GISF^{Q&As}

GIAC Information Security Fundamentals

Pass GIAC GISF Exam with 100% Guarantee

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

https://www.pass4itsure.com/gisf.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

What are the benefits of using a proxy server on a network? Each correct answer represents a complete solution. Choose all that apply.

A. It enhances network security.

B. It uses a single registered IP address for multiple connections to the Internet.

C. It cuts down dial-up charges.

D. It is used for automated assignment of IP addresses to a TCP/IP client in the domain.

Correct Answer: AB

QUESTION 2

You work as a Software Developer for Mansoft Inc. You have participated in the customization of a previously developed Configuration Management Application Block (CMAB) that manages an application configuration setting in multiple data stores. Based on requirements, you have extended the CMAB to read and write configuration data to and from an Oracle database. You need to create a unit test strategy. Which of the following steps would you include in a unit test of the CMAB? Each correct answer represents a part of the solution. Choose all that apply.

A. Perform White box testing

B. Regression test the existing functionality

C. Execute Use cases of the application

D. Perform Stress testing

E. Review the implementation

Correct Answer: ABE

QUESTION 3

Peter, a malicious hacker, wants to perform an attack. He first compromises computers distributed across the internet and then installs specialized software on these computers. He then instructs the compromised hosts to execute the attack. Every host can then be used to launch its own attack on the target computers. Which of the following attacks is Peter performing?

A. Teardrop attack

B. SYN flood attack

C. Ping of Death attack

D. DDoS attack

Correct Answer: D

QUESTION 4

The executive team wants you to track labor costs for your project as well as progress on task completion and the resulting dates. What information must you update for tasks to provide this information?

A. Start, Work, and Remaining Work

B. Actual Start and Percent Complete

C. Actual Start, Actual Work, and Remaining Work

D. Actual Start, Percent Complete, and Remaining Duration

Correct Answer: C

QUESTION 5

The TCP/IP protocol suite uses _____ to identify which service a certain packet is destined for.

A. Subnet masks

B. IP addresses

C. MAC addresses

D. Port numbers

Correct Answer: D

QUESTION 6

Which of the following is used to determine whether or not a principal is allowed to perform a requested action?

A. Authentication

B. Security policy

C. Authorization

D. Principal

Correct Answer: C

QUESTION 7

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory domain-based network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company\'s security policy, you want to apply Windows firewall setting to all the computers in the domain to improve security. Which of the following is the fastest and the most effective way to accomplish the task?

A. Apply firewall settings manually.

B. Apply firewall settings on the domain controller of the domain.

C. Use group policy to apply firewall settings.

D. Use a batch file to apply firewall setting.

Correct Answer: C

QUESTION 8

Which of the following are used as primary technologies to create a layered defense for giving protection

to a network?

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

A. Vulnerability

B. Firewall

C. Endpoint authentication

D. IDS

Correct Answer: BCD

QUESTION 9

Mark works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains four Windows 2008 member servers and 250 Windows Vista client computers. One of the member servers works as a Web server that hosts an intranet Web site. According to the company security policy, Mark needs to fulfill the following requirements:

1.

 Encryption should be used for authentication of all traffic to the Web site.

2.

 SSL should not be used on the Web server for performance reasons.

3.

 Users should be authenticated using their Active Directory credentials.

In order to fulfill the requirements, Mark has disabled the Anonymous Authentication setting on the server. What else does he have to do?

A. Enable the Anonymous Authentication setting on the server.

B. Enable the Encrypting File System (EFS) on the server.

C. Enable the Digest Authentication setting on the server.

D. Enable the Windows Authentication setting on the server.

Correct Answer: CD

QUESTION 10

You work as a SharePoint Administrator for TechWorld Inc. You must protect your SharePoint server farm from viruses that are accidentally uploaded to the SharePoint libraries. You have installed antivirus software that is designed for use with Windows SharePoint server. You have logged on to the Central Administration site. How can you configure the SharePoint site so that the document libraries are protected?

A. SharePoint does not support antivirus solutions.

B. Restrict users to read only on document libraries.

C. Choose the Scan documents on upload option in the antivirus settings.

D. Require all documents to be scanned on the local PC before uploading to the SharePoint sit e.

Correct Answer: C

QUESTION 11

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee\'s computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

A. Availability

B. Integrity

C. Confidentiality

D. Authenticity

Correct Answer: C

QUESTION 12

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Windows

B. Red Hat

C. Solaris

D. Knoppix

Correct Answer: A

QUESTION 13

Which of the following objects in an Active Directory serve as security principles? Each correct answer represents a part of the solution. Choose all that apply.

A. User accounts

B. Organizational units (OUs)

C. Computer accounts

D. Groups

Correct Answer: ACD

QUESTION 14

You are concerned about an attacker being able to get into your network. You want to make sure that you are informed of any network activity that is outside normal parameters. What is the best way to do this?

A. Utilize protocol analyzers.

B. User performance monitors.

C. Implement signature based antivirus.

D. Implement an anomaly based IDS.

Correct Answer: D

QUESTION 15

At which OSI layer does UDP operate?

A. Network layer

B. Data-link layer

C. Session layer

D. Transport layer

E. Presentation layer

Correct Answer: D