



Up-to-date Practice Test with Latest Questions and Answers covering latest syllabus and topics of the exam. Makes you ready to face actual exam.



CPEH-001 Practice Questions
CPEH-001 Practice Test
CPEH-001 Practice Exam
CPEH-001 Exam Questions
CPEH-001 Study Guide



killexams.com

GAQM

CPEH-001

Certified Professional Ethical Hacker (CPEH)

ORDER FULL VERSION

<https://killexams.com/pass4sure/exam-detail/CPEH-001>



Question: 91

DHCP snooping is a great solution to prevent rogue DHCP servers on your network.

Which security feature on switches leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

- A . Port security
- B . A Layer 2 Attack Prevention Protocol (LAPP)
- C . Dynamic ARP inspection (DAI)
- D . Spanning tree

Answer: C

Question: 92

In the field of cryptanalysis, what is meant by a “rubber-hose” attack?

- A . Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- B . Extraction of cryptographic secrets through coercion or torture.
- C . Forcing the targeted key stream through a hardware-accelerated device such as an ASI
- E . A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

Question: 93

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it.

What would be a good step to have in the procedures for a situation like this?

- A . Have the network team document the reason why the rule was implemented without prior manager approval.
- B . Monitor all traffic using the firewall rule until a manager can approve it.
- C . Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D . Immediately roll back the firewall rule until a manager can approve it

Answer: D

Question: 94

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the

logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours.

What protocol used on Linux servers to synchronize the time has stopped working?

- A . Time Keeper
- B . NTP
- C . PPP
- D . OSPP

Answer: B

Question: 95

Darius is analysing logs from IDS. He want to understand what have triggered one alert and verify if it's true positive or false positive.

Looking at the logs he copy and paste basic details like below:

source IP: 192.168.21.100

source port: 80

destination IP: 192.168.10.23

destination port: 63221

What is the most proper answer?

- A . This is most probably true negative.
- B . This is most probably true positive which triggered on secure communication between client and server.
- C . This is most probably false-positive, because an alert triggered on reversed traffic.
- D . This is most probably false-positive because IDS is monitoring one direction traffic.

Answer: A

Question: 96

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

- A . PPP
- B . IPSEC
- C . PEM
- D . SET

Answer: B

Question: 97

Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

- A . Bluesmacking
- B . Bluesniffing
- C . Bluesnarfing
- D . Bluejacking

Answer: D

Question: 98

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach.

After that, people must approximate their RFID badges. Both the identifications are required to open the door.

In this case, we can say:

- A . Although the approach has two phases, it actually implements just one authentication factor
- B . The solution implements the two authentication factors: physical object and physical characteristic
- C . The solution will have a high level of false positives
- D . Biological motion cannot be used to identify people

Answer: B

Question: 99

You perform a scan of your company's network and discover that TCP port 123 is open.

What services by default run on TCP port 123?

- A . Telnet
- B . POP3
- C . Network Time Protocol
- D . DNS

Answer: C

Question: 100

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation.

Which of the following is appropriate to analyze?

- A . Event logs on the PC
- B . Internet Firewall/Proxy log
- C . IDS log
- D . Event logs on domain controller

Answer: B

Question: 101

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.

What may be the problem?

- A . Traffic is Blocked on UDP Port 53
- B . Traffic is Blocked on UDP Port 80
- C . Traffic is Blocked on UDP Port 54
- D . Traffic is Blocked on UDP Port 80

Answer: A

Question: 102

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- A . SHA-2
- B . SHA-3
- C . SHA-1
- D . SHA-0

Answer: C

Question: 103

Why containers are less secure than virtual machines?

- A . Host OS on containers has a larger surface attack.
- B . Containers may full fill disk space of the host.
- C . A compromise container may cause a CPU starvation of the host.
- D . Containers are attached to the same virtual network.

Answer: A

Question: 104

Your business has decided to add credit card numbers to the data it backs up to tape.

Which of the following represents the best practice your business should observe?

- A . Hire a security consultant to provide direction.
- B . Do not back up either the credit card numbers or their hashes.
- C . Back up the hashes of the credit card numbers not the actual credit card numbers.
- D . Encrypt backup tapes that are sent off-site.

Answer: A

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including Exam Questions, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.



Practice Exam Questions Based on Current Exam Objectives

Killexams.com provides practice exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these practice questions, candidates will cover the structure, difficulty level, and topics of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Practice Exams (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of practice questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online Test Engine & Desktop Test Engine)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Test Engine. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions, with latest syllabus and topics of the exam. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our practice question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying up-to-date, relevant material, and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.