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.pass4itsure.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

_____ will let you assume a users identity at a dynamically generated web page or site.

A. SQL attack

B. Injection attack

C. Cross site scripting

D. The shell attack

E. Winzapper

Correct Answer: C

QUESTION 2

What is the proper response for a FIN scan if the port is closed?

A. SYN

B. ACK

C. FIN

D. PSH

E. RST

Correct Answer: E

QUESTION 3

What happens during a SYN flood attack?

A. TCP connection requests floods a target machine is flooded with randomized source address and ports for the TCP ports.

B. A TCP SYN packet, which is a connection initiation, is sent to a target machine, giving the target host\\'s address as both source and destination, and is using the same port on the target host as both source and destination.

C. A TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.

D. A TCP packet is received with both the SYN and the FIN bits set in the flags field.

Correct Answer: A

QUESTION 4

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts.

Which of the following features makes this possible? (Choose two)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

Correct Answer: BD

QUESTION 5

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city\\'s computer network are secure from all angles. Bill is an IT technician that works with Hampton in the same IT department. Bill\\'s primary responsibility is to keep PC\\'s and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees. After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network. Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill\\'s boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill\\'s boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company\\'s building.

How was Bill able to get Internet access without using an agency laptop?

A. Bill spoofed the MAC address of Dell laptop

B. Bill connected to a Rogue access point

C. Toshiba and Dell laptops share the same hardware address

D. Bill brute forced the Mac address ACLs

Correct Answer: A

[Latest CEH-001 Dumps](#)   [CEH-001 VCE Dumps](#)   [CEH-001 Braindumps](#)