

# GIAC

GCIA  
*GIAC Intrusion Analyst*



**For More Information – Visit link below:**

**<https://www.examsboost.com/>**

## Product Version

- ✓ Up to Date products, reliable and verified.
- ✓ Questions and Answers in PDF Format.

---

# Latest Version: 6.0

## Question: 1

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company. You have physically installed sensors at all key positions throughout the network such that they all report to the command console.

What will be the key functions of the sensors in such a physical layout?

Each correct answer represents a complete solution. Choose all that apply.

Response:

- A. To collect data from operating system logs
- B. To notify the console with an alert if any intrusion is detected
- C. To analyze for known signatures
- D. To collect data from Web servers

**Answer: B,C**

## Question: 2

Which of the following monitors program activities and modifies malicious activities on a system?

Response:

- A. RADIUS
- B. NIDS
- C. Back door
- D. HIDS

**Answer: D**

## Question: 3

Which of the following tools can be used to check whether the network interface is in promiscuous mode or not?

Response:

- A. IPTraf
- B. MRTG
- C. Chkrootkit
- D. Ntop

---

**Answer: C**

**Question: 4**

Which of the following attacks involves multiple compromised systems to attack a single target?  
Response:

- A. Brute force attack
- B. DDoS attack
- C. Replay attack
- D. Dictionary attack

**Answer: B**

**Question: 5**

In which of the following attacks does a hacker imitate a DNS server and obtain the entire DNS database?  
Response:

- A. DNS poisoning attack
- B. Illicit zone transfer attack
- C. Illicit poisoning attack
- D. DNS transfer attack

**Answer: B**

**Question: 6**

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft's Windows XP operating system?  
Response:

- A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
- B. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe
- C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
- D. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe

**Answer: D**

### Question: 7

You work as a technician for Tech Perfect Inc. You are troubleshooting an Internet name resolution issue. You ping your ISP's DNS server address and find that the server is down. You want to continuously ping the DNS address until you have stopped the command.

Which of the following commands will you use?

Response:

- A. ping -a
- B. ping -l
- C. ping -t
- D. ping -n

**Answer: C**

### Question: 8

Which of the following types of write blocker device uses one interface for one side and a different one for the other?

Response:

- A. Pros
- B. Tailgate.
- C. Indiff
- D. Native

**Answer: B**

### Question: 9

Which of the following work as traffic monitoring tools in the Linux operating system?

Each correct answer represents a complete solution. Choose all that apply.

Response:

- A. MRTG
- B. John the Ripper
- C. IPTraf
- D. Ntop

**Answer: A,C,D**

---

### Question: 10

Routers work at which layer of the OSI reference model?

Response:

- A. Transport
- B. Physical
- C. Presentation
- D. Network

<b>Answer: D</b>
------------------

---

# Thank You for Trying Our Product

Discount Coupon Code:

**EXAMSBOOST10**

For More Information – **Visit link below:**

**<http://www.examsboost.com/>**



## FEATURES

- ✓ **90 Days Free Updates**
- ✓ **Money Back Pass Guarantee**
- ✓ **Instant Download or Email**

**Attachment**

- ✓ **24/7 Live Chat Support**
  - ✓ **PDF file could be used at any**
- Platform**

- ✓ **50,000 Happy Customer**

Visit us at <https://www.examsboost.com/test/gcia/>