Exam Questions GISF

GIAC Information Security Fundamentals

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

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

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

Answer: C

NEW QUESTION 3
- (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 4
- (Topic 1)
Security is responsible for well-being of information and infrastructures in which the
possibilities of successful yet undetected theft, tampering, and/or disruption of information and services are kept low or tolerable. Which of the following are the elements of security?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABCD

NEW QUESTION 5
- (Topic 1)
Which of the following statements about testing are true?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 6
- (Topic 1)
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 7
- (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 8
- (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 9
- (Topic 1)
How long are cookies in effect if no expiration date is set?

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

Answer: B

NEW QUESTION 10
- (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. Cryptography
B. OODA loop
C. Risk analysis
D. Firewall security

Answer: A

NEW QUESTION 10
- (Topic 1)
Which of the following protocols can help you get notified in case a router on a network fails?

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

Answer: B

NEW QUESTION 13
- (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 18

- (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 21
- (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 25
- (Topic 1)
Which of the following service provider classes is used to create a digital signature?

A. RC2CryptoServiceProvider
B. RNGCryptoServiceProvider
C. DESCryptoServiceProvider
D. SHA1CryptoServiceProvider
E. MD5CryptoServiceProvider
F. DSACryptoServiceProvider

Answer: F

NEW QUESTION 28
- (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 33
- (Topic 1)
Which of the following network connectivity devices translates one protocol into another and is used to connect dissimilar network technologies?

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

Answer: D

NEW QUESTION 37
- (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 42
- (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 43
- (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 45
- (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 46
- (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 48
- (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 53
- (Topic 1)
You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domainbased network. The network has three Windows Server 2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that Windows firewall allows or blocks?

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

Answer: D

NEW QUESTION 58
- (Topic 1)

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

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

Answer: A

NEW QUESTION 63
- (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 64
- (Topic 1)
Which of the following terms is used for a router that filters traffic before it is passed to the firewall?

A. Screened host
B. Demilitarized zone (DMZ)
C. Honey pot
D. Bastion host

Answer: A

NEW QUESTION 68
- (Topic 1)
Which of the following is a remote access protocol that supports encryption?

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

Answer: A

NEW QUESTION 69
- (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 73
- (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 75
- (Topic 1)
Which of the following statements is not true about a digital certificate?

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

Answer: D

NEW QUESTION 80
- (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 83
- (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 88
- (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 89
- (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 90
- (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 92
- (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 93
- (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 97
- (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 101
- (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 104
- (Topic 1)
You are the project manager of a new project in your organization. You and the project team have identified the project risks, completed risk analysis, and are planning the most appropriate risk responses. Which of the following tools is most effective to choose the most appropriate risk response?

A. Project network diagrams
B. Delphi Technique
C. Decision tree analysis
D. Cause-and-effect diagrams

Answer: C

NEW QUESTION 107
- (Topic 1)
Based on the information given in the case study, which two authentication methods should you use to allow customers to access their photos on the Web site? (Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a part of the solution. Choose two.

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

Answer: BE

NEW QUESTION 112
- (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 115
- (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 118
- (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 122
- (Topic 1)
Which of the following algorithms produce 160-bit hash values? Each correct answer represents a complete solution. Choose two.

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

Answer: CD

NEW QUESTION 126
- (Topic 1)
In a complex network, Router transfers data packets by observing some form of parameters or metrics provided in the routing table. Which of the following metrics is NOT included in the routing table?

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

Answer: D

NEW QUESTION 131
- (Topic 1)
Which of the following is an organization that defines standards for anti-virus software?

A. ICSA
B. IETF
C. IIS
D. IEEE

Answer: A

NEW QUESTION 132
- (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 137
- (Topic 1)
The security of a computer against the unauthorized usage largely depends upon the efficiency of the applied access control method. Which of the following statements are true about a computer access control method?
Each correct answer represents a complete solution. Choose all that apply.

A. It can be based upon fingerprint or eye recognition.
B. It can be time-synchronous.

C. It provides security against the virus attacks.
D. It provides security against Eavesdropping.
E. It checks the authenticity of a person.
F. It is used to encrypt a message before transmitting it on a network.

Answer: ABE

NEW QUESTION 139
- (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 142
- (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 146
- (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 147
- (Topic 2)
You have been tasked with finding an encryption methodology for your company's network. The solution must use public key encryption which is keyed to the users email address. Which of the following should you select?

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

Answer: C

NEW QUESTION 150
- (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 155
- (Topic 2)
Which of the following U.S.C. laws is governs the fraudulent activities associated with computers?

A. 18 U.S.
B. 2251
C. 18 U.S.
D. 3771
E. 18 U.S.
F. 2257
G. 18 U.S.
H. 1030

Answer: D

NEW QUESTION 158
- (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 163
- (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:
l Configure the router to require a password to move from user EXEC mode to privileged EXEC mode.
l 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 166
- (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 169
- (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 174
- (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 175
- (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 178
- (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 180
- (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 182
- (Topic 2)
The method used to encrypt messages by transposing or scrambling the characters in a certain manner is known as _____.

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

Answer: B

NEW QUESTION 185
- (Topic 2)
Which of the following is a technique of attacks in which the attacker secretly listens to the private conversation between victims?

A. Eavesdropping
B. Intrusion
C. Dialler attack
D. Denial of service

Answer: A

NEW QUESTION 186
- (Topic 2)
Which of the following can be used to prevent routing loops in distance vector routing protocols?
Each correct answer represents a complete solution. Choose two.

A. Split horizon
B. Link-state advertisement
C. Spanning Tree Protocol
D. Hold-down timers

Answer: AD

NEW QUESTION 189
- (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 194
- (Topic 2)
Which of the following types of firewalls looks deep into packets and makes granular access control decisions?

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

Answer: B

NEW QUESTION 198
- (Topic 2)
Which of the following security applications is used to secure a database from unauthorized accesses in a network infrastructure?

A. Antivirus
B. Anti-Malware
C. Anti-Spoofing
D. Firewall

Answer: D

NEW QUESTION 200
- (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 202
- (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 204
- (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 205
- (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 208
- (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 209

- (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 211
- (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 216
- (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 218
- (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 222
- (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 225
- (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 228
- (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 230
- (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 234
- (Topic 2)
John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He analyzes that the company has blocked all ports except port 80.
Which of the following attacking methods can he use to send the dangerous software protocols?

A. HTTP tunneling
B. URL obfuscation
C. Banner grabbing
D. MAC spoofing

Answer: A

NEW QUESTION 235
- (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 238
- (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 240
- (Topic 2)
Which of the following methods of encryption uses a single key to encrypt and decrypt data?

A. S/MIME
B. Asymmetric

C. PGP
D. Symmetric

Answer: D

NEW QUESTION 243
- (Topic 2)
Which two security components should you implement on the sales personnel portable computers to increase security?
(Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a complete solution. Choose two.

A. Remote access policy
B. L2TP over IPSec
C. PPTP
D. Remote Authentication Dial-In User Service (RADIUS)
E. Encrypting File System (EFS)

Answer: BE

NEW QUESTION 248
- (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 249
- (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 250
- (Topic 2)
Which of the following viruses is designed to prevent antivirus researchers from examining its code by using various methods that make tracing and disassembling difficult?

A. Multipartite virus
B. Polymorphic virus
C. Armored virus
D. Stealth virus

Answer: C

NEW QUESTION 255
- (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 257
- (Topic 2)
Joseph works as a Software Developer for WebTech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Trademark laws
B. Patent laws
C. Copyright laws

D. Code Security law

Answer: B

NEW QUESTION 260
- (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 261
- (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 262
- (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 264
- (Topic 2)
John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He is working on the Linux operating system and wants to install an Intrusion Detection System on the We-are-secure server so that he can receive alerts about any hacking attempts. Which of the following tools can John use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. Samhain
B. SARA
C. Snort
D. Tripwire

Answer: AC

NEW QUESTION 265
- (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 270
- (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 275
- (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 278
- (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 280
- (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 285
- (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 286
- (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 290
- (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 294
- (Topic 2)
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

A. TCP FTP proxy scanning
B. Eavesdropping
C. Fingerprinting
D. Web ripping

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 300
- (Topic 2)
Which of the following types of firewall functions by creating two different communications, one between the client and the firewall, and the other between the firewall and the end server?

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

Answer: B

NEW QUESTION 301
- (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 302
- (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 305
- (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 306
- (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 308
- (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 313
- (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 318
- (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 319
- (Topic 3)
Which of the following is used in asymmetric encryption?

A. Public key and user key
B. Public key and private key
C. SSL
D. NTFS

Answer: B

NEW QUESTION 323
- (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)
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 330
- (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 331
- (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 333
- (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 336
- (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 337
- (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 340
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

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

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

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

Money Back Guarantee

GISF Practice Exam Features:

* GISF Questions and Answers Updated Frequently

* GISF Practice Questions Verified by Expert Senior Certified Staff

* GISF Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GISF Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year