



GCIA^{Q&As}

GIAC Certified Intrusion Analyst

Pass GIAC GCIA Exam with 100% Guarantee

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

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

100% Passing Guarantee
100% Money Back Assurance

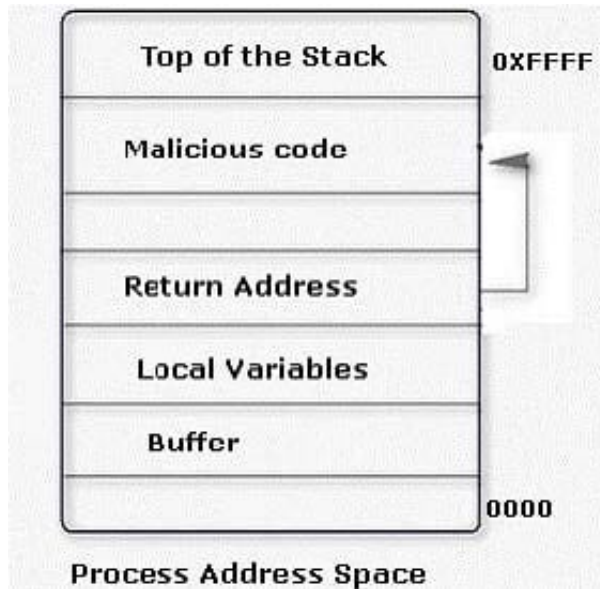
Following Questions and Answers are all new published by GIAC
Official Exam Center

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



**QUESTION 1**

An attacker changes the address of a sub-routine in such a manner that it begins to point to the address of the malicious code. As a result, when the function has been exited, the application can be forced to shift to the malicious code. The image given below explains this phenomenon:



Which of the following tools can be used as a countermeasure to such an attack?

- A. Obiwan
- B. SmashGuard
- C. Kismet
- D. Absinthe

Correct Answer: B

QUESTION 2

Rick works as the Network Administrator of Baby Blue Inc. He wants to upgrade the existing network to the Active Directory based Windows 2000 network. He configures a DNS on the network. Which of the following is the primary reason that the DNS is required in an Active Directory environment?

- A. Without installing the DNS, you cannot install the Active Directory in the network.
- B. Netlogon uses the DNS to find a domain controller in the network.
- C. The Active Directory uses the DNS zone transfer protocol during replication.
- D. The Active Directory is stored within the DNS database.

Correct Answer: B



QUESTION 3

_____ is a command-line tool that can check the DNS registration of a domain controller.

- A. NBTSTAT
- B. NETSH
- C. DNSCMD
- D. DCDIAG

Correct Answer: D

QUESTION 4

Which of the following commands will you use with the tcpdump command to capture the traffic from a filter stored in a file?

- A. tcpdump -A file_name
- B. tcpdump -D file_name
- C. tcpdump -X file_name
- D. tcpdump -F file_name

Correct Answer: D

QUESTION 5

John enters a URL <http://www.cisco.com/web/learning> in the web browser. A web page appears after he enters the URL. Which of the following protocols is used to resolve [www.cisco.com](http://www.cisco.com/web/learning) into the correct IP address?

- A. DNS
- B. SMTP
- C. DHCP
- D. ARP

Correct Answer: A

[Latest GCIA Dumps](#)

[GCIA VCE Dumps](#)

[GCIA Study Guide](#)