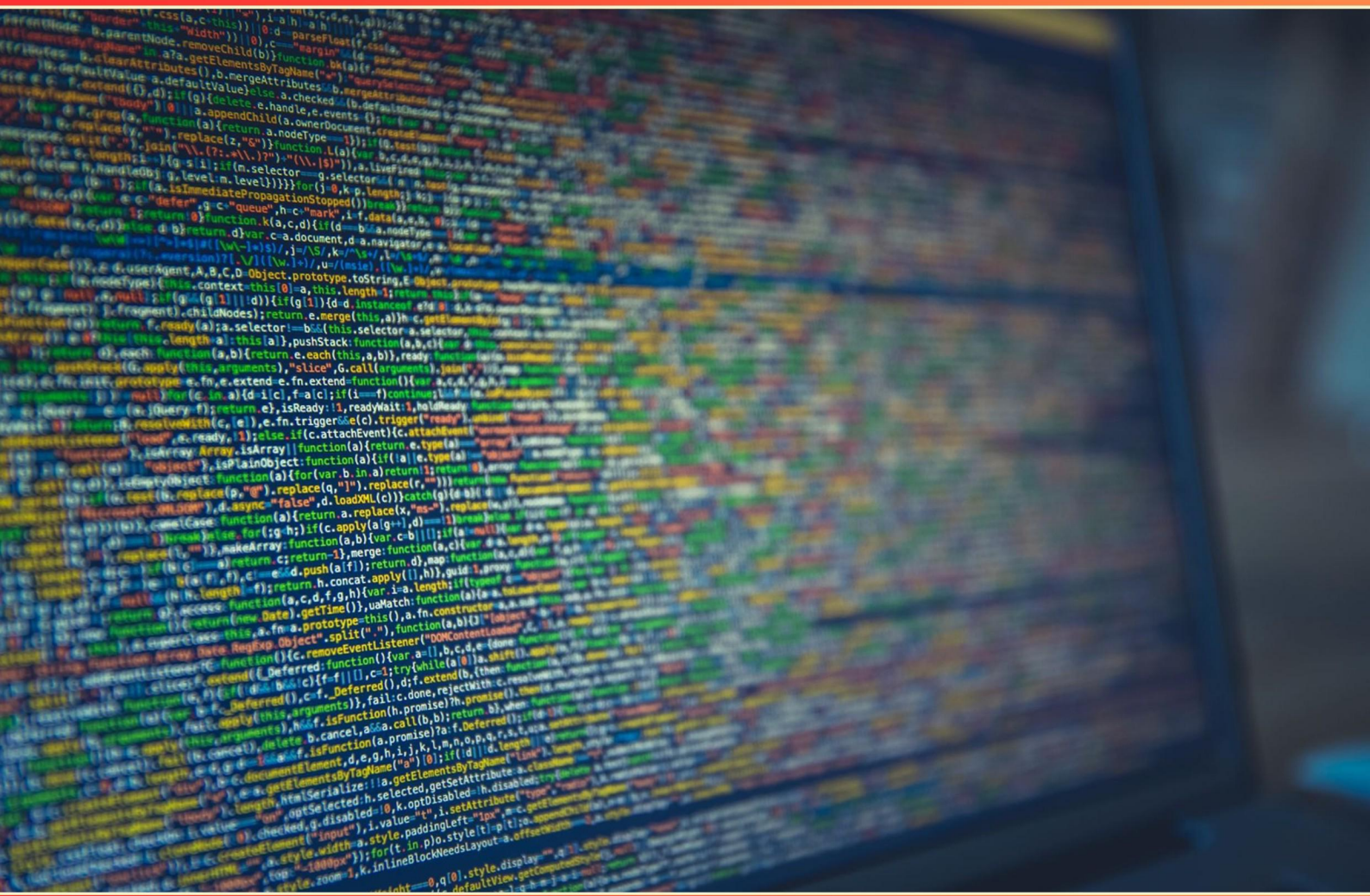
CERTIFIED ETHICAL HACKER VERSION 11 (CEHV11) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cehv11.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 tool would you use to obtain system information such as host name and uptime?**

   A. PsInfo

   B. PsLoggedOn

   C. PsList

   D. PsShutdown

2. **Which publication is a paid resource known for publishing industry reports?**

   A. The Wall Street Transcript

   B. MarketWatch

   C. LexisNexis

   D. Business Wire

3. **Which command scans the target IP address for an open NFS port (2049) and the NFS services running on it?**

   A. ntpdate

   B. ntpq

   C. rpcinfo

   D. ntptrace

4. **Which technique can be used to determine if an IP or service is a threat source within a security framework?**

   A. Cisco IPS Source IP Reputation Filtering

   B. RFC 3704 Filtering

   C. Traffic Pattern Analysis

   D. Event Log Analysis

5. **Which technology detects runtime attacks and provides visibility into vulnerabilities in real-time apps?**

   A. Security misconfiguration

   B. N-Stalker Web App Security Scanner

   C. BeEF

   D. Runtime Application Self Protection

6. Redirects packets from a target host on the LAN intended for another host on the LAN by forging ARP replies?

A. ARP

B. DHCP attack

C. VoIP Call Tapping

D. Arpspoof

7. Which AWS hacking tool includes automated scripts for reconnaissance, escalating privileges, maintaining access, and clearing tracks?

A. AWS pwn

B. GCPBucketBrute

C. Misconfiguration Attack

D. Operating System Attack

8. NetPatch Firewall is best described as what kind of system?

A. A honeypot or deception system that simulates a complete system and lures attackers, logs activity, and notifies security staff.

B. A mobile no-root firewall for Android devices.

C. An agent-less log analytics tool.

D. An obfuscation utility.

9. Which tool provides a lookup database for default passwords, credentials, and ports?

A. Sequencer tool

B. cirt.net

C. NCollector Studio

D. Acunetix WVS

10. What is the primary function of spider honeypots?

A. Honeynets

B. Spider Honeypots

C. Snort

D. Suricata

Answers

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

Explanations

1. Which tool would you use to obtain system information such as host name and uptime?

A. PsInfo

B. PsLoggedOn

C. PsList

D. PsShutdown

To quickly gather basic system details like the host name and how long the system has been running, PsInfo is the right choice. This Sysinternals tool is designed to query a machine and display essential system information, including the host name, uptime, OS version, and other details, either locally or on a remote computer. The other tools in the Ps family serve different purposes—PsLoggedOn shows who's logged on, PsList lists processes, and PsShutdown handles shutdown/reboot actions—so they wouldn't provide a straightforward view of host name and uptime.

2. Which publication is a paid resource known for publishing industry reports?

A. The Wall Street Transcript

B. MarketWatch

C. LexisNexis

D. Business Wire

The Wall Street Transcript stands out because it operates on a subscription model and is known for delivering in-depth industry reports and analyses for investors. This publication curates and publishes detailed sector-focused reports that readers pay to access, making it a paid resource specifically dedicated to industry insights. MarketWatch provides market news and data, often free or with optional premium services, but it isn't primarily a repository of targeted industry reports you subscribe to. LexisNexis is a paid research platform for legal, news, and business information, not a publication known for publishing standalone industry reports to subscribers. Business Wire distributes press releases, not in-depth industry reports published for subscribers. So the paid resource known for publishing industry reports is The Wall Street Transcript.

3. Which command scans the target IP address for an open NFS port (2049) and the NFS services running on it?

A. ntpdate

B. ntpq

C. rpcinfo

D. ntptrace

NFS runs over RPC, so to find an open NFS port and the services it provides you check the RPC service registry on the target. The tool that asks the registry (the portmapper) what RPC programs are registered, their versions, and which ports they listen on is ideally suited for this. By querying the target, you'll see the NFS program (with its versions) and the port it's using, which commonly appears as the NFS port 2049. This confirms both that NFS is available and exactly which port it's on. Other options are focused on time synchronization or NTP-related tasks, not on discovering RPC-based services like NFS.

4. Which technique can be used to determine if an IP or service is a threat source within a security framework?

A. Cisco IPS Source IP Reputation Filtering

B. RFC 3704 Filtering

C. Traffic Pattern Analysis

D. Event Log Analysis

Reputation-based filtering uses threat intelligence to classify IP addresses and other sources as known threats. In a security framework, evaluating whether an IP or service is a threat source lets the system block or limit traffic from that source before it reaches sensitive resources. Cisco IPS Source IP Reputation Filtering does this directly by consulting threat-intelligence feeds to mark certain source IPs as malicious or suspicious and enforce blocking or restrictions accordingly, reducing exposure from compromised hosts, botnets, or scanners. RFC 3704 Filtering is about preventing spoofed addresses by ensuring packets have believable source addresses, not about judging whether the source itself is harmful. Traffic Pattern Analysis examines how traffic behaves to spot anomalies, which helps detect potential threats but doesn't inherently tag a source as a threat by reputation. Event Log Analysis involves reviewing logs to detect and investigate incidents after they occur, rather than proactively identifying threat sources at the entry point.

5. Which technology detects runtime attacks and provides visibility into vulnerabilities in real-time apps?

A. Security misconfiguration

B. N-Stalker Web App Security Scanner

C. BeEF

D. Runtime Application Self Protection

Runtime Application Self-Protection is a security technology that sits inside the running application and watches its own execution in real time. It monitors data flows, code paths, and inputs as requests come in, applying security policies to detect suspicious activity that indicates an attack. When something malicious is detected, it can block or mitigate the attack immediately and provide detailed telemetry about what's happening in the live app. This combination of real-time attack detection and visibility into the app's vulnerabilities as it runs is what makes RASP the right choice for detecting runtime attacks in real-time applications. Other options are not designed to do this. A security misconfiguration refers to a type of vulnerability or risk, not a runtime protection mechanism. A web app security scanner like the N-Stalker is used to discover weaknesses by probing the app, not to protect and monitor it as it runs. BeEF focuses on browser exploitation and post-compromise activities, not on in-application runtime protection or real-time visibility.

6. Redirects packets from a target host on the LAN intended for another host on the LAN by forging ARP replies?

A. ARP

B. DHCP attack

C. VoIP Call Tapping

D. Arpspoof

On a local network, devices learn how to reach each other by mapping IP addresses to MAC addresses using ARP. That mapping is stored in each device's ARP cache and ARP replies aren't authenticated, so they can be forged. By sending forged ARP replies, a malicious host can convince a target that the attacker's MAC address corresponds to the IP of another host (like the gateway or another device). When the target sends traffic to that IP, it actually goes to the attacker. If the attacker then forwards the traffic to the true destination, the communication remains ongoing while the attacker eavesdrops or manipulates it—this is a man in the middle attack. The situation described—redirecting packets from a target host on the LAN intended for another host on the LAN by forging ARP replies—is ARP spoofing (often implemented with a tool like arpspoof). The other options don't describe this technique: ARP is the protocol itself, a DHCP attack centers on manipulating IP configuration, VoIP call tapping targets voice traffic, and arpspoof refers to the tool used to perform ARP spoofing.

7. Which AWS hacking tool includes automated scripts for reconnaissance, escalating privileges, maintaining access, and clearing tracks?

A. AWS pwn

B. GCPBucketBrute

C. Misconfiguration Attack

D. Operating System Attack

Focusing on post-exploitation automation within a cloud environment is what this question tests. An AWS-focused tool that includes automated scripts for reconnaissance, privilege escalation, maintaining access, and clearing tracks fits this pattern exactly: it is built to carry out the full sequence of post compromise actions inside Amazon Web Services, from mapping resources and permissions to exploiting gaps, establishing persistence, and attempting to erase or obscure audit trails. That combination—AWS-specific automation across all four stages—is what sets it apart from the other options. The other choices don't align with this AWS-centric, four-stage automation concept: one targets Google Cloud Platform storage buckets, another is a broad misconfiguration concept, and the last centers on operating system-level attacks rather than cloud-infrastructure post-exploitation.

8. NetPatch Firewall is best described as what kind of system?

A. A honeypot or deception system that simulates a complete system and lures attackers, logs activity, and notifies security staff.

B. A mobile no-root firewall for Android devices.

C. An agent-less log analytics tool.

D. An obfuscation utility.

Deception and honeypot concepts are built around luring attackers into a controlled, fake environment so defenders can observe their methods, collect evidence, and alert the security team. NetPatch Firewall fits this idea by acting as a high-interaction deception system that simulates a complete, real-looking target. Attackers engage with it as if it were a real host, while all their actions are logged in detail and the security staff are notified. This approach provides actionable threat intelligence and visibility into attacker techniques without risking production assets. It's not describing a traditional firewall that merely filters traffic, nor is it simply an agent-less log tool or an obfuscation utility. NetPatch Firewall's strength lies in creating a convincing decoy that lures intruders, captures their behavior, and signals defenders to respond.

9. Which tool provides a lookup database for default passwords, credentials, and ports?

A. Sequencer tool

B. cirt.net

C. NCollector Studio

D. Acunetix WVS

Looking up default credentials and common port information is a quick-reference task used during reconnaissance and credential testing in a pentest. A resource that specializes in this is a database of factory-default usernames and passwords for devices and services, paired with the standard ports those services listen on. This allows you to rapidly check if an asset might be left with defaults or exposed on well-known ports, which can reveal easy-entry points or misconfigurations. cirt.net is the resource built for this purpose. It hosts a comprehensive default password database and a port/service reference, making it easy to search for a device, service, or port and compare it against widely used defaults. This focused purpose makes it the best fit for looking up credentials and port mappings. The other tools mentioned serve different roles. A sequencing-related tool isn't designed for credential lookups, NCollector Studio focuses on collecting and inventorying data rather than providing a defaults reference, and Acunetix WVS is a web vulnerability scanner without a centralized database of default credentials and ports.

10. What is the primary function of spider honeypots?

A. Honeynets

B. Spider Honeypots

C. Snort

D. Suricata

Trapping and studying automated web crawlers by serving decoy pages and logging their activity is the main purpose of spider honeypots. They're set up to lure spiders—like search engine crawlers or scraping bots—into interacting with fake content, and then you capture data such as which URLs are requested, how often, what user agents are used, and what behavior follows. This helps you distinguish legitimate indexing bots from malicious scrapers and collect intelligence on bot techniques and patterns for defense. This isn't about broad decoy networks for attackers (that would describe honeynets), nor is it about real-time traffic analysis or intrusion detection (roles of tools like Snort or Suricata).

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://cehv11.examzify.com

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