



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

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He scans the We-are-secure server and gets the following result:

```
sysDescr.0 = STRING. "SunOS we-are-secure.com 4.1.3_U1 1 sun4m" sysObjectID.0 = OID.
```

```
enterprises.hp.nm.hpsystem.10.1.1
```

```
sysUpTime.0 = Timeticks: (156474552) 18 days, 12:00:09
```

```
sysContact.0 = STRING. ""
```

```
sysName.0 = STRING. "we-are-secure.com"
```

```
sysLocation.0 = STRING. ""
```

```
sysServices.0 = INTEGER: 6
```

Which of the following tools is John using to perform the scan?

- A. snmpwalk
- B. Kismet
- C. AirMagnet
- D. AiroPeek

Correct Answer: A

QUESTION 2

Which of the following is a form of cheating or copying someone else's work or idea without acknowledging the source?

- A. Patent
- B. Turnitin
- C. Copyright
- D. Plagiarism

Correct Answer: D

QUESTION 3

Which of the following terms describes an attempt to transfer DNS zone data?

- A. Reconnaissance



- B. Encapsulation
- C. Dumpster diving
- D. Spam

Correct Answer: A

QUESTION 4

You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross- Site Scripting attack on your company's Website. Which of the following methods of investigation can you use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

- A. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.
- B. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.
- C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.
- D. Look at the Web servers logs and normal traffic logging.

Correct Answer: ABD

QUESTION 5

The Intrusion Detection System (IDS) instructs the firewall to reject any request from a particular IP address if the network is repeatedly attacked from this address. What is this action known as?

- A. Spoofing
- B. Sending deceptive e-mails
- C. Network Configuration Changes
- D. Shunning
- E. Logging
- F. Sending notifications

Correct Answer: C

[Latest GCIA Dumps](#)

[GCIA PDF Dumps](#)

[GCIA Study Guide](#)