

GISF Dumps

GIAC Information Security Fundamentals

<https://www.certleader.com/GISF-dumps.html>



NEW QUESTION 1

- (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 2

- (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 3

- (Topic 1)

According to the case study, what protocol should be used to protect a customer's privacy and credit card information?

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

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

Answer: E

NEW QUESTION 4

- (Topic 1)

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

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

Answer: B

NEW QUESTION 5

- (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. On the We-are-secure login page, he enters '=' as a username and successfully logs in to the user page of the Web site. The We-are-secure login page is vulnerable to a ____.

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

Answer: A

NEW QUESTION 6

- (Topic 1)

Which of the following processes is accountable for monitoring an IT Service and detecting when the performance drops beneath adequate limits?

- A. Service Asset and Configuration Management
- B. Service Request Management
- C. Event Management
- D. Service Level Management

Answer: C

NEW QUESTION 7

- (Topic 1)

You are the security manager of Microliss Inc. Your enterprise uses a wireless network infrastructure with access points ranging 150-350 feet. The employees using the network complain that their passwords and important official information have been traced. You discover the following clues:

The information has proved beneficial to another company.

The other company is located about 340 feet away from your office. The other company is also using wireless network.

The bandwidth of your network has degraded to a great extent. Which of the following methods of attack has been used?

- A. A piggybacking attack has been performed.
- B. The information is traced using Bluebugging.
- C. A DOS attack has been performed.
- D. A worm has exported the information.

Answer: A

NEW QUESTION 8

- (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 9

- (Topic 1)

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

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

Answer: ABC

NEW QUESTION 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 14

- (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 16

- (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 server.
- 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 20

- (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 24

- (Topic 1)

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

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

Answer: ABC

NEW QUESTION 27

- (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 32

- (Topic 1)

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

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

Answer: B

NEW QUESTION 34

- (Topic 1)

Mark works as a Network Administrator for Roadways Travel Inc. The company wants to implement a strategy for its external employees so that they can connect to Web-based applications. What will Mark do to achieve this?
(Click the Exhibit button on the toolbar to see the case study.)

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

Answer: C

NEW QUESTION 38

- (Topic 1)

You have an antivirus program for your network. It is dependent upon using lists of known viruses. What is this type of scan called?

- A. Heuristic
- B. Fixed List
- C. Dictionary
- D. Host Based

Answer: C

NEW QUESTION 42

- (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 46

- (Topic 1)

You work in an enterprise as a Network Engineer. Your enterprise has a secure internal network.

You want to apply an additional network packet filtering device that is intermediate to your enterprise's internal network and the outer network (internet). Which of the following network zones will you create to accomplish this task?

- A. Autonomous system area (AS)
- B. Demilitarized zone (DMZ)
- C. Border network area
- D. Site network area

Answer: C

NEW QUESTION 50

- (Topic 1)

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

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

Answer: D

NEW QUESTION 54

- (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 57

- (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 60

- (Topic 1)

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

Which of the following are its significant steps?

Each correct answer represents a complete solution. Choose two.

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

Answer: BD

NEW QUESTION 65

- (Topic 1)

In which of the following access control models can a user not grant permissions to other

users to see a copy of an object marked as secret that he has received, unless they have the appropriate permissions?

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

Answer: D

NEW QUESTION 67

- (Topic 1)

Which of the following factors determine the strength of the encryption?

- A. Character-set encoding
- B. Length of the key
- C. Operating system
- D. Ease of use

Answer: B

NEW QUESTION 70

- (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 72

- (Topic 1)

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

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

Answer: C

NEW QUESTION 75

- (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 76

- (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 78

- (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 82

- (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 86

- (Topic 1)

Which of the following protocols work at the Network layer of the OSI model?

- A. Internet Group Management Protocol (IGMP)
- B. Simple Network Management Protocol (SNMP)
- C. Routing Information Protocol (RIP)
- D. File Transfer Protocol (FTP)

Answer: AC

NEW QUESTION 88

- (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 89

- (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 91

- (Topic 1)

In which type of access control do user ID and password system come under?

- A. Physical
- B. Power
- C. Technical
- D. Administrative

Answer: C

NEW QUESTION 96

- (Topic 1)

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

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

Answer: D

NEW QUESTION 97

- (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 99

- (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 102

- (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 105

- (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 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)

Which of the following protocols implements VPN using IPSec?

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

Answer: D

NEW QUESTION 110

- (Topic 2)

You are the project manager of a new project to install new hardware for your organization's computer network. You have never worked with networking software or hardware before so you enroll in a class to learn more about the technology you'll be managing in your project. This is an example of which one of the following?

- A. Cost of nonconformance to quality
- B. Enhancing your personal professional competence
- C. Team development
- D. A waste for the project as the project manager does not need to know much about the project's application

Answer: B

NEW QUESTION 111

- (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 113

- (Topic 2)

What are packet sniffers?

- A. Packet sniffers encrypt the packages as they cross the network.
- B. Packet sniffers test package security.
- C. Packet sniffers test the packages to verify data integrity.
- D. Packet sniffers capture the packages as they cross the network.

Answer: D

NEW QUESTION 116

- (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 117

- (Topic 2)

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

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

Answer: D

NEW QUESTION 122

- (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 123

- (Topic 2)

Which of the following encryption techniques does digital signatures use?

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

Answer: C

NEW QUESTION 124

- (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 126

- (Topic 2)

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

- A. 448 bit
- B. 256 bit
- C. 64 bit
- D. 16 bit

Answer: A

NEW QUESTION 129

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 a 160-bit message digest

NEW QUESTION 132

- (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 134

- (Topic 2)

Which of the following is most useful against DOS attacks?

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

Answer: D

NEW QUESTION 138

- (Topic 2)

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

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

Answer: D

NEW QUESTION 140

- (Topic 2)

Which of the following components are usually found in an Intrusion detection system (IDS)?

Each correct answer represents a complete solution. Choose two.

- A. Console
- B. Sensor
- C. Firewall
- D. Modem
- E. Gateway

Answer: AB

NEW QUESTION 142

- (Topic 2)

Which of the following are the types of access controls?

Each correct answer represents a complete solution. Choose three.

- A. Physical
- B. Administrative
- C. Automatic
- D. Technical

Answer: ABD

NEW QUESTION 143

- (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 145

- (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 146

- (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 150

- (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 154

- (Topic 2)

You are concerned about possible hackers doing penetration testing on your network as a prelude to an attack. What would be most helpful to you in finding out if this is occurring?

- A. Examining your firewall logs
- B. Examining your DNS Server logs
- C. Examining your domain controller server logs
- D. Examining your antivirus logs

Answer: A

NEW QUESTION 158

- (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 160

- (Topic 2)

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

- A. Snort
- B. Wireshark
- C. NetWitness
- D. Netresident

Answer: B

NEW QUESTION 162

- (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 163

- (Topic 2)

Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process. Configuration Management is used for which of the following?

- * 1. To account for all IT assets
- * 2. To provide precise information support to other ITIL disciplines
- * 3. To provide a solid base only for Incident and Problem Management
- * 4. To verify configuration records and correct any exceptions

- A. 2 and 4 only
- B. 1, 3, and 4 only
- C. 1, 2, and 4 only
- D. 2, 3, and 4 only

Answer: C

NEW QUESTION 165

- (Topic 2)

This type of virus infects programs that can execute and load into memory to perform predefined steps for infecting systems. It infects files with the extensions .EXE, .COM, .BIN, and .SYS. As it can replicate or destroy these types of files, the operating system becomes corrupted and needs reinstallation. This type of virus is known as .

- A. Multipartite virus
- B. Boot sector virus
- C. File virus
- D. Stealth virus
- E. Polymorphic virus

Answer: C

NEW QUESTION 168

- (Topic 2)

You work as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. You are troubleshooting a computer of a user who is working on Windows Vista.

He 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 will you configure to save the user's data?

- A. Malware protection
- B. Automatic updating
- C. Firewall
- D. Other security settings

Answer: C

NEW QUESTION 171

- (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 175

- (Topic 2)

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

The email header of the suspicious email is given below:

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

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

Answer: D

NEW QUESTION 179

- (Topic 2)

Which of the following layers of the OSI model corresponds to the Host-to-Host layer of the TCP/IP model?

- A. The presentation layer
- B. The application layer
- C. The transport layer
- D. The session layer

Answer: C

NEW QUESTION 180

- (Topic 2)

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

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

Answer: C

NEW QUESTION 184

- (Topic 2)

You work as a Network Administrator for NetTech Inc. The company wants to encrypt its e- mails.

Which of the following will you use to accomplish this?

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

Answer: C

NEW QUESTION 187

- (Topic 2)

Your corporate network uses a Proxy Server for Internet access. The Manufacturing group has access permission for WWW protocol in the Web Proxy service, and access permission for POP3 protocol, in the WinSock Proxy service. The Supervisors group has access permission for WWW and FTP Read protocols in the Web Proxy service, and access permission for the SMTP protocol in the WinSock Proxy service. The Quality Control group has access permission only for WWW protocol in the Web Proxy service. The Interns group has no permissions granted in any of the Proxy Server services. Kate is a member of all four groups. In the Proxy Server services, which protocols does Kate have permission to use?

- A. WWW only
- B. FTP Read and SMTP only
- C. WWW, FTP Read, POP3, and SMTP
- D. WWW and POP3 only

Answer: C

NEW QUESTION 188

- (Topic 2)

Cryptography is the science of?

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

Answer: A

NEW QUESTION 189

- (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 193

- (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 195

- (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 198

- (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 201

- (Topic 2)

You work as the Network Administrator of TechJobs. You implement a security policy, to be in effect at all times, on the client computer in your network. While troubleshooting, assistant administrators often change security settings on the network. You want the security policy to be reapplied after changes have been made. How can you automate this task? (Click the Exhibit button on the toolbar to see the case study.)

- A. Create a group policy object (GPO) and implement it to the domain.
- B. Configure a security policy on the domain controller.
- C. Give Administrators read-only permission on that GPO.
- D. Create a separate OU for the Administrators to test the security settings.
- E. Ask the assistant administrators to re-apply the security policy after the changes have been made.
- F. Schedule the SECEDIT command to run on the client computers.

Answer: D

NEW QUESTION 205

- (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 208

- (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 209

- (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 212

- (Topic 2)

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

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

Answer: B

NEW QUESTION 217

- (Topic 2)

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

- A. Start, Work, and Remaining Work
- B. Actual Start and Percent Complete
- C. Actual Start, Actual Work, and Remaining Work
- D. Actual Start, Percent Complete, and Remaining Duration

Answer: C

NEW QUESTION 218

- (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 219

- (Topic 3)

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

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

Answer: A

NEW QUESTION 224

- (Topic 3)

You are responsible for virus protection for a large college campus. You are very concerned that your antivirus solution must be able to capture the latest virus threats. What sort of virus protection should you implement?

- A. Network Based
- B. Dictionary
- C. Heuristic
- D. Host based

Answer: C

NEW QUESTION 226

- (Topic 3)

Which of the following statements about a brute force attack is true?

- A. It is a program that allows access to a computer without using security checks.
- B. It is an attack in which someone accesses your e-mail server and sends misleading information to others.
- C. It is a virus that attacks the hard drive of a computer.
- D. It is a type of spoofing attack.
- E. It is an attempt by an attacker to guess passwords until he succeeds.

Answer: E

NEW QUESTION 231

- (Topic 3)

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

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

Answer: CD

NEW QUESTION 233

- (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 237

- (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 238

- (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 241

- (Topic 3)

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

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

Answer: C

NEW QUESTION 245

- (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 247

- (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 249

- (Topic 3)

You work in a company that accesses the Internet frequently. This makes the company's files susceptible to attacks from unauthorized access. You want to protect your company's network from external attacks. Which of the following options will help you in achieving your aim?

- A. FTP
- B. Gopher
- C. Firewall
- D. HTTP

Answer: C

NEW QUESTION 254

- (Topic 3)

The Intrusion Detection System (IDS) instructs the firewall to reject any request from a particular IP address if the network is repeatedly attacked from this address. What is this action known as?

- A. Sending deceptive e-mails
- B. Sending notifications
- C. Shunning
- D. Logging
- E. Spoofing
- F. Network Configuration Changes

Answer: F

NEW QUESTION 257

- (Topic 3)

Which of the following statements are true about Public-key cryptography? Each correct answer represents a complete solution. Choose two.

- A. Data encrypted with the secret key can only be decrypted by another secret key.
- B. The secret key can encrypt a message, and anyone with the public key can decrypt it.
- C. Data encrypted by the public key can only be decrypted by the secret key.
- D. The distinguishing technique used in public key-private key cryptography is the use of symmetric key algorithms.

Answer: BC

NEW QUESTION 262

- (Topic 3)

Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

- A. Packet filtering
- B. Firewall
- C. Intrusion detection system (IDS)
- D. Demilitarized zone (DMZ)

Answer: C

NEW QUESTION 265

- (Topic 3)

You work as a Software Developer for uCertify Inc. The company has several branches worldwide. The company uses Visual Studio.NET 2005 as its application development platform. You have recently finished the development of an application using .NET Framework 2.0. The application can be used only for cryptography. Therefore, you have implemented the application on a computer. What will you call the computer that implemented cryptography?

- A. Cryptographer
- B. Cryptographic toolkit
- C. Cryptosystem
- D. Cryptanalyst

Answer: C

NEW QUESTION 266

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GISF Exam with Our Prep Materials Via below:

<https://www.certleader.com/GISF-dumps.html>