall behavior in the IPv6 environment.

8. Which scan type establishes a full three-way handshake (TCP Connect Scan)?

A. -sT

B. -sO

C. -sP

D. -sR

The scan type that establishes a full three-way handshake is the TCP connect approach. It uses the system's connect() call to try to open a real TCP connection to the target port, which means the full handshake—SYN, SYN-ACK, and ACK—occurs. If the port is open, the handshake completes and the connection is established (and then typically torn down by the scanner). This provides definitive evidence that the port is open, but it's noisier and more easily detected because it completes a full TCP connection. The other options don't perform a standard TCP handshake: the IP protocol scan sends crafted IP packets to detect which IP protocols the host supports; the ping sweep simply checks if a host is up; the RPC scan targets remote procedure call services and asks about RPC-specific ports rather than establishing a general TCP connection.

9. Which timing template corresponds to the Sneaky (1) IDS evasion level?

A. -T0

B. -T2

C. -T3

D. -T1

Timing templates control how aggressively Nmap sends probes, balancing speed with stealth. The Sneaky level, labeled as 1, maps to the timing option -T1. This template is designed to be stealthy enough to avoid triggering IDS/IPS rules, slowing down the scan and reducing probe frequency so traffic looks more like normal activity. It sits between the very cautious paranoid template (-T0) and the slightly faster polite template (-T2), offering a practical trade-off between covertness and completion time. So, for Sneaky (1) IDS evasion, the appropriate choice is the one that specifies -T1. The more paranoid option (-T0) is slower and extremely cautious, while the polite (-T2), normal (-T3), and aggressive (-T4) templates raise speed and detection risk, respectively.

10. What does the -sV option do in Nmap?

A. It performs an initial ping sweep.

B. It enables service/version detection to identify running software.

C. It enables script scanning.

D. It increases the retry count.

The main idea this question tests is how Nmap identifies exactly what software is running on open ports, not just which ports are reachable. The -sV option enables service and version detection, so Nmap probes the services it discovers and compares the responses to a database to tell you the service name and often the specific version (for example, an HTTP server like Apache/2.4.41). This is the best answer because it matches the purpose of -sV: to reveal what software is running on each open port and which version of that software is present. Knowing the service and version is crucial for vulnerability assessment and inventory. Other options describe different functionality. A ping sweep is about discovering which hosts are up, not identifying running services. Script scanning uses the Nmap Scripting Engine to run NSE scripts for additional checks. Increasing the retry count changes how many times Nmap resends probes, affecting scan thoroughness and timing rather than identifying services or versions.

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!