

# GIAC

## Exam Questions GISF

GIAC Information Security Fundamentals



#### NEW QUESTION 1

- (Topic 1)

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

- A. Public key
- B. Digital certificates
- C. Twofish
- D. RSA

**Answer:** AB

#### NEW QUESTION 2

- (Topic 1)

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions, which is available to the Internet. Which of the following security threats may occur if DMZ protocol attacks are performed?

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

- A. Attacker can exploit any protocol used to go into the internal network or intranet of the company.
- B. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.
- C. Attacker can gain access to the Web server in a DMZ and exploit the database.
- D. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

**Answer:** ACD

#### NEW QUESTION 3

- (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 4

- (Topic 1)

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?

- A. F936.28A1.5BCD.DEFA
- B. A3-07-B9-E3-BC-F9
- C. 1011-0011-1010-1110-1100-0001
- D. 132.298.1.23

**Answer:** B

#### NEW QUESTION 5

- (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 6

- (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 7

- (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 8

- (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 9

- (Topic 1)

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

- A. By examining your firewall logs.
- B. By examining your domain controller server logs.
- C. By setting up a DMZ.
- D. You cannot, you need an IDS.

**Answer:** A

#### NEW QUESTION 10

- (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 10

- (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 14

- (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 18

- (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 22

- (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 25

- (Topic 1)

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning:

```
nmap -PN -p- -sI IP_Address_of_Company_Server
```

He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.

Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

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

**Answer:** A

#### NEW QUESTION 30

- (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 32

- (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 36

- (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 38

- (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 39

- (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 43

- (Topic 1)

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 46

- (Topic 1)

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

Each correct answer represents a part of the solution. Choose all that apply.

- A. Perform White box testing
- B. Regression test the existing functionality
- C. Execute Use cases of the application
- D. Perform Stress testing
- E. Review the implementation

**Answer:** ABE

#### NEW QUESTION 47

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 48

- (Topic 1)

Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

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

**Answer:** B

#### NEW QUESTION 49

- (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 50**

- (Topic 1)

You and your project team have identified the project risks and now are analyzing the probability and impact of the risks. What type of analysis of the risks provides a quick and high-level review of each identified risk event?

- A. A risk probability-impact matrix
- B. Quantitative risk analysis
- C. Qualitative risk analysis
- D. Seven risk responses

**Answer:** C

**NEW QUESTION 52**

- (Topic 1)

Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

- A. Corrective controls
- B. Detective controls
- C. Safeguards
- D. Preventive controls

**Answer:** A

**NEW QUESTION 54**

- (Topic 1)

Which of the following statements about digital signature is true?

- A. Digital signature is required for an e-mail message to get through a firewall.
- B. Digital signature verifies the identity of the person who applies it to a document.
- C. Digital signature decrypts the contents of documents.
- D. Digital signature compresses the message to which it is applied.

**Answer:** B

**NEW QUESTION 56**

- (Topic 1)

You are a Product manager of Marioxiss Inc. Your company management is having a conflict with another company Texasoftg Inc. over an issue of security policies. Your legal advisor has prepared a document that includes the negotiation of views for both the companies. This solution is supposed to be the key for conflict resolution. Which of the following are the forms of conflict resolution that have been employed by the legal advisor?

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

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

**Answer:** BCD

**NEW QUESTION 59**

- (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 61**

- (Topic 1)

Which of the following books is used to examine integrity and availability?

- A. Brown Book
- B. Red Book
- C. Purple Book
- D. Orange Book

**Answer:** B

#### NEW QUESTION 66

- (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 70

- (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 72

- (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 73

- (Topic 1)

Which of the following is the most secure place to host a server that will be accessed publicly through the Internet?

- A. A DNS Zone
- B. An Intranet
- C. A demilitarized zone (DMZ)
- D. A stub zone

**Answer:** C

#### NEW QUESTION 77

- (Topic 1)

The MBR of a hard disk is a collection of boot records that contain disk information such as disk architecture, cluster size, and so on. The main work of the MBR is to locate and run necessary operating system files that are required to run a hard disk. In the context of the operating system, MBR is also known as the boot loader. Which of the following viruses can infect the MBR of a hard disk?

Each correct answer represents a complete solution. Choose two.

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

**Answer:** AB

#### NEW QUESTION 82

- (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 84

- (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 88

- (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 91

- (Topic 1)

Which of the following tools can be used to perform tasks such as Windows password cracking Windows enumeration, and VoIP session sniffing?

- A. John the Ripper
- B. Obiwan
- C. Cain
- D. L0phtcrack

**Answer:** C

#### NEW QUESTION 95

- (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 97

- (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 99

- (Topic 2)

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information.

Which of the following disk spaces will he use to store this secret information?

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

- A. Slack space
- B. Unused Sectors
- C. Dumb space
- D. Hidden partition

**Answer:** ABD

#### NEW QUESTION 104

- (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 106



- (Topic 2)

You work as a Network Administrator for Tech World Inc. The company has a TCP/IP- based router. You have configured a router on your network. You want to accomplish the following goals:

I Configure the router to require a password to move from user EXEC mode to privileged EXEC mode.

I The password must be listed as a hidden entry in the configuration file. You run the following command: enable password <password>

Which of the goals will this action accomplish?

- A. The password will be listed as a hidden entry in the configuration file
- B. The action will accomplish neither of the goals
- C. The action will accomplish both the goals
- D. The router will require a password to move from user EXEC mode to privileged EXEC mode

**Answer: D**

#### NEW QUESTION 108

- (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 110

- (Topic 2)

Which of the following protocols implements VPN using IPSec?

- A. SLIP
- B. PPTP
- C. PPP
- D. L2TP

**Answer: D**

#### NEW QUESTION 112

- (Topic 2)

Which of the following is NOT a phase of the OODA Loop strategy?

- A. Observe
- B. Define
- C. Orient
- D. Act

**Answer: B**

#### NEW QUESTION 115

- (Topic 2)

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

- A. They extend the IP addressing scheme.
- B. The same subnet mask is used everywhere on the network.
- C. They support VLSM and discontinuous networks.
- D. IGRP is a classless routing protocol.

**Answer: AC**

#### NEW QUESTION 116

- (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 118

- (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 123

- (Topic 2)

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

- A. They are considered an indicator of threats coupled with vulnerability.
- B. They can be mitigated by reviewing and taking responsible actions based on possible risks.
- C. They can be removed completely by taking proper actions.
- D. They can be analyzed and measured by the risk analysis process.

**Answer:** ABD

#### NEW QUESTION 128

- (Topic 2)

Which of the following firewalls inspects the actual contents of packets?

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

**Answer:** B

#### NEW QUESTION 130

- (Topic 2)

In packet filtering types of firewalls, which of the following specifies what traffic can and cannot traverse the firewall?

- A. Internet bot
- B. Access control list
- C. ASDM
- D. RIP

**Answer:** B

#### NEW QUESTION 132

- (Topic 2)

You send and receive messages on Internet. A man-in-the-middle attack can be performed to capture and read your message. Which of the following Information assurance pillars ensures the security of your message or data against this type of attack?

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

**Answer:** D

#### NEW QUESTION 136

- (Topic 2)

Which of the following encryption techniques does digital signatures use?

- A. MD5
- B. RSA
- C. IDEA
- D. Blowfish

**Answer:** C

#### NEW QUESTION 137

- (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 139

- (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 143

- (Topic 2)

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

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

- A. Vulnerability
- B. Firewall
- C. Endpoint authentication
- D. IDS

**Answer:** BCD

#### NEW QUESTION 146

- (Topic 2)

Which of the following statements are true about routers?

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

- A. Routers do not limit physical broadcast traffic.
- B. Routers act as protocol translators and bind dissimilar networks.
- C. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.
- D. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

**Answer:** BCD

#### NEW QUESTION 147

- (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 152

- (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 154

- (Topic 2)

Which of the following refers to the process of verifying the identity of a person, network host, or system process?

- A. Hacking
- B. Authentication
- C. Packet filtering
- D. Auditing

**Answer:** B

#### NEW QUESTION 155

- (Topic 2)

The Incident handling process implemented in an enterprise is responsible to deal with all the incidents regarding the enterprise. Which of the following procedures will be involved by the preparation phase of the Incident handling process?

- A. Organizing a solution to remove an incident
- B. Building up an incident response kit
- C. Working with QA to validate security of the enterprise
- D. Setting up the initial position after an incident

**Answer:** B

**NEW QUESTION 157**

- (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 160**

- (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 162**

- (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 164**

- (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 167**

- (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 170**

- (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 172**

- (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 175**

- (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 177**

- (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 179**

- (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 182**

- (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 186**

- (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 189**

- (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 191

- (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 195

- (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 198

- (Topic 2)

Which of the following combines the characteristics of a bridge and a router?

- A. Firewall
- B. Brouter
- C. Switch
- D. Hub
- E. Repeater

**Answer:** B

#### NEW QUESTION 201

- (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 204

- (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 205

- (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 207

- (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 208

- (Topic 2)

Which of the following types of firewalls forms a session flow table?

- A. Proxy server firewall
- B. Packet filtering firewall
- C. Stateless packet filtering firewall
- D. Stateful packet filtering firewall

**Answer:** D

#### NEW QUESTION 213

- (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 218

- (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 220

- (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 224

- (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 227

- (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 229

- (Topic 2)

Which term best describes an e-mail that contains incorrect and misleading information or warnings about viruses?

- A. Blowfish
- B. Spam
- C. Virus
- D. Trojan horse
- E. Hoax
- F. Rlogin

**Answer:** E

#### NEW QUESTION 232

- (Topic 2)

You work as a Software Developer for uCertify Inc. You have developed a Data Access Logic (DAL) component that will be part of a distributed application. You are conducting integration testing with other components of the distributed application. Which of the following types of testing methods will you need to perform to identify potential security-related issues? Each correct answer represents a part of the solution. Choose two.

- A. Unit testing
- B. Stress testing
- C. Load testing
- D. Black box testing
- E. White box testing

**Answer:** DE

#### NEW QUESTION 233

- (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 235

- (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 238

- (Topic 2)

Which of the following statements about Public Key Infrastructure (PKI) is true?

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

**Answer:** D

#### **NEW QUESTION 241**

- (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 243**

- (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 244**

- (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 245**

- (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 248**

- (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 253**

- (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 257**

- (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 261**

- (Topic 3)

Which of the following are parts of applying professional knowledge? Each correct answer represents a complete solution. Choose all that apply.

- A. Maintaining cordial relationship with project sponsors
- B. Reporting your project management appearance
- C. Staying up-to-date with project management practices
- D. Staying up-to-date with latest industry trends and new technology

**Answer:** BCD

**NEW QUESTION 265**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The GISF Practice Test Here](#)**