



GSEC^{Q&As}

GIAC Security Essentials Certification

Pass GIAC GSEC Exam with 100% Guarantee

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

<https://www.passapply.com/gsec.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

SSL session keys are available in which of the following lengths?

- A. 40-bit and 128-bit.
- B. 64-bit and 128-bit.
- C. 128-bit and 1,024-bit.
- D. 40-bit and 64-bit.

Correct Answer: A

QUESTION 2

IPS devices that are classified as "In-line NIDS" devices use a combination of anomaly analysis, signature-based rules, and what else to identify malicious events on the network?

- A. Firewall compatibility rules
- B. Application analysis
- C. ICMP and UDP active scanning
- D. MAC address filtering

Correct Answer: B

QUESTION 3

Which of the following quantifies the effects of a potential disaster over a period of time?

- A. Risk Assessment
- B. Business Impact Analysis
- C. Disaster Recovery Planning
- D. Lessons Learned

Correct Answer: B

QUESTION 4

Regarding the UDP header below, what is the length in bytes of the UDP datagram?

04 1a 00 a1 00 55 db 51



A. 161

B. 81

C. 219

D. 85

Correct Answer: D

QUESTION 5

Which of the following heights of fence deters only casual trespassers?

A. 8 feet

B. 2 to 2.5 feet

C. 6 to 7 feet

D. 3 to 4 feet

Correct Answer: D

QUESTION 6

You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?

No. .	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (pi

A. Block DNS traffic across the router

B. Disable forwarding of unsolicited TCP requests

C. Disable IP-directed broadcast requests

D. Block UDP packets at the firewall

Correct Answer: C

QUESTION 7

Which of the following is a valid password for a system with the default "Password must meet complexity requirements" setting enabled as part of the GPO Password policy requirements?

A. The Cat Chased its Tail All Night



B. disk ACCESS failed

C. SETI@HOME

D. SaNS2006

Correct Answer: D

QUESTION 8

An employee attempting to use your wireless portal reports receiving the error shown below. Which scenario is occurring?



A. A denial-of-service attack is preventing a response from the portal.

B. Another access point is deauthenticating legitimate clients.

C. The encrypted data is being intercepted and decrypted.

D. Another access point is attempting to intercept the data.

Correct Answer: D

QUESTION 9

Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patches.

B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web application.

C. It is good practice to never use integrated Windows authentication for SQL Server.

D. It is good practice to not allow users to send raw SQL commands to the SQL Server.

Correct Answer: D



QUESTION 10

Where is the source address located in an IPv4 header?

- A. At an offset of 20 bytes
- B. At an offset of 8 bytes
- C. At an offset of 16 bytes
- D. At an offset of 12 bytes

Correct Answer: D

QUESTION 11

It is possible to sniff traffic from other hosts on a switched Ethernet network by impersonating which type of network device?

- A. Switch
- B. Bridge
- C. Hub
- D. Router

Correct Answer: D

QUESTION 12

How is a Distributed Denial of Service (DDOS) attack distinguished from a regular DOS attack?

- A. DDOS attacks are perpetrated by many distributed hosts.
- B. DDOS affects many distributed targets.
- C. Regular DOS focuses on a single router.
- D. DDOS affects the entire Internet.

Correct Answer: A

QUESTION 13

Which of the following terms refers to the process in which headers and trailers are added around user data?

- A. Encapsulation



B. Authentication

C. Authorization

D. Encryption

Correct Answer: A

QUESTION 14

Which of the following best describes the level of risk associated with using proprietary crypto algorithms.?

A. Proprietary cryptographic algorithms are required by law to use shorter key lengths in the United States, so the risk is high.

B. Proprietary algorithms have not been subjected to public scrutiny, so they have been checked less thoroughly for vulnerabilities.

C. Proprietary algorithms are less likely be vulnerable than algorithms that have been publicly disclosed because of enhanced secrecy of the algorithm.

D. Proprietary algorithms are not known to generally be any more or less vulnerable than publicly scrutinized algorithms.

Correct Answer: B

QUESTION 15

While using Wire shark to investigate complaints of users being unable to login to a web application, you come across an HTTP POST submitted through your web application. The contents of the POST are listed below. Based on what you see below, which of the following would you recommend to prevent future damage to your database?

```
POST /samplelogin.cfm HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/5.0 (X11; U; en-US;) Gecko/200910 Ubuntu/8.4
Firefox/2.6
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.example.com/
Cookie: SID=026DCB9CBBF2339C2CBFAEBA8F1DD656;
Content-Type: application/x-www-form-urlencoded
Content-Length: 64
username='a'&password=DROP+TABLE+members;+--
```

A. Use ssh to prevent a denial of service attack



- B. Sanitize user inputs to prevent injection attacks
- C. Authenticate users to prevent hackers from using your database
- D. Use https to prevent hackers from inserting malware

Correct Answer: D

[GSEC VCE Dumps](#)

[GSEC Practice Test](#)

[GSEC Study Guide](#)