GIAC

Exam Questions GISF

GIAC Information Security Fundamentals

NEW QUESTION 1
- (Topic 1)
John works as an Exchange Administrator for Apple Inc. The company has a Windows 2003 Active Directory domain-based network. The network contains several Windows Server 2003 servers. Three of them have been configured as domain controllers. John complains to the Network Administrator that he is unable to manage group memberships. Which of the following operations master roles is responsible for managing group memberships?

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

Answer: B

NEW QUESTION 2
- (Topic 1)
Which of the following types of attacks cannot be prevented by technical measures only?

A. Social engineering
B. Smurf DoS
C. Brute force
D. Ping flood attack

Answer: A

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)
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: ABDEFG

NEW QUESTION 5
- (Topic 1)
The new security policy requires you to encrypt all data transmitted from the laptop computers of sales personnel to the distribution centers. How will you implement the security requirements?
(Click the Exhibit button on the toolbar to see the case study.)

A. Use 40-bit encryption for Routing and Remote Access Service(RRAS) Serve
B. Use PPTP without packet filtering for VPN.
C. Use 128-bit encryption for Routing and Remote Access Service(RRAS) Serve
D. Use PPTP without packet filtering for VPN.
E. Use 128-bit encryption for Routing and Remote Access Service(RRAS) Serve
F. Use PPTP with packet filtering for VPN.
G. Use 40-bit encryption for the Routing and Remote Access Service(RRAS) Serve
H. Use PPTP with packet filtering for VPN.

Answer: C

NEW QUESTION 6
- (Topic 1)
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: BCD

NEW QUESTION 7
- (Topic 1)
Which U.S. government agency is responsible for establishing standards concerning cryptography for nonmilitary use?

A. American Bankers Association
B. Central Security Service (CSS)
C. National Institute of Standards and Technology (NIST)
D. International Telecommunications Union
E. Request for Comments (RFC)
F. National Security Agency (NSA)

Answer: C

NEW QUESTION 8
- (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 9
- (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 10
- (Topic 1)
Which of the following statements are true about UDP?
Each correct answer represents a complete solution. Choose all that apply.

A. UDP is an unreliable protocol.
B. FTP uses a UDP port for communication.
C. UDP is a connectionless protocol.
D. TFTP uses a UDP port for communication.
E. UDP works at the data-link layer of the OSI model.

Answer: ACD

NEW QUESTION 10
- (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 12
- (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 13
- (Topic 1)
Adam, a novice Web user is getting large amount of unsolicited commercial emails on his email address. He suspects that the emails he is receiving are the Spam. Which of the following steps will he take to stop the Spam?
Each correct answer represents a complete solution. Choose all that apply.

A. Forward a copy of the spam to the ISP to make the ISP conscious of the spam.
B. Send an email to the domain administrator responsible for the initiating IP address.
C. Report the incident to the FTC (The U.
D. Federal Trade Commission) by sending a copy of the spam message.
E. Close existing email account and open new email account.

Answer: AC

NEW QUESTION 15
- (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 18
- (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 22
- (Topic 1)
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 think are 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: ABCD

NEW QUESTION 26
- (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 27
- (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 30
- (Topic 1)
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. Risk analysis
B. Firewall security
C. OODA loop
D. Cryptography

Answer: D

NEW QUESTION 32
- (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 36
- (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 39
- (Topic 1)
The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

A. Biometric devices
B. Intrusion detection systems
C. Key card
D. CCTV Cameras

Answer: D

NEW QUESTION 40
- (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 42
- (Topic 1)
Which of the following are the examples of administrative controls?
Each correct answer represents a complete solution. Choose all that apply.

A. Data Backup
B. Security policy
C. Security awareness training
D. Auditing

Answer: BC

NEW QUESTION 44
- (Topic 1)
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

NEW QUESTION 46
- (Topic 1)
The Project Risk Management knowledge area focuses on which of the following processes?
Each correct answer represents a complete solution. Choose all that apply.

A. Risk Management Planning
B. Quantitative Risk Analysis
C. Potential Risk Monitoring
D. Risk Monitoring and Control

Answer: ABD

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 50
- (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 correc
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 55
- (Topic 1)
Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

NEW QUESTION 56
- (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 58

- (Topic 1)
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

Answer: ACD

NEW QUESTION 62
- (Topic 1)
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 you employ to accomplish the task?

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

Answer: A

NEW QUESTION 63
- (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 64
- (Topic 1)
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 the best choice for you to use?

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

Answer: B

NEW QUESTION 65
- (Topic 1)
Which of the following is not needed for effective procurement planning?

A. Activity resource management
B. Project schedule
C. Cost baseline
D. Quality risk analysis

Answer: D

NEW QUESTION 68
- (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 71
- (Topic 1)
The SALES folder has a file named XFILE.DOC that contains critical information about your company. This folder resides on an NTFS volume. The company's Senior Sales Manager asks you to provide security for that file. You make a backup of that file and keep it in a locked cupboard, and then you deny access on the file for the Sales group. John, a member of the Sales group, accidentally deletes that file. You have verified that John is not a member of any other group.

Although you restore the file from backup, you are confused how John was able to delete the file despite having no access to that file.
What is the most likely cause?

A. The Sales group has the Full Control permission on the SALES folder.
B. The Deny Access permission does not work on files.
C. The Deny Access permission does not restrict the deletion of files.
D. John is a member of another group having the Full Control permission on that file.

Answer: A

NEW QUESTION 72
- (Topic 1)
Which of the following provide data confidentiality services by encrypting the data sent between wireless systems?
Each correct answer represents a complete solution. Choose two.

A. MS-CHAP v2
B. WEP
C. PAP
D. WPA

Answer: BC

NEW QUESTION 75
- (Topic 1)
Which of the following are application layer protocols of Internet protocol (IP) suite? Each correct answer represents a complete solution. Choose two.

A. IGP
B. IGRP
C. Telnet
D. SMTP

Answer: CD

NEW QUESTION 76
- (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 78
- (Topic 1)
Which of the following techniques allows an attacker to take network traffic coming towards a host at one port and redirect it from that host to another host?

A. Blackbox testing
B. Firewalking
C. Brainstorming
D. Port redirection

Answer: D

NEW QUESTION 81
- (Topic 1)
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system. He wants to sniff the weare- secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

A. Hunt
B. IPChains
C. Ethercap
D. Tripwire

Answer: A

NEW QUESTION 84
- (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 85
- (Topic 1)
You want to ensure that everyone who sends you an email should encrypt it. However you do not wish to exchange individual keys with all people who send you emails. In order to accomplish this goal which of the following should you choose?

A. DES
B. AES
C. Symmetric Encryption
D. Public Key encryption

Answer: D

NEW QUESTION 90
- (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 94
- (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 95
- (Topic 1)
Which of the following options cannot be accessed from Windows Update?

A. Restore Hidden Updates
B. Check for Updates
C. View Update History
D. View AntiVirus Software Update

Answer: D

NEW QUESTION 96
- (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 101
- (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 103
- (Topic 1)
Which of the following does an anti-virus program update regularly from its manufacturer's Web site?

A. Hotfixes
B. Definition
C. Service packs
D. Permissions

Answer: B

NEW QUESTION 107
- (Topic 1)
Your company is covered under a liability insurance policy, which provides various liability coverage 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

NEW QUESTION 112
- (Topic 1)
Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer?

A. IPLog
B. Snort
C. Timbersee
D. Swatch

Answer: B

NEW QUESTION 113
- (Topic 1)
Based on the case study, to implement more security, which of the following additional technologies should you implement for laptop computers? (Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a complete solution. Choose two.

A. Encrypted Data Transmissions
B. Digital certificates
C. Two-factor authentication
D. PAP authentication
E. Encrypting File System (EFS)

Answer: BE

NEW QUESTION 117
- (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 121
- (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 126
- (Topic 1)
Which of the following are the differences between routed protocols and routing protocols?
Each correct answer represents a complete solution. Choose two.

A. A routing protocol is configured on an interface and decides the method of packet delivery.

B. A routing protocol decides the path for a packet through the network.
C. A routed protocol is configured on an interface and decides how a packet will be delivered.
D. A routed protocol works on the transport layer of the OSI model.

Answer: BC

NEW QUESTION 131
- (Topic 1)
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: BD

NEW QUESTION 133
- (Topic 1)
You work as a security manager in Mariotiss Inc. Your enterprise has been facing network and software security threats since a few months. You want to renew your current security policies and management to enhance the safety of your information systems. Which of the following is the best practice to initiate the renewal process from the lowest level with the least managerial effort?

A. Start the Incident handling process.
B. Change the entire security policy.
C. Perform an IT audit.
D. Switch to a new network infrastructure.

Answer: C

NEW QUESTION 137
- (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 139
- (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 143
- (Topic 1)
Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

A. Electronic Communications Privacy Act of 1986
B. Economic Espionage Act of 1996
C. Computer Fraud and Abuse Act
D. Wiretap Act

Answer: A

NEW QUESTION 145
- (Topic 2)
Which of the following evidences is NOT the potential evidence for Routers?

A. Routing tables
B. MAC address
C. ACL
D. Logs

Answer: B

NEW QUESTION 149
- (Topic 2)
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

Answer: C

NEW QUESTION 154
- (Topic 2)
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 157
- (Topic 2)
Which of the following refers to a small space having two sets of interlocking doors such that the first set of doors must close before the second set opens?

A. Man-trap
B. Man-in-the-middle
C. Demilitarized zone (DMZ)
D. Firewall

Answer: A

NEW QUESTION 161
- (Topic 2)
Which of the following processes is responsible for low risk, frequently occurring low cost changes?

A. Incident Management
B. IT Facilities Management
C. Request Fulfillment
D. Release Management

Answer: C

NEW QUESTION 162
- (Topic 2)
You are the Administrator for a corporate network. You are concerned about denial of service attacks. Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

A. Shorten the timeout for connection attempts.
B. Place a honey pot in the DMZ.
C. Implement a strong password policy.
D. Implement network based antivirus.

Answer: A

NEW QUESTION 167
- (Topic 2)
Which of the following tools can be used for stress testing of a Web server? Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Spyware
C. Scripts
D. Anti-virus software

Answer: AC

NEW QUESTION 169
- (Topic 2)
You work as a Network Administrator for Infosec Inc. You find that not only have security applications running on the server, including software firewalls, anti-virus programs, and anti-spyware programs been disabled, but anti-virus and anti-spyware definitions have also been deleted. You suspect that this situation has arisen due to malware infection. Which of the following types of malware is the most likely cause of the issue?

A. Whack-A-Mole

B. FireKiller 2000
C. Beast
D. SubSeven

Answer: B

NEW QUESTION 174
- (Topic 2)
Which of the following protocols provides connectionless integrity and data origin authentication of IP packets?

A. ESP
B. IKE
C. ISAKMP
D. AH

Answer: D

NEW QUESTION 176
- (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 180
- (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 185
CORRECT TEXT - (Topic 2)
Fill in the blank with the appropriate value. SHA-1 produces a _____ -bit message digest.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
SHA-1 produces a160-bit message digest

NEW QUESTION 186
- (Topic 2)
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

A. Availability
B. Integrity
C. Confidentiality
D. Non-repudiation

Answer: B

NEW QUESTION 189
- (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 191
- (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 193
- (Topic 2)
You discover that someone has been logging onto your network after office hours. After investigating this you find the login belongs to someone who left the company 12 months ago. What would have been the best method to prevent this?

A. A policy with time of day restrictions.
B. An IDS system.
C. A policy with account expiration.
D. A DMZ firewall.

Answer: C

NEW QUESTION 195
- (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 198
- (Topic 2)
You work as a Network Administrator for ABC Inc. The company uses a secure wireless network.
John complains to you that his computer is not working properly. What type of security
audit do you need to conduct to resolve the problem?

A. Operational audit
B. Non-operational audit
C. Independent audit
D. Dependent audit

Answer: C

NEW QUESTION 203
- (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 204
- (Topic 2)
Tom and Gary are in a debate over which software should be purchased as part of their project. Gary tells Tom that because he's the senior software developer and has been with the company for 12 years, he'll be making the decision on the software. What type of conflict resolution has happened in this instance?

A. Avoiding
B. Forcing
C. Compromising
D. Smoothing

Answer: B

NEW QUESTION 208

- (Topic 2)
You are the Network Administrator for a company that frequently exchanges confidential emails without outside parties (clients, vendors, etc.). You want those emails to be encrypted, however, you want the least overhead/difficulty in the encryption process. Which of the following should you choose?

A. MD5
B. DES
C. Symmetric Encryption
D. Asymmetric Encryption

Answer: D

NEW QUESTION 213
- (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 215
- (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 220
- (Topic 2)
Which of the following is the primary function of VPNs?

A. To establish private connections over public networks
B. To make virtual connections for remote access
C. To establish a wireless connections to networks
D. To access networks remotely

Answer: A

NEW QUESTION 221
- (Topic 2)
Your computer continues to operate even if its disk drive has failed. This ability is known as _____.

A. Recovery
B. Fault Tolerance
C. Backups
D. Disaster Recovery
E. Hashing
F. Independent Disks

Answer: B

NEW QUESTION 226
- (Topic 2)
Which of the following statements about Encapsulating Security Payload (ESP) are true? Each correct answer represents a complete solution. Choose two.

A. It can also be nested with the Layer Two Tunneling Protocol (L2TP).
B. It is an IPSec protocol.
C. It is a text-based communication protocol.
D. It uses TCP port 22 as the default port and operates at the application layer.

Answer: AB

NEW QUESTION 227
- (Topic 2)
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for uCertify Software Systems Pvt. Ltd.?
(Click the Exhibit button on the toolbar to see the case study.)

A. Providing secure communications between Washington and the headquarters office.
B. Implementing Certificate services on Texas office.
C. Preventing denial-of-service attacks.
D. Ensuring secure authentication.
E. Preventing unauthorized network access.
F. Providing two-factor authentication.
G. Protecting employee data on portable computers.
H. Providing secure communications between the overseas office and the headquarters.

Answer: DEGH

NEW QUESTION 232
- (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 antispyware software
B. Secure Sockets Layer and digital certificates
C. Firewall security
D. Automatic Updates in Windows XP

Answer: AC

NEW QUESTION 233
- (Topic 2)
Which of the following policies define how Identification and Authorization occur and determine access control, audits, and network connectivity?

A. Information policies
B. Usage policies
C. Security policies
D. Administrative policies
E. Disaster Recovery Plans
F. Design Requirements

Answer: C

NEW QUESTION 237
- (Topic 2)
Adam works as a Professional Penetration Tester for Umbrella Inc. A project has been assigned to him to carry out a Black Box penetration testing as a regular evaluation of the system security and integrity of the company's network. Which of the following statements are true about the Black Box penetration testing? Each correct answer represents a complete solution. Choose all that apply.

A. Black box testing provides the testers with complete knowledge of the infrastructure to be tested.
B. Black box testing simulates an attack from someone who is unfamiliar with the system.
C. Black box testing simulates an attack from someone who is familiar with the system.
D. Black box testing assumes no prior knowledge of the infrastructure to be tested.

Answer: BC

NEW QUESTION 241
- (Topic 2)
You are hired by Techmart Inc. to upgrade its existing network. You have prepared a case study for planning the network.
According to your study, how many domains are required to setup the network of Techmart Inc.?
(Click the Exhibit button on the toolbar to see the case study.)

A. Two
B. Four
C. Three
D. One

Answer: D

NEW QUESTION 243
- (Topic 2)
You work as a Network administrator for Infonet Inc. The company has 135 Windows XP Professional computers and twenty Windows 2003 Server computers. You want to specify the number of invalid logon attempts allowed before a user account is locked out. What will you do to accomplish the task?

A. Reset Account Lockout Counter After policy
B. Set Account Lockout Threshold policy
C. Enforce Password Must Meet Complexity Requirements policy
D. Set Account Lockout Duration policy

Answer: B

NEW QUESTION 248

- (Topic 2)
The workstations on your network utilize Windows XP (service pack 2 or later). Many users
take their laptops on the road. You are very concerned about the security and want to have a robust firewall solution for mobile users. You have decided that all your firewalls to use the Stateful Packet Inspection (SPI) method. What must you do to provide SPI to your mobile users?

A. You must purchase a third party firewall solution for your mobile users.
B. Do nothin
C. Windows XP service pack 2 has a firewall turned on by default.
D. Download the SPI template from Microsoft.
E. Configure the Windows XP firewall to use SPI.

Answer: A

NEW QUESTION 253
- (Topic 2)
Which of the following statements about Public Key Infrastructure (PKI) are true? Each correct answer represents a complete solution. Choose two.

A. It is a digital representation of information that identifies users.
B. It uses asymmetric key pairs.
C. It provides security using data encryption and digital signature.
D. It uses symmetric key pairs.

Answer: BC

NEW QUESTION 254
- (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 255
- (Topic 2)
Which of the following types of viruses can prevent itself from being detected by an antivirus application?

A. File virus
B. Boot sector virus
C. Multipartite virus
D. Stealth virus

Answer: D

NEW QUESTION 259
- (Topic 2)
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.

Answer: CD

NEW QUESTION 260
- (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 261

- (Topic 2)
Donna is the project manager for her organization. She is preparing a plan to manage changes to the project should changes be requested. Her change management plan defines the process for documenting, tracking, and determining if the changes should be approved or declined. What system is considered the parent of the change control system documented in Donna's plan?

A. Project Management Information System
B. Integrated Change Control System
C. Change Control System
D. Quality Management System

Answer: A

NEW QUESTION 266
- (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 270
- (Topic 2)
What is a variant with regard to Configuration Management?

A. A CI that has the same name as another CI but shares no relationship.
B. A CI that has the same essential functionality as another CI but a bit different in some small manner.
C. A CI that particularly refers to a hardware specification.
D. A CI that particularly refers to a software version.

Answer: B

NEW QUESTION 275
- (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 279
- (Topic 2)
Which of the following is the main purpose of using OODA loops?

A. Providing economic balance
B. Making the information delivery process faster
C. Information welfare
D. Creating advanced military weapons

Answer: C

NEW QUESTION 283
- (Topic 2)
Which of the following is the purpose of employing DMZ (Demilitarized zone) in a network?

A. It adds an additional layer of security to a Local Area Network (LAN).
B. It creates a check-point to a Local Area Network (LAN).
C. It adds an extra node to the Local Area Network (LAN).
D. It works along with the firewall to filter unwanted data packets.

Answer: A

NEW QUESTION 285
- (Topic 2)
Which of the following federal laws are related to hacking activities? Each correct answer represents a complete solution. Choose three.

A. 18 U.S.
B. 1029
C. 18 U.S.

D. 1028
E. 18 U.S.
F. 1030
G. 18 U.S.
H. 2510

Answer: ACD

NEW QUESTION 289
- (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 291
- (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 293
- (Topic 2)
Which of the following categories of the network management model is used to detect and log network problems or device failures?

A. Fault Management
B. Configuration Management
C. Security Management
D. Performance Management

Answer: A

NEW QUESTION 298
- (Topic 2)
At which OSI layer does UDP operate?

A. Network layer
B. Data-link layer
C. Session layer
D. Transport layer
E. Presentation layer

Answer: D

NEW QUESTION 299
- (Topic 2)
You work as a Software Developer for Mansoft Inc. You, together with a team, develop a distributed application that processes orders from multiple types of clients. The application uses SQL Server to store data for all orders. The application does not implement any custom performance counters. After the application is deployed to production, it must be monitored for performance spikes. What will you do to monitor performance spikes in the application in a deployment environment?
Each correct answer represents a part of the solution. Choose all that apply.

A. Use SQL Profiler
B. Use CLR Profiler
C. Use Windows System Monitor
D. Use Microsoft Operations Manager

Answer: ACD

NEW QUESTION 302
- (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. Antivirus software is running on the computer.

B. You have provided an improper product key.
C. The computer is running a driver that is incompatible with Vista.
D. The computer has a hardware device that is incompatible with Vista.

Answer: A

NEW QUESTION 307
- (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 310
- (Topic 2)
Which of the following is the phase of Incident handling process in which the distinction between an event and an incident is made?

A. Preparation phase
B. Eradication phase
C. Differential phase
D. Identification phase

Answer: D

NEW QUESTION 311
- (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 313
- (Topic 2)
Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?

A. The Service Level Manager
B. The Configuration Manager
C. The IT Security Manager
D. The Change Manager

Answer: C

NEW QUESTION 314
- (Topic 2)
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

Answer: C

NEW QUESTION 316
- (Topic 2)
Each time you start your computer, you receive an error message that your TCP/IP address is in use. Which of the following attacks is this?

A. Worm attack
B. ICMP attack
C. Back door attack
D. TCP/IP hijacking
E. TCP Sequence Number attack
F. TCP SYN or TCP ACK flood attack

Answer: D

NEW QUESTION 321
- (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 326
- (Topic 3)
You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of _____.

A. Bribery
B. Irresponsible practice
C. Illegal practice
D. Conflict of interest

Answer: D

NEW QUESTION 328
- (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 332
- (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 335
- (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 338
- (Topic 3)
You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution? Each correct answer represents a part of the solution. Choose all that apply.

A. Recovery
B. Contamination
C. Identification
D. Eradication
E. Preparation

Answer: ABD

NEW QUESTION 342
- (Topic 3)

You work as the Security Administrator for Prodotxiss Inc. You want to ensure the security of your Wi-Fi enterprise network against the wireless snooping attacks. Which of the following measures will you take over the site network devices of the network?

A. Apply firewalls at appropriate spots.
B. Download and install new firmware patch for the router.
C. Disable the SSID broadcast feature of the router.
D. Apply a standard ACL on the router.

Answer: C

NEW QUESTION 344
- (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 348
- (Topic 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

Answer: D

NEW QUESTION 350
- (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 353
- (Topic 3)
You are the Network Administrator for a bank. You discover that someone has logged in with a user account access, but then used various techniques to obtain access to other user accounts. What is this called?

A. Vertical Privilege Escalation
B. Session Hijacking
C. Account hijacking
D. Horizontal Privilege Escalation

Answer: D

NEW QUESTION 354
- (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 359
- (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 362
- (Topic 3)
John is a merchant. He has set up a LAN in his office. Some important files are deleted as a result of virus attack. John wants to ensure that it does not happen again. What will he use to protect his data from virus?

A. Antivirus
B. Backup
C. Symmetric encryption
D. Firewall

Answer: A

NEW QUESTION 363
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

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