



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, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

- A. Rainbow attack
- B. DoS attack
- C. ARP spoofing
- D. Replay attack

Correct Answer: B

QUESTION 2

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 3

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Request for service, initial analysis, data collection, data reporting, data analysis



- B. Initial analysis, request for service, data collection, data analysis, data reporting
- C. Initial analysis, request for service, data collection, data reporting, data analysis
- D. Request for service, initial analysis, data collection, data analysis, data reporting

Correct Answer: D

QUESTION 4

Which of the following Windows Registry key contains the password file of the user?

- A. HKEY_USER
- B. HKEY_DYN_DATA
- C. HKEY_LOCAL_MACHINE
- D. HKEY_CURRENT_CONFIG

Correct Answer: C

QUESTION 5

Which of the following commands is a Packet sniffer?

- A. tcpdump
- B. strace
- C. nmap
- D. tail

Correct Answer: A

[Latest GCIA Dumps](#)

[GCIA Practice Test](#)

[GCIA Exam Questions](#)