GIAC

GISF Exam

GIAC Information Security Fundamentals

[Questions & Answers Demo]

Version: 5.0

Question: 1

Your company is covered under a liability insurance policy, which provides various liabilitycoverage for information security risks, including any physical damage of assets, hacking attacks,etc. Which of the following risk management techniques is your company using?

A. Risk acceptance
B. Risk transfer
C. Risk avoidance
D. Risk mitigation

Answer: B

Question: 2

You have successfully installed an IRM server into your environment. This IRM server will be utilized to protect the company's videos, which are available to all employees but contain sensitive data. You log on to the WSS 3.0 server with administrator permissions and navigate to the Operations section. What option should you now choose so that you can input the RMS server name for the WSS 3.0 server to use?

A. Self-service site management
B. Content databases
C. Information Rights Management
D. Define managed paths

Answer: C

Question: 3

You work as a security manager for Qualxiss Inc. Your Company involves OODA loop for resolvingand deciding over company issues. You have detected a security breach issue in your company.
Which of the following procedures regarding the breach is involved in the observe phase of the OODA loop?

A. Follow the company security guidelines.
B. Decide an activity based on a hypothesis.
C. Implement an action practically as policies.
D. Consider previous experiences of security breaches.

Answer: A

Question: 4

How should you configure the Regional Centers' e-mail, so that it is secure and encrypted?
(Click the Exhibit button on the toolbar to see the case study.)

A. Use EFS.
B. Use IPSec.
C. Use S/MIME.
D. Use TLS.

Answer: C

Question: 5

How long are cookies in effect if no expiration date is set?

A. Fifteen days
B. Until the session ends.
C. Forever
D. One year

Answer: B

Question: 6

You work as a Network Administrator for ABC Inc. The company has a secure wireless network. However, in the last few days, an attack has been taking place over and over again. This attack istaking advantage of ICMP directed broadcast. To stop this attack, you need to disable ICMPdirected broadcasts. Which of the following attacks is taking place?

A. Smurf attack
B. Sniffer attack
C. Cryptographic attack
D. FMS attack

Answer: A

Question: 7

Which of the following statements are true about Dsniff?
Each correct answer represents a complete solution. Choose two.

A. It is a virus.
B. It contains Trojans.

C. It is antivirus.
D. It is a collection of various hacking tools.

Answer: B,D

Question: 8

Based on the information given in the case study, which two authentication methods should youuse to allow customers to access their photos on the Web site?
(Click the Exhibit button on the toolbar to see the case study.)
Each correct answer represents a part of the solution. Choose two.

A. Basic authentication without SSL
B. Digest authentication with SSL
C. Integrated Windows authentication
D. Anonymous access
E. Basic authentication with SSL
F. Digest authentication without SSL

Answer: B,E

Question: 9

Which of the following are the goals of the cryptographic systems?
Each correct answer represents a complete solution. Choose three.

A. Availability
B. Authentication
C. Confidentiality
D. Integrity

Answer: B,C,D

Question: 10

John works as an Exchange Administrator for Apple Inc. The company has a Windows 2003 ActiveDirectory domain-based network. The network contains several Windows Server 2003 servers. Threeof them have been configured as domain controllers. John complains to the Network Administrator thathe is unable to manage group memberships. Which of the following operations master roles isresponsible for managing group memberships?

A. PDC emulator
B. Infrastructure master
C. Schema master
D. RID master

Answer: B

Question: 11

You are the project manager of SST project. You are in the process of collecting and distributing performance information including status report, progress measurements, and forecasts. Which of the following process are you performing?

A. Perform Quality Control
B. Verify Scope
C. Report Performance
D. Control Scope

Answer: C

Question: 12

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning:
nmap -PN -p- -sI IP_Address_of_Company_Server
He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.
Which of the following security policies is the company using during this entire process to mitigate therisk of hacking attacks?

A. Audit policy
B. Antivirus policy
C. Non-disclosure agreement
D. Acceptable use policy

Answer: A

Question: 13

Which of the following protocols provides secured transaction of data between two computers?

A. SSH
B. FTP
C. Telnet
D. RSH

Answer: A

Question: 14

A firewall is a combination of hardware and software, used to provide security to a network. It isused to protect an internal network or intranet against unauthorized access from the Internet orother outside networks. It restricts inbound and outbound access and can analyze all trafficbetween an internal network and the Internet. Users can configure a firewall to pass or blockpackets from specific IP addresses and ports. Which of the following tools works as a firewall forthe Linux 2.4 kernel?

A. IPChains
B. OpenSSH
C. Stunnel
D. IPTables

Answer: D

Question: 15

Which of the following concepts represent the three fundamental principles of informationsecurity? Each correct answer represents a complete solution. Choose three.

A. Privacy
B. Availability
C. Integrity
D. Confidentiality

Answer: B,C,D

Question: 16

You work as a Software Developer for Mansoft Inc. You create an application. You want to use the application to encrypt data. You use the HashAlgorithmType enumeration to specify the algorithm used for generating Message Authentication Code (MAC) in Secure Sockets Layer (SSL) communications.
Which of the following are valid values for HashAlgorithmType enumeration?
Each correct answer represents a part of the solution. Choose all that apply.

A. MD5
B. None
C. DES
D. RSA
E. SHA1
F. 3DES

Answer: A,B,E

Question: 17

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you thinkare the reasons why the antivirus installed on the server did not detect the virus injected by John?
Each correct answer represents a complete solution. Choose all that apply.

A. The virus, used by John, is not in the database of the antivirus program installed on the ser ver.
B. The mutation engine of the virus is generating a new encrypted code.
C. John has created a new virus.
D. John has changed the signature of the virus.

Answer: A,B,C,D

Question: 18

Which of the following types of virus is capable of changing its signature to avoid detection?

A. Stealth virus
B. Boot sector virus
C. Macro virus
D. Polymorphic virus

Answer: D

Question: 19

Which of the following protocols can help you get notified in case a router on a network fails?

A. SMTP
B. SNMP
C. TCP
D. ARP

Answer: B

Question: 20

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages, providing Information and Cyber security, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Cryptography
B. OODA loop
C. Risk analysis

D. Firewall security

Answer: A

Question: 21

In a complex network, Router transfers data packets by observing some form of parameters or metrics provided in the routing table. Which of the following metrics is NOT included in the routing table?

A. Bandwidth
B. Load
C. Delay
D. Frequency

Answer: D

Question: 22

Mark is implementing security on his e-commerce site. He wants to ensure that a customer sending a message is really the one he claims to be. Which of the following techniques will he use to ensure this?

A. Packet filtering
B. Authentication
C. Firewall
D. Digital signature

Answer: D

Question: 23

You work as a Network Administrator for Net World Inc. The company has a TCP/IP-based network. You have configured an Internet access router on the network. A user complains that he is unable to access a resource on the Web. You know that a bad NAT table entry is causing the issue. You decide to clear all the entries on the table. Which of the following commands will you use?

A. show ip dhcp binding
B. ipconfig /flushdns
C. ipconfig /all
D. clear ip nat translation *

Answer: D

Question: 24

You are a Consumer Support Technician. You are helping a user troubleshoot computer-related issues. While troubleshooting the user's computer, you find a malicious program similar to a virus or worm. The program negatively affects the privacy and security of the computer and is capable of damaging the computer. Which of the following alert levels of Windows Defender is set for thisprogram?

A. Low
B. High
C. Severe
D. Medium

Answer: C

Question: 25

Which of the following provides a credential that can be used by all Kerberos-enabled servers and applications?

A. Remote Authentication Dial In User Service (RADIUS)
B. Internet service provider (ISP)
C. Network Access Point (NAP)
D. Key Distribution Center (KDC)

Answer: D

Question: 26

You work as an Exchange Administrator for TechWorld Inc. The company has a Windows 2008 Active Directory-based network. The network contains an Exchange Server 2010 organization. The messagingorganization contains one Hub Transport server, one Client Access server, and two Mailbox servers.
You are planning to deploy an Edge Transport server in your messaging organization to minimize theattack surface. At which of the following locations will you deploy the Edge Transport server?

A. Active Directory site
B. Intranet
C. Behind the inner firewall of an organization
D. Perimeter network

Answer: D

Question: 27

You are a Product manager of Marioxiss Inc. Your company management is having a conflict with another company Texasoftg Inc. over an issue of security policies. Your legal advisor has prepared a document that includes the negotiation of views for both the companies. This solution is supposed

tobe the key for conflict resolution. Which of the following are the forms of conflict resolution that have been employed by the legal advisor?
Each correct answer represents a complete solution. Choose all that apply.

A. Orientation
B. Mediation
C. Negotiation
D. Arbitration

Answer: B,C,D

Question: 28

You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will youemploy to accomplish the task?

A. Physical configuration audit
B. Configuration control
C. Functional configuration audit
D. Configuration identification

Answer: A

Question: 29

Availability Management allows organizations to sustain the IT service availability to support the business at a justifiable cost. Which of the following elements of Availability Management is used to perform at an agreed level over a period of time?
Each correct answer represents a part of the solution. Choose all that apply.

A. Maintainability
B. Resilience
C. Error control
D. Recoverability
E. Reliability
F. Security
G. Serviceability

Answer: A,B,D,E,F,G

Question: 30

Your company is going to add wireless connectivity to the existing LAN. You have concerns about the security of the wireless access and wish to implement encryption. Which of the following would be thebest choice for you to use?

A. WAP
B. WEP
C. DES
D. PKI

Answer: B