



# SEC504<sup>Q&As</sup>

Hacker Tools, Techniques, Exploits and Incident Handling

**Pass SANS SEC504 Exam with 100% Guarantee**

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

<https://www.geekcert.com/sec504.html>

100% Passing Guarantee  
100% Money Back Assurance

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

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





### QUESTION 1

Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.

Which of the following is the mostly likely the cause of the problem?

- A. Computer is infected with the stealth kernel level rootkit.
- B. Computer is infected with stealth virus.
- C. Computer is infected with the Stealth Trojan Virus.
- D. Computer is infected with the Self-Replication Worm.

Correct Answer: A

---

### QUESTION 2

Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

- A. Piggybacking
- B. Hacking
- C. Session hijacking
- D. Keystroke logging

Correct Answer: C

---

### QUESTION 3

Fill in the blank with the correct numeric value. ARP poisoning is achieved in \_\_\_\_\_ steps.

- A. 2

Correct Answer: A

---

### QUESTION 4

Which of the following are open-source vulnerability scanners?



- A. Nessus
- B. Hackbot
- C. NetRecon
- D. Nikto

Correct Answer: ABD

---

#### QUESTION 5

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form.

Which of the following techniques is Sam using? Each correct answer represents a part of the solution.

Choose all that apply.

- A. Linguistic steganography
- B. Perceptual masking
- C. Technical steganography
- D. Text Semagrams

Correct Answer: AD

[SEC504 PDF Dumps](#)

[SEC504 Study Guide](#)

[SEC504 Exam Questions](#)