



CEH-001^{Q&As}

Certified Ethical Hacker (CEH)

Pass GAQM CEH-001 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/ceh-001.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GAQM
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

This TCP flag instructs the sending system to transmit all buffered data immediately.

- A. SYN
- B. RST
- C. PSH
- D. URG
- E. FIN

Correct Answer: C

QUESTION 2

Wayne is the senior security analyst for his company. Wayne is examining some traffic logs on a server and came across some inconsistencies. Wayne finds some IP packets from a computer purporting to be on the internal network. The packets originate from 192.168.12.35 with a TTL of 15. The server replied to this computer and received a response from 192.168.12.35 with a TTL of 21. What can Wayne infer from this traffic log?

- A. The initial traffic from 192.168.12.35 was being spoofed.
- B. The traffic from 192.168.12.25 is from a Linux computer.
- C. The TTL of 21 means that the client computer is on wireless.
- D. The client computer at 192.168.12.35 is a zombie computer.

Correct Answer: A

QUESTION 3

What is the broadcast address for the subnet 190.86.168.0/22?

- A. 190.86.168.255
- B. 190.86.255.255
- C. 190.86.171.255
- D. 190.86.169.255

Correct Answer: C

QUESTION 4



Attackers can potentially intercept and modify unsigned SMB packets, modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after a legitimate authentication and gain unauthorized access to data. Which of the following is NOT a means that can be used to minimize or protect against such an attack?

- A. Timestamps
- B. SMB Signing
- C. File permissions
- D. Sequence numbers monitoring

Correct Answer: ABD

QUESTION 5

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

Correct Answer: D

[Latest CEH-001 Dumps](#)

[CEH-001 PDF Dumps](#)

[CEH-001 Exam Questions](#)