

Exam Questions GISF

GIAC Information Security Fundamentals

<https://www.2passeasy.com/dumps/GISF/>



NEW QUESTION 1

- (Topic 1)

Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

- A. Cross-Site Request Forgery
- B. Code injection attack
- C. Cross-Site Scripting attack
- D. Command injection attack

Answer: B

NEW QUESTION 2

- (Topic 1)

Key Distribution Center is used in which authentication method?

- A. Multi-factor
- B. Smart cards
- C. Biometrics
- D. Security tokens
- E. Kerberos
- F. Challenge Handshake Authentication Protocol

Answer: E

NEW QUESTION 3

- (Topic 1)

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 this program?

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

Answer: C

NEW QUESTION 4

- (Topic 1)

Security is responsible for well-being of information and infrastructures in which the possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security?

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

- A. Availability
- B. Confidentiality
- C. Confidentiality
- D. Authenticity

Answer: ABCD

NEW QUESTION 5

- (Topic 1)

Which of the following statements about testing are true?

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

- A. A stub is a program that simulates a calling unit, and a driver is a program that simulates a called unit.
- B. In unit testing, each independent unit of an application is tested separately.
- C. In integration testing, a developer combines two units that have already been tested into a component.
- D. The bottom-up approach to integration testing helps minimize the need for stubs.

Answer: BCD

NEW QUESTION 6

- (Topic 1)

According to the case study, what protocol should be used to protect a customer's privacy and credit card information?
(Click the Exhibit button on the toolbar to see the case study.)

- A. L2TP
- B. FTP
- C. HTTP
- D. MS-CHAP
- E. HTTPS
- F. PPTP

Answer: E

NEW QUESTION 7

- (Topic 1)

You work as an executive manager for Mariotx.Inc. You entered into a business contract with a firm called Helfixnet.Inc. You passed on the contract details to Helfixnet.Inc and also got an acceptance approval. You later find that Helfixnet.Inc is violating the rules of the contract and they claim that they had never entered into any contract with Mariotx.Inc when asked. Which of the following directives of Information Assurance can you apply to ensure prevention from such issues?

- A. Confidentiality
- B. Non-repudiation
- C. Data integrity
- D. Data availability

Answer: B

NEW QUESTION 8

- (Topic 1)

Which of the following is a valid IP address for class B Networks?

- A. 172.157.88.3
- B. 80.33.5.7
- C. 212.136.45.8
- D. 225.128.98.7

Answer: A

NEW QUESTION 9

- (Topic 1)

Which of the following cryptographic algorithm uses public key and private key to encrypt or decrypt data?

- A. Symmetric
- B. Numeric
- C. Hashing
- D. Asymmetric

Answer: D

NEW QUESTION 10

- (Topic 1)

You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus.

Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

- A. Recovery
- B. Identification
- C. Containment
- D. Eradication

Answer: D

NEW QUESTION 10

- (Topic 1)

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

NEW QUESTION 11

- (Topic 1)

You have been assigned the task of selecting a hash algorithm. The algorithm will be specifically used to ensure the integrity of certain sensitive files. It must use a 128 bit hash value. Which of the following should you use?

- A. SHA
- B. AES
- C. MD5
- D. DES

Answer: C

NEW QUESTION 13

- (Topic 1)

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

- A. The Configuration Manager
- B. The Supplier Manager
- C. The IT Service Continuity Manager
- D. The Service Catalogue Manager

Answer: B

NEW QUESTION 15

- (Topic 1)

Which of the following statements about Secure Shell (SSH) are true? Each correct answer represents a complete solution. Choose three.

- A. It was designed as a replacement for TELNET and other insecure shells.
- B. It is a network protocol used primarily on Linux and Unix based systems.
- C. It allows data to be exchanged using a secure channel between two networked devices.
- D. It is the core routing protocol of the Internet.

Answer: ABC

NEW QUESTION 16

- (Topic 1)

Andrew works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains five Windows 2008 member servers and 120 Windows XP Professional client computers. Andrew is concerned about the member servers that are not meeting the security requirements as mentioned in the security policy of the company. Andrew wants to compare the current security settings of the member servers with the security template that is configured according to the security policy of the company. Which of the following tools will Andrew use to accomplish this?

- A. Security Configuration and Analysis Tool
- B. Active Directory Migration Tool (ADMT)
- C. Task Manager
- D. Group Policy Management Console (GPMC)

Answer: A

NEW QUESTION 20

- (Topic 1)

Which Wireless network standard operates at 2.4 GHz and transfers data at a rate of 54 Mbps?

- A. 802.11a
- B. 802.11n
- C. 802.11b
- D. 802.11g

Answer: D

NEW QUESTION 24

- (Topic 1)

You are working on your computer system with Linux Operating system. After working for a few hours, the hard disk goes to the inactive state (sleep). You try to restart the system and check the power circuits. You later discover that the hard disk has crashed. Which of the following precaution methods should you apply to keep your computer safe from such issues?

- A. Use Incident handling
- B. Use OODA loop
- C. Use Information assurance
- D. Use SMART model.

Answer: D

NEW QUESTION 28

- (Topic 1)

Which of the following network connectivity devices translates one protocol into another and is used to connect dissimilar network technologies?

- A. Hub
- B. Firewall
- C. Bridge
- D. Gateway

Answer: D

NEW QUESTION 32

- (Topic 1)

John works as a Network Administrator for Bordeaux Inc. He is planning to design a strategy, so that the employees can connect to a scheduling application. Which of the following strategies is best suited for the company?

(Click the Exhibit button on the toolbar to see the case study.)

- A. Deploy a VPN server on the VLAN network, and an IIS server on the corporate LAN at the headquarters.
- B. Deploy a VPN server on the VLAN network, and an IIS server on DMZ.
- C. Deploy a VPN server on the corporate LAN at the headquarters, and an IIS server on DMZ.
- D. Deploy a VPN server on DMZ, and an IIS server on the corporate LAN at the headquarters.

Answer: D

NEW QUESTION 34

- (Topic 1)

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

- A. Asymmetric encryption is faster as compared to symmetric encryption.
- B. Asymmetric encryption uses a public key and a private key pair for data encryption.
- C. In asymmetric encryption, only one key is needed to encrypt and decrypt data.
- D. In asymmetric encryption, the public key is distributed and the private key is available only to the recipient of the message.

Answer: BD

NEW QUESTION 36

- (Topic 1)

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

NEW QUESTION 37

- (Topic 1)

Your Company is receiving false and abusive e-mails from the e-mail address of your partner company. When you complain, the partner company tells you that they have never sent any such e-mails. Which of the following types of cyber crimes involves this form of network attack?

- A. Cyber squatting
- B. Cyber Stalking
- C. Man-in-the-middle attack
- D. Spoofing

Answer: D

NEW QUESTION 39

- (Topic 1)

Which of the following statements are TRUE regarding asymmetric encryption and symmetric encryption? Each correct answer represents a complete solution. Choose all that apply.

- A. Data Encryption Standard (DES) is a symmetric encryption key algorithm.
- B. In symmetric encryption, the secret key is available only to the recipient of the message.
- C. Symmetric encryption is commonly used when a message sender needs to encrypt a large amount of data.
- D. Asymmetric encryption uses a public key and a private key pair for data encryption.

Answer: ACD

NEW QUESTION 41

- (Topic 1)

Which of the following monitors program activities and modifies malicious activities on a system?

- A. Back door
- B. HIDS
- C. RADIUS
- D. NIDS

Answer: B

NEW QUESTION 42

- (Topic 1)

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 is taking advantage of ICMP directed broadcast. To stop this attack, you need to disable ICMP directed broadcasts. Which of the following attacks is taking place?

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

Answer: A

NEW QUESTION 46

- (Topic 1)

Which of the following types of authentications supported by OSPF? Each correct answer represents a complete solution. Choose three.

- A. MD5 authentication
- B. Simple password authentication
- C. Null authentication
- D. Kerberos v5 authentication

Answer: ABC

NEW QUESTION 49

CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate layer name.

The Network layer of the OSI model corresponds to the _____ layer of the TCP/IP model.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Internet

NEW QUESTION 52

- (Topic 1)

Your network utilizes a coax cable for connections between various network segments. Your predecessor made sure none of the coax cables were in an exposed area that could easily be accessed. This caused the use of significant extra cabling. Why do you think this was done?

- A. This was an error you should correct.
- B. It wastes the cable and may make maintenance more difficult.
- C. He was concerned about wireless interception of data.
- D. He was concerned about electromagnetic emanation being used to gather data.
- E. He was concerned about vampire taps.

Answer: D

NEW QUESTION 53

- (Topic 1)

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domainbased network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that Windows firewall allows or blocks?

- A. Configure Network address translation (NAT).
- B. Disable Windows firewall logging.
- C. Configure Internet Protocol Security (IPSec).
- D. Enable Windows firewall logging.

Answer: D

NEW QUESTION 54

- (Topic 1)

John works as a security manager in Mariotx.Inc. He has been tasked to resolve a network attack issue. To solve the problem, he first examines the critical information about the attacker's interaction to the network environment. He prepares a past record and behavioral document of the attack to find a direction of the solution. Then he decides to perform an action based on the previous hypothesis and takes the appropriate action against the attack. Which of the following strategies has John followed?

- A. Maneuver warfare
- B. Control theory
- C. SWOT Analysis
- D. OODA loop

Answer: D

NEW QUESTION 56

- (Topic 1)

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

- A. Install a DMZ firewall
- B. Enable verbose logging on the firewall
- C. Install a host-based IDS
- D. Install a network-based IDS

Answer: D

NEW QUESTION 58

- (Topic 1)

You work as a project manager for TYU project. You are planning for risk mitigation. You need to identify the risks that will need a more in-depth analysis. Which of the following activities will help you in this?

- A. Quantitative analysis
- B. Qualitative analysis
- C. Estimate activity duration
- D. Risk identification

Answer: B

NEW QUESTION 59

- (Topic 1)

What does Wireless Transport Layer Security (WTLS) provide for wireless devices? Each correct answer represents a complete solution. Choose all that apply.

- A. Data integrity
- B. Authentication
- C. Encryption
- D. Bandwidth

Answer: ABC

NEW QUESTION 61

- (Topic 1)

Mark work as a Network Administrator for Roadways Travel Inc. The company wants to implement a strategy for its external employees so that they can connect to Web based applications. What will Mark do to achieve this?

(Click the Exhibit button on the toolbar to see the case study.)

- A. He will install a VPN server in the VLAN, Roadways, and an IIS server in the corporate LAN at the headquarters.
- B. He will install a VPN server in the corporate LAN at the headquarters and an IIS server in the DMZ.
- C. He will install a VPN server in the DMZ and an IIS server in the corporate LAN at the headquarters.
- D. He will install a VPN server in the VLAN, Roadways, and an IIS server in the DMZ.

Answer: C

NEW QUESTION 64

- (Topic 1)

Which of the following is a remote access protocol that supports encryption?

- A. PPP
- B. SLIP
- C. UDP
- D. SNMP

Answer: A

NEW QUESTION 67

- (Topic 1)

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

NEW QUESTION 68

- (Topic 1)

Which of the following statements is not true about a digital certificate?

- A. It is used with both public key encryption and private key encryption.
- B. It is used with private key encryption.
- C. It is neither used with public key encryption nor with private key encryption.
- D. It is used with public key encryption.

Answer: D

NEW QUESTION 71

- (Topic 1)

Which of the following protocols are used by Network Attached Storage (NAS)? Each correct answer represents a complete solution. Choose all that apply.

- A. Apple Filing Protocol (AFP)
- B. Server Message Block (SMB)
- C. Network File System (NFS)
- D. Distributed file system (Dfs)

Answer: ABC

NEW QUESTION 76

- (Topic 1)

You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

- A. Quantitative risk analysis
- B. Risk audits
- C. Qualitative risk analysis
- D. Requested changes

Answer: D

NEW QUESTION 80

- (Topic 1)

A Cisco Unified Wireless Network has an AP that does not rely on the central control device of the network. Which type of AP has this characteristic?

- A. Lightweight AP
- B. Rogue AP
- C. LWAPP
- D. Autonomous AP

Answer: D

NEW QUESTION 82

- (Topic 1)

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: ABE

NEW QUESTION 86

- (Topic 1)

Tom works as the project manager for BlueWell Inc. He is working with his project to ensure timely and appropriate generation, retrieval, distribution, collection, storage, and ultimate disposition of project information. What is the process in which Tom is working?

- A. Stakeholder expectation management
- B. Stakeholder analysis
- C. Work performance measurement
- D. Project communication management

Answer: D

NEW QUESTION 87

- (Topic 1)

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want to the information security policies.

Which of the following are its significant steps?

Each correct answer represents a complete solution. Choose two.

- A. Awareness and Training Material Effectiveness
- B. Awareness and Training Material Development
- C. Awareness and Training Material Implementation
- D. Awareness and Training Program Design

Answer: BD

NEW QUESTION 91

- (Topic 1)

In which of the following access control models can a user not grant permissions to other users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

- A. Discretionary Access Control (DAC)
- B. Role Based Access Control (RBAC)
- C. Access Control List (ACL)
- D. Mandatory Access Control (MAC)

Answer: D

NEW QUESTION 94

- (Topic 1)

You work as a security manager for Qualxiss Inc. Your Company involves OODA loop for resolving and 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

NEW QUESTION 99

- (Topic 1)

Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

- A. NetBus
- B. EliteWrap
- C. Trojan Man
- D. Tiny

Answer: C

NEW QUESTION 103

- (Topic 1)

Which of the following are some of the parts of a project plan?

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

- A. Risk identification
- B. Project schedule
- C. Team members list
- D. Risk analysis

Answer: ABC

NEW QUESTION 106

- (Topic 1)

Which of the following protocols is used to provide remote monitoring and administration to network management machines on the network? The management machines will use this protocol to collect information for network monitoring. At times, the protocol can also be used for remote configuration.

- A. NNTP
- B. Telnet
- C. SSH
- D. SNMP

Answer: D

NEW QUESTION 107

- (Topic 1)

Which of the following cryptographic algorithms uses a single key to encrypt and decrypt data?

- A. Asymmetric
- B. Symmetric
- C. Numeric
- D. Hashing

Answer: B

NEW QUESTION 112

- (Topic 1)

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 messaging organization 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 the attack 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

NEW QUESTION 116

- (Topic 1)

You switch on your mobile Bluetooth device to transfer data to another Bluetooth device. Which of the following Information assurance pillars ensures that the data

transfer is being performed with the targeted authorized Bluetooth device and not with any other or unauthorized device?

- A. Data integrity
- B. Confidentiality
- C. Authentication
- D. Non-repudiation

Answer: C

NEW QUESTION 117

- (Topic 1)

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

NEW QUESTION 121

- (Topic 1)

Which of the following algorithms produce 160-bit hash values? Each correct answer represents a complete solution. Choose two.

- A. MD2
- B. MD5
- C. SHA-1
- D. SHA-0

Answer: CD

NEW QUESTION 124

- (Topic 1)

You are configuring the Terminal service. What Protocols are required with Terminal services? (Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a part of the solution. Choose two.

- A. L2TP
- B. TCP/IP
- C. RDP
- D. CHAP
- E. PPTP

Answer: BC

NEW QUESTION 125

- (Topic 1)

Which of the following tools are used to determine the hop counts of an IP packet? Each correct answer represents a complete solution. Choose two.

- A. Netstat
- B. Ping
- C. TRACERT
- D. IPCONFIG

Answer: BC

NEW QUESTION 129

- (Topic 1)

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

NEW QUESTION 131

- (Topic 1)

Which of the following processes is described in the statement below?

"It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

- A. Perform Quantitative Risk Analysis
- B. Perform Qualitative Risk Analysis

- C. Monitor and Control Risks
- D. Identify Risks

Answer: C

NEW QUESTION 132

- (Topic 1)

You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

- A. Denial-of-Service
- B. Eavesdropping
- C. Spoofing
- D. Packet manipulation

Answer: A

NEW QUESTION 133

- (Topic 1)

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

Answer: A

NEW QUESTION 134

- (Topic 1)

What does a firewall check to prevent certain ports and applications from getting the packets into an Enterprise?

- A. The application layer port numbers and the transport layer headers
- B. The presentation layer headers and the session layer port numbers
- C. The network layer headers and the session layer port numbers
- D. The transport layer port numbers and the application layer headers

Answer: D

NEW QUESTION 135

- (Topic 1)

Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

- A. Disaster Invocation Guideline
- B. Business Continuity Strategy
- C. Index of Disaster-Relevant Information
- D. Availability/ ITSCM/ Security Testing Schedule

Answer: B

NEW QUESTION 137

- (Topic 1)

You have decided to implement an intrusion detection system on your network. You primarily are interested in the IDS being able to recognized known attack techniques. Which type of IDS should you choose?

- A. Signature Based
- B. Passive
- C. Active
- D. Anomaly Based

Answer: A

NEW QUESTION 142

- (Topic 2)

You have been tasked with finding an encryption methodology for your company's network. The solution must use public key encryption which is keyed to the users email address. Which of the following should you select?

- A. AES
- B. 3DES
- C. PGP
- D. Blowfish

Answer: C

NEW QUESTION 145

- (Topic 2)

Which of the following is the process of making additional copies of data so that they may be used to restore the original after a data loss event?

- A. Data mining
- B. Back-up
- C. Data recovery
- D. File storage

Answer: B

NEW QUESTION 146

- (Topic 2)

Mark works as a Customer Support Technician for uCertify Inc. The company provides troubleshooting support to users. Mark is troubleshooting a computer of a user who is working on Windows Vista. The user reports that his sensitive data is being accessed by someone because of security vulnerability in the component of Windows Vista. Which of the following features of Windows Security Center should Mark configure to save the user's data?

- A. Automatic updating
- B. Firewall
- C. Malware protection
- D. Content Advisor

Answer: A

NEW QUESTION 148

- (Topic 2)

Which of the following types of cipher encrypts alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword?

- A. Block cipher
- B. Transposition cipher
- C. Vigen re cipher
- D. Stream cipher

Answer: C

NEW QUESTION 151

- (Topic 2)

You work as a Security manager for Orangesect Inc. The enterprise is using the OODA loop strategy to counter the security issues in the enterprise. Some of the IP addresses of the enterprise have been hacked. You match up the present hacking issue and condition with the past hacking experiences to find a solution. Which of the following phases of the OODA loop involves the procedure followed by you?

- A. The decide phase
- B. The orient phase
- C. The observe phase
- D. The act phase

Answer: B

NEW QUESTION 156

- (Topic 2)

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

Answer: D

NEW QUESTION 161

- (Topic 2)

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.

Answer: AB

NEW QUESTION 165

- (Topic 2)

Which of the following is the maximum variable key length for the Blowfish encryption algorithm?

- A. 448 bit

- B. 256 bit
- C. 64 bit
- D. 16 bit

Answer: A

NEW QUESTION 169

- (Topic 2)

How should you configure USSOWA1 and USSTIME1 to allow secure access for remote employees?

(Click the Exhibit button on the toolbar to see the case study.)

Each correct answer represents a complete solution. Choose three.

- A. Place USSTIME1 on the internal network
- B. Place USSOWA1 on the internal network
- C. Enable all connections from external network
- D. Place USSTIME1 in a DMZ
- E. Place USSOWA1 in a DMZ
- F. Allow only TCP port 443 connections from the external network
- G. Allow only TCP port 80 connections from the external network

Answer: DEF

NEW QUESTION 172

- (Topic 2)

The method used to encrypt messages by transposing or scrambling the characters in a certain manner is known as _____.

- A. Quantum cipher
- B. Transposition cipher
- C. Hybrid systems
- D. Mathematical cipher
- E. Substitution cipher
- F. Steganography

Answer: B

NEW QUESTION 175

- (Topic 2)

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

Answer: D

NEW QUESTION 179

- (Topic 2)

Which of the following techniques can be used by an administrator while working with the symmetric encryption cryptography? Each correct answer represents a complete solution. Choose all that apply.

- A. Transposition cipher
- B. Message Authentication Code
- C. Stream cipher
- D. Block cipher

Answer: BCD

NEW QUESTION 184

- (Topic 2)

Which of the following types of firewall functions at the Session layer of OSI model?

- A. Circuit-level firewall
- B. Application-level firewall
- C. Switch-level firewall
- D. Packet filtering firewall

Answer: A

NEW QUESTION 186

- (Topic 2)

Which of the following types of firewalls looks deep into packets and makes granular access control decisions?

- A. Stateful
- B. Application level proxy
- C. Circuit level proxy
- D. Packet filtering

Answer: B

NEW QUESTION 188

- (Topic 2)

Jane works as a Consumer Support Technician for McRoberts Inc. The company provides troubleshooting support to users. A user named Peter installs Windows Vista on his computer. He connects his computer on the network. He wants to protect his computer from malicious software and prevent hackers from gaining access to his computer through the network. Which of the following actions will Jane assist Peter to perform to accomplish the task?

- A. Don't stay logged on as an administrator.
- B. Use a firewall.
- C. Keep the computer up-to-date.
- D. Run antivirus software on the computer.

Answer: B

NEW QUESTION 190

- (Topic 2)

Which of the following is most useful against DOS attacks?

- A. Packet filtering firewall
- B. Honey pot
- C. Network surveys
- D. SPI firewall

Answer: D

NEW QUESTION 192

- (Topic 2)

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

NEW QUESTION 197

- (Topic 2)

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

- A. Web ripping
- B. Email spoofing
- C. Steganography
- D. Social engineering

Answer: C

NEW QUESTION 200

- (Topic 2)

Which of the following attacks saturates network resources and disrupts services to a specific computer?

- A. Teardrop attack
- B. Replay attack
- C. Denial-of-Service (DoS) attack
- D. Polymorphic shell code attack

Answer: C

NEW QUESTION 201

- (Topic 2)

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He enters a single quote in the input field of the login page of the Weare- secure Web site and receives the following error message:

Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'

This error message shows that the We-are-secure Website is vulnerable to ____.

- A. A buffer overflow
- B. An XSS attack
- C. A Denial-of-Service attack
- D. A SQL injection attack

Answer: D

NEW QUESTION 202

- (Topic 2)

The Information assurance pillars provide the surety of data availability to the users of an Information system. Which of the following network infrastructure techniques accomplishes the objective of an efficient data availability management on a network?

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

- A. SAN
- B. EFS
- C. NAS
- D. RAID

Answer: ACD

NEW QUESTION 206

- (Topic 2)

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

- A. PING attack
- B. Spoofing
- C. Hacking
- D. SYN attack

Answer: D

NEW QUESTION 211

- (Topic 2)

Which of the following refers to the emulation of the identity of a network computer by an attacking computer?

- A. Spoofing
- B. PING attack
- C. Hacking
- D. SYN attack

Answer: A

NEW QUESTION 215

- (Topic 2)

Peter is a merchant. He uses symmetric encryption to send confidential messages to different users of his Web site. Which of the following is the other name for asymmetric encryption?

- A. Session key encryption
- B. Public key encryption
- C. Secret key encryption
- D. Shared key encryption

Answer: B

NEW QUESTION 219

- (Topic 2)

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks? Each correct answer represents a complete solution. Choose all that apply.

- A. Dictionary attack
- B. Rule based attack
- C. Brute Force attack
- D. Hybrid attack

Answer: ACD

NEW QUESTION 222

- (Topic 2)

A company would like your consulting firm to review its current network and suggest changes that will increase its efficiency and optimize the business processes. To design such a network, you prepare a case study.

Which of the following policies should be implemented through a group policy that is associated with the netperfect.com domain?

(Click the Exhibit button on the toolbar to see the case study.)

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

- A. Account lockout policy.
- B. Password policy.
- C. Limit computers that can access production schedule software.
- D. Assign MS Office suite to appropriate users.

Answer: ABD

NEW QUESTION 223

- (Topic 2)

You are developing an online business solution for National Institute of Meteorological and Oceanographic Research (NIMOR). A case study for the organization is given in the exhibit. Based on the case study, you need to implement Internet security so that no user can hack confidential data. According to you, which of the following security options will you use for your solution? Each correct answer represents a complete solution. Choose all that apply. (Click the Exhibit button on the toolbar to see the case study.)

- A. Antivirus and antispymware software
- B. Secure Sockets Layer and digital certificates
- C. Firewall security
- D. Automatic Updates in Windows XP

Answer: AC

NEW QUESTION 225

- (Topic 2)

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. Look at the Web servers logs and normal traffic logging.
- 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. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.

Answer: ABD

NEW QUESTION 226

- (Topic 2)

Which of the following is an information gathering technique that is used to identify risks?

- A. Diagramming technique
- B. Assumption analysis
- C. Checklist analysis
- D. Delphi technique

Answer: D

NEW QUESTION 230

- (Topic 2)

Which of the following best describes the identification, analysis, and ranking of risks?

- A. Design of experiments
- B. Fast tracking
- C. Fixed-price contracts
- D. Plan Risk management

Answer: D

NEW QUESTION 233

- (Topic 2)

Rick is the project manager of a construction project. He is in a process to procure some construction equipments. There are four vendors available for supplying the equipments. Rick does not want one of them to participate in the bidding as he has some personal grudges against the owner of the vendor. This is the violation of which of the following categories of the Project Management Institute Code of Ethics and Professional Conduct?

- A. Respect
- B. Honesty
- C. Responsibility
- D. Fairness

Answer: D

NEW QUESTION 236

- (Topic 2)

Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

- A. Trademark laws
- B. Patent laws
- C. Copyright laws
- D. Code Security law

Answer: B

NEW QUESTION 238

- (Topic 2)

Which of the following can be used to protect a computer system from malware, viruses, spyware, and various types of keyloggers? Each correct answer represents a complete solution. Choose all that apply.

- A. KFSensor
- B. Sheep dip
- C. Enum
- D. SocketShield

Answer: BD

NEW QUESTION 241

- (Topic 2)

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases.

The email header of the suspicious email is given below:

What is the IP address of the sender of this email?

- A. 209.191.91.180
- B. 141.1.1.1
- C. 172.16.10.90
- D. 216.168.54.25

Answer: D

NEW QUESTION 246

- (Topic 2)

The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

- A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- B. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
- C. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices

Answer: B

NEW QUESTION 248

- (Topic 2)

You work as a Network Administrator for McRoberts Inc. You are required to upgrade a client computer on the company's network to Windows Vista Ultimate. During installation, the computer stops responding, and the screen does not change. What is the most likely cause?

- A. Teardrop attack
- B. Replay attack
- C. Denial-of-Service (DoS) attack
- D. Polymorphic shell code attack

Answer: C

NEW QUESTION 251

- (Topic 2)

Sam works as a Web Developer for McRobert Inc. He wants to control the way in which a Web browser receives information and downloads content from Web sites. Which of the following browser settings will Sam use to accomplish this?

- A. Proxy server
- B. Cookies
- C. Security
- D. Certificate

Answer: C

NEW QUESTION 255

- (Topic 2)

Web applications play a vital role in deploying different databases with user accessibility on the Internet. Which of the following allows an attacker to get unauthorized access to the database of a Web application by sending (attacking) user-supplied data to an interpreter as part of a command or query?

- A. Cross Site Scripting
- B. Injection flaw
- C. Cross Site Request Forgery (CSRF)
- D. Malicious File Execution

Answer: B

NEW QUESTION 259

- (Topic 2)

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e- mails. Which of the following will you use to accomplish this?

- A. NTFS
- B. PPTP
- C. PGP
- D. IPSec

Answer: C

NEW QUESTION 262

- (Topic 2)

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration.

The tool uses raw IP packets to determine the following:

What ports are open on our network systems. What hosts are available on the network. Identify unauthorized wireless access points.

What services (application name and version) those hosts are offering. What operating systems (and OS versions) they are running.

What type of packet filters/firewalls are in use. Which of the following tools is Victor using?

- A. Nessus
- B. Kismet
- C. Nmap
- D. Sniffer

Answer: C

NEW QUESTION 265

- (Topic 2)

Which of the following statements are true about TCP/IP model?

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

- A. It is consists of various protocols present in each layer.
- B. It describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network.
- C. It provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.
- D. It is generally described as having five abstraction layers.

Answer: ABC

NEW QUESTION 266

- (Topic 2)

Cryptography is the science of?

- A. Encrypting and decrypting plain text messages.
- B. Decrypting encrypted text messages.
- C. Encrypting plain text messages.
- D. Hacking secure information.

Answer: A

NEW QUESTION 270

- (Topic 2)

You and your project team want to perform some qualitative analysis on the risks you have identified and documented in Project Web Access for your project. You would like to create a table that captures the likelihood and affect of the risk on the project. What type of a chart or table would you like to create for the project risks?

- A. Risk Breakdown Structure

- B. Risk Probability and Impact Matrix
- C. Risk Review Table
- D. Risk Impact and Affect Matrix

Answer: B

NEW QUESTION 272

- (Topic 2)

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

- A. Sensitive
- B. Unclassified
- C. Confidential
- D. Public
- E. Secret
- F. Private

Answer: ACDF

NEW QUESTION 275

- (Topic 2)

You work as a Network Administrator for Tech Perfect Inc. The company has recruited a large number of fresh employees. You have been asked to give them a presentation on data protection and confidentiality to ensure a secure wireless communication between the employees. What types of information require confidentiality? Each correct answer represents a complete solution. Choose all that apply.

- A. Information that is public
- B. Information that reveals technical data
- C. Information that may reveal systems relationships
- D. Information that may reveal organizational relationships

Answer: BCD

NEW QUESTION 279

- (Topic 2)

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.

Answer: C

NEW QUESTION 281

- (Topic 2)

Firekiller 2000 is an example of a _____.

- A. DoS attack Trojan
- B. Data sending Trojan
- C. Remote access Trojan
- D. Security software disabler Trojan

Answer: D

NEW QUESTION 282

- (Topic 2)

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. John wants to redirect all TCP port 80 traffic to UDP port 40, so that he can bypass the firewall of the We-are-secure server. Which of the following tools will John use to accomplish his task?

- A. PsList
- B. Fpipe
- C. Cain
- D. PsExec

Answer: B

NEW QUESTION 287

- (Topic 2)

You work as a Network Administrator for NetTech Inc. Employees in remote locations connect to the company's network using Remote Access Service (RAS). Which of the following will you use to protect the network against unauthorized access?

- A. Antivirus software

- B. Gateway
- C. Firewall
- D. Bridge

Answer: C

NEW QUESTION 290

- (Topic 2)

Which of the following types of firewall functions by creating two different communications, one between the client and the firewall, and the other between the firewall and the end server?

- A. Packet filter firewall
- B. Proxy-based firewall
- C. Stateful firewall
- D. Endian firew

Answer: B

NEW QUESTION 292

- (Topic 2)

You want to install a server that can be accessed by external users. You also want to ensure that these users cannot access the rest of the network. Where will you place the server?

- A. Intranet
- B. Local Area Network
- C. Internet
- D. Demilitarized Zone
- E. Extranet
- F. Wide Area Network

Answer: D

NEW QUESTION 293

- (Topic 2)

You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project?

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

- A. It provides the risk analysis of project configurations.
- B. It provides object, orient, decide and act strategy.
- C. It provides the versions for network devices.
- D. It provides a live documentation of the project.

Answer: CD

NEW QUESTION 298

- (Topic 2)

Which of the following prevents malicious programs from attacking a system?

- A. Smart cards
- B. Anti-virus program
- C. Firewall
- D. Biometric devices

Answer: B

NEW QUESTION 302

- (Topic 2)

Which of the following is the best approach to conflict resolution?

- A. Hard work and understanding
- B. Mutual respect and cooperation
- C. Flexibility
- D. Sincerity and hard work

Answer: B

NEW QUESTION 303

- (Topic 2)

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

Answer: C

NEW QUESTION 307

- (Topic 3)

You have purchased a wireless router for your home network. What will you do first to enhance the security?

- A. Change the default password and administrator's username on the router
- B. Disable the network interface card on the computer
- C. Configure DMZ on the router
- D. Assign a static IP address to the computers

Answer: A

NEW QUESTION 308

- (Topic 3)

Which of the following protocols is used to prevent switching loops in networks with redundant switched paths?

- A. Cisco Discovery Protocol (CDP)
- B. Spanning Tree Protocol (STP)
- C. File Transfer Protocol (FTP)
- D. VLAN Trunking Protocol (VTP)

Answer: B

NEW QUESTION 312

- (Topic 3)

Which of the following are the types of Intrusion detection system?

- A. Server-based intrusion detection system (SIDS)
- B. Client based intrusion detection system (CIDS)
- C. Host-based intrusion detection system (HIDS)
- D. Network intrusion detection system (NIDS)

Answer: CD

NEW QUESTION 316

- (Topic 3)

You are the project manager for a software technology company. You and the project team have identified that the executive staff is not fully committed to the project. Which of the following best describes the risk?

- A. Residual risks
- B. Trend analysis
- C. Schedule control
- D. Organizational risks

Answer: D

NEW QUESTION 318

- (Topic 3)

Which of the following logs contains events pertaining to security as defined in the Audit policy?

- A. DNS server log
- B. Application log
- C. System log
- D. Directory Service log
- E. Security log
- F. File Replication Service log

Answer: E

NEW QUESTION 323

- (Topic 3)

Which of the following devices or hardware parts employs SMART model system as a monitoring system?

- A. Modem
- B. RAM
- C. Hard disk
- D. IDS

Answer: C

NEW QUESTION 326

- (Topic 3)

Which of the following types of attack can guess a hashed password?

- A. Teardrop attack
- B. Evasion attack
- C. Denial of Service attack
- D. Brute force attack

Answer: D

NEW QUESTION 330

- (Topic 3)

You are the project manager for BlueWell Inc. You are reviewing the risk register for your project. The risk register provides much information to you, the project manager and to the project team during the risk response planning. All of the following are included in the risk register except for which item?

- A. Trends in qualitative risk analysis results
- B. Symptoms and warning signs of risks
- C. List of potential risk responses
- D. Network diagram analysis of critical path activities

Answer: D

NEW QUESTION 333

- (Topic 3)

The IT Director of the company is very concerned about the security of the network. Which audit policy should he implement to detect possible intrusions into the network? (Click the Exhibit button on the toolbar to see the case study.)

- A. The success and failure auditing for policy change.
- B. The success and failure auditing for process tracking.
- C. The success and failure auditing for logon events.
- D. The success and failure auditing for privilege use.

Answer: C

NEW QUESTION 338

- (Topic 3)

Which of the following wireless security features provides the best wireless security mechanism?

- A. WPA with 802.1X authentication
- B. WPA with Pre Shared Key
- C. WPA
- D. WEP

Answer: A

NEW QUESTION 342

- (Topic 3)

You work as an Application Developer for uCertify Inc. The company uses Visual Studio .NET Framework 3.5 as its application development platform. You are working on a WCF service. You have decided to implement transport level security. Which of the following security protocols will you use?

- A. Kerberos
- B. HTTPS
- C. RSA
- D. IPSEC

Answer: B

NEW QUESTION 343

- (Topic 3)

You work as the project manager for Bluewell Inc. Your project has several risks that will affect several stakeholder requirements. Which project management plan will define who will be available to share information on the project risks?

- A. Risk Management Plan
- B. Communications Management Plan
- C. Stakeholder management strategy
- D. Resource Management Plan

Answer: B

NEW QUESTION 347

- (Topic 3)

Which of the following Windows Security Center features is implemented to give a logical layer protection between computers in a networked environment?

- A. Firewall
- B. Automatic Updating
- C. Other Security Settings
- D. Malware Protection

Answer: A

NEW QUESTION 350

- (Topic 3)

Which of the following are the benefits of information classification for an organization?

- A. It helps identify which information is the most sensitive or vital to an organization.
- B. It ensures that modifications are not made to data by unauthorized personnel or processes
- C. It helps identify which protections apply to which information.
- D. It helps reduce the Total Cost of Ownership (TCO).

Answer: AC

NEW QUESTION 353

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual GISF Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the GISF Product From:

<https://www.2passeasy.com/dumps/GISF/>

Money Back Guarantee

GISF Practice Exam Features:

- * GISF Questions and Answers Updated Frequently
- * GISF Practice Questions Verified by Expert Senior Certified Staff
- * GISF Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * GISF Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year