

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.certbus.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

What are the two basic types of attacks? (Choose two.)

- A. DoS
- B. Passive
- C. Sniffing
- D. Active
- E. Cracking

Correct Answer: BD

QUESTION 2

You are doing IP spoofing while you scan your target. You find that the target has port 23 open. Anyway you are unable to connect. Why?

- A. A firewall is blocking port 23
- B. You cannot spoof + TCP
- C. You need an automated telnet tool
- D. The OS does not reply to telnet even if port 23 is open

Correct Answer: A

QUESTION 3

According to the CEH methodology, what is the next step to be performed after footprinting?

- A. Enumeration
- B. Scanning
- C. System Hacking
- D. Social Engineering
- E. Expanding Influence

Correct Answer: B

QUESTION 4

You have the SOA presented below in your Zone. Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

Correct Answer: C

QUESTION 5

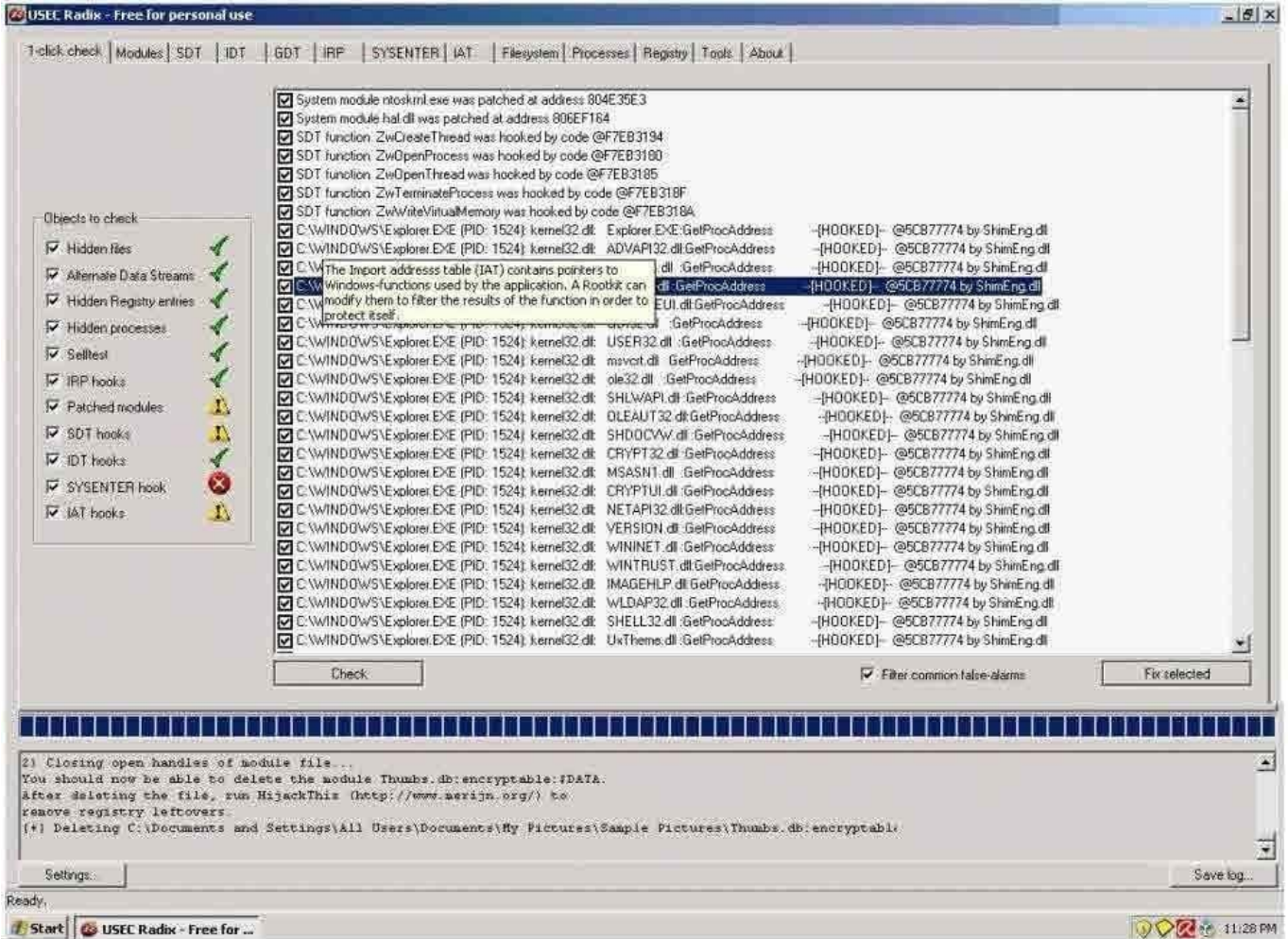
Windows LAN Manager (LM) hashes are known to be weak. Which of the following are known weaknesses of LM? (Choose three)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32 bit encryption.
- D. Effective length is 7 characters.

Correct Answer: ABD

QUESTION 6

A rootkit is a collection of tools (programs) that enable administrator-level access to a computer. This program hides itself deep into an operating system for malicious activity and is extremely difficult to detect. The malicious software operates in a stealth fashion by hiding its files, processes and registry keys and may be used to create a hidden directory or folder designed to keep out of view from a user's operating system and security software.



What privilege level does a rootkit require to infect successfully on a Victim's machine?

- A. User level privileges
- B. Ring 3 Privileges
- C. System level privileges
- D. Kernel level privileges

Correct Answer: D

QUESTION 7

Which one of the following network attacks takes advantages of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. Smurf
- C. Ping of Death

D. SYN flood

E. SNMP Attack

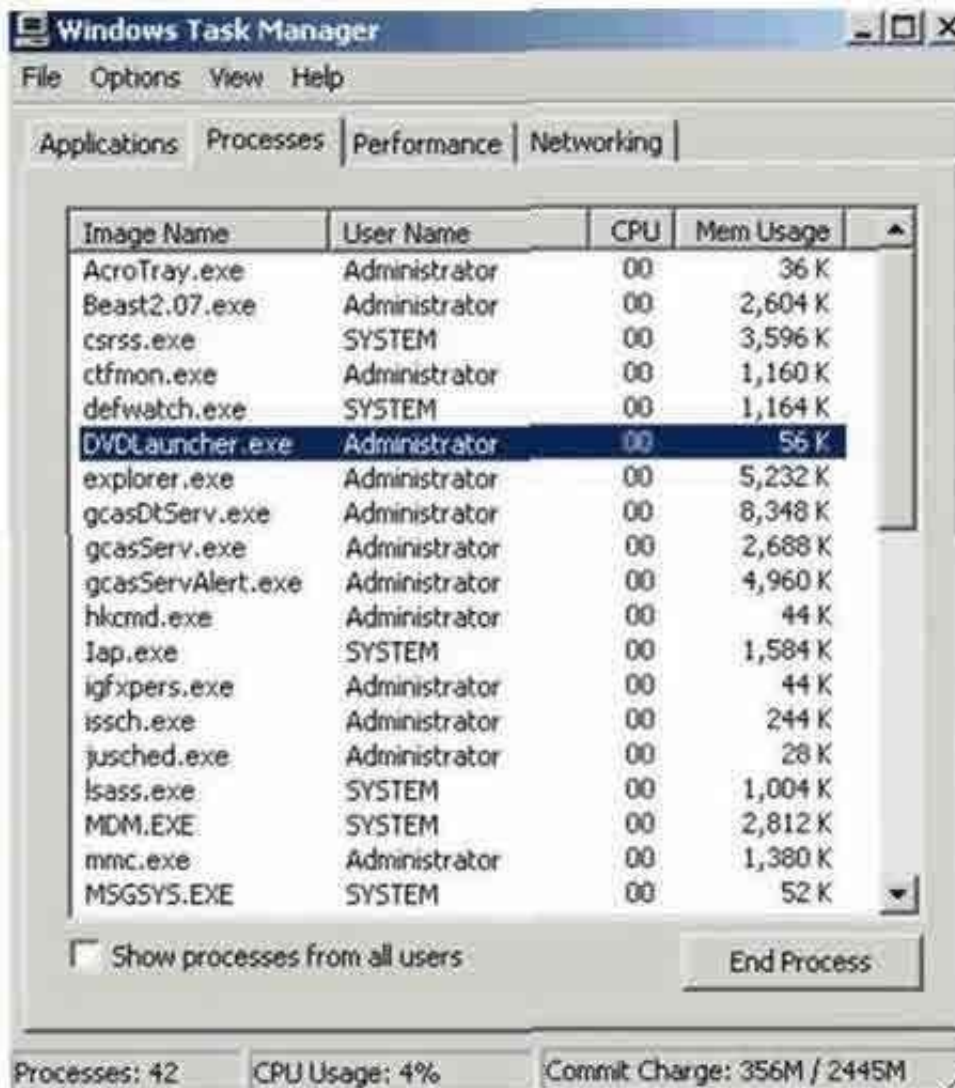
Correct Answer: A

QUESTION 8

William has received a Chess game from someone in his computer programming class through email. William does not really know the person who sent the game very well, but decides to install the game anyway because he really likes Chess.



After William installs the game, he plays it for a couple of hours. The next day, William plays the Chess game again and notices that his machine has begun to slow down. He brings up his Task Manager and sees the following programs running:



What has William just installed?

- A. Zombie Zapper (ZoZ)
- B. Remote Access Trojan (RAT)
- C. Bot IRC Tunnel (BIT)
- D. Root Digger (RD)

Correct Answer: B

QUESTION 9

Derek has stumbled upon a wireless network and wants to assess its security. However, he does not find enough traffic for a good capture. He intends to use AirSnort on the captured traffic to crack the WEP key and does not know the IP address range or the AP. How can he generate traffic on the network so that he can capture enough packets to crack the WEP key?

- A. Use any ARP requests found in the capture
- B. Derek can use a session replay on the packets captured
- C. Derek can use KisMAC as it needs two USB devices to generate traffic
- D. Use Ettercap to discover the gateway and ICMP ping flood tool to generate traffic

Correct Answer: D

QUESTION 10

What are two things that are possible when scanning UDP ports? (Choose two.)

- A. A reset will be returned
- B. An ICMP message will be returned
- C. The four-way handshake will not be completed
- D. An RFC 1294 message will be returned
- E. Nothing

Correct Answer: BE

QUESTION 11

What is the best means of prevention against viruses?

- A. Assign read only permission to all files on your system.
- B. Remove any external devices such as floppy and USB connectors.
- C. Install a rootkit detection tool.
- D. Install and update anti-virus scanner.

Correct Answer: D

QUESTION 12

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

- A. Proper testing
- B. Secure coding principles
- C. Systems security and architecture review

D. Analysis of interrupts within the software

Correct Answer: D

QUESTION 13

Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?

- A. Smurf
- B. Bubonic
- C. SYN Flood
- D. Ping of Death

Correct Answer: A

QUESTION 14

One of your junior administrator is concerned with Windows LM hashes and password cracking. In your discussion with them, which of the following are true statements that you would point out?

Select the best answers.

- A. John the Ripper can be used to crack a variety of passwords, but one limitation is that the output doesn't show if the password is upper or lower case.
- B. BY using NTLMV1, you have implemented an effective countermeasure to password cracking.
- C. SYSKEY is an effective countermeasure.
- D. If a Windows LM password is 7 characters or less, the hash will be passed with the following characters, in HEX-00112233445566778899.
- E. Enforcing Windows complex passwords is an effective countermeasure.

Correct Answer: ACE

QUESTION 15

Which of the following techniques can be used to mitigate the risk of an on-site attacker from connecting to an unused network port and gaining full access to the network? (Choose three.)

- A. Port Security
- B. IPSec Encryption
- C. Network Admission Control (NAC)

D. 802.1q Port Based Authentication

E. 802.1x Port Based Authentication

F. Intrusion Detection System (IDS)

Correct Answer: ACE

[CEH-001 PDF Dumps](#)

[CEH-001 VCE Dumps](#)

[CEH-001 Braindumps](#)