Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

CPEH-001 Dumps
CPEH-001 Braindumps
CPEH-001 Real Questions
CPEH-001 Practice Test
CPEH-001 Actual Questions

PASS

GAQM

CPEH-001

Certified Professional Ethical Hacker (CPEH)

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 staring 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 compliant 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 that 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 cither the credit card numbers or then 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

SAMPLE QUESTIONS

These questions are for demo purpose only. ***Full version*** *is up to date and contains actual questions and answers.*

Killexams.com is an online platform that offers a wide range of services related to certification exam preparation. The platform provides actual questions, exam dumps, and practice tests to help individuals prepare for various certification exams with confidence. Here are some key features and services offered by Killexams.com:

Actual Exam Questions*: Killexams.com provides actual exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these actual questions, candidates can familiarize themselves with the content and format of the real exam.*

Exam Dumps*: Killexams.com offers exam dumps in PDF format. These dumps contain a comprehensive collection of questions and answers that cover the exam topics. By using these dumps, candidates can enhance their knowledge and improve their chances of success in the certification exam.*

Practice Tests*: Killexams.com provides practice tests through their desktop VCE exam simulator and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice tests cover a wide range of questions and enable candidates to identify their strengths and weaknesses.*

Guaranteed Success*: Killexams.com offers a success guarantee with their exam dumps. They claim that by using their materials, candidates will pass their exams on the first attempt or they will refund the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exams.*

Updated Content: *Killexams.com regularly updates its question bank and exam dumps to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.*

Technical Support*: Killexams.com provides free 24x7 technical support to assist candidates with any queries or issues they may encounter while using their services. Their certified experts are available to provide guidance and help candidates throughout their exam preparation journey.*