GIAC

Exam Questions GISF

GIAC Information Security Fundamentals

NEW QUESTION 1
- (Topic 1)
Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

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

Answer: AB

NEW QUESTION 2
- (Topic 1)
You are the project manager of the HHH Project. The stakeholders for this project are scattered across the world and you need a method to promote interaction. You determine that a Web conferencing software would be the most cost effective solution. The stakeholders can watch a slide show while you walk them through the project details. The stakeholders can hear you, ask questions via a chat software, and post concerns. What is the danger in this presentation?

A. 55 percent of all communication is nonverbal and this approach does not provide non- verbal communications.
B. The technology is not proven as reliable.
C. The stakeholders won't really see you.
D. The stakeholders are not required to attend the entire session.

Answer: A

NEW QUESTION 3
- (Topic 1)
Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access. Which of the following addresses is a valid MAC address?

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

Answer: B

NEW QUESTION 4
- (Topic 1)
You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

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

Answer: A

NEW QUESTION 5
- (Topic 1)
Which U.S. government agency is responsible for establishing standards concerning cryptography for nonmilitary use?

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

Answer: C

NEW QUESTION 6
- (Topic 1)
Which of the following is a valid IP address for class B Networks?

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

Answer: A

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

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

Answer: D

NEW QUESTION 9
- (Topic 1)
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 10
- (Topic 1)
You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

A. Containment
B. Identification
C. Preparation
D. Eradication

Answer: C

NEW QUESTION 10
- (Topic 1)
You work as an Incident handling manager for Orangesect Inc. You detect a virus attack incident in the network of your company. You develop a signature based on the characteristics of the detected virus.
Which of the following phases in the Incident handling process will utilize the signature to resolve this incident?

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

Answer: D

NEW QUESTION 12
- (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 15
- (Topic 1)
Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

A. The Configuration Manager

B. The Supplier Manager
C. The IT Service Continuity Manager
D. The Service Catalogue Manager

Answer: B

NEW QUESTION 17
- (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 21
- (Topic 1)
You are working on your computer system with Linux Operating system. After working for a few hours, the hard disk goes to the inactive state (sleep). You try to restart the system and check the power circuits. You later discover that the hard disk has crashed. Which of the following precaution methods should you apply to keep your computer safe from such issues?

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

Answer: D

NEW QUESTION 26
- (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 30
- (Topic 1)
John works as a Network Administrator for Bordeaux Inc. He is planning to design a strategy, so that the employees can connect to a scheduling application. Which of the following strategies is best suited for the company?
(Click the Exhibit button on the toolbar to see the case study.)

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

Answer: D

NEW QUESTION 33
- (Topic 1)
You work as a Security manager for Qualoxizz Inc. Your company has number of network switches in the site network infrastructure. Which of the following actions will you perform to ensure the security of the switches in your company?

A. Set long session timeouts.
B. Open up all the unused management ports.
C. Set similar passwords for each management port.
D. Ignore usage of the default account settings.

Answer: D

NEW QUESTION 37
- (Topic 1)
The ATM of a bank is robbed by breaking the ATM machine. Which of the following physical security devices can now be used for verification and historical analysis of the ATM robbery?

A. Biometric devices
B. Intrusion detection systems
C. Key card

D. CCTV Cameras

Answer: D

NEW QUESTION 41
- (Topic 1)
You work as a Network Administrator for ABC Inc. The company has a secure wireless network.
However, in the last few days, an attack has been taking place over and over again. This attack is taking advantage of ICMP directed broadcast. To stop this attack, you need to disable ICMP directed broadcasts. Which of the following attacks is taking place?

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

Answer: A

NEW QUESTION 44
- (Topic 1)
Which of the following types of authentications supported by OSPF? Each correct answer represents a complete solution. Choose three.

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

Answer: ABC

NEW QUESTION 49
- (Topic 1)
Which of the following are the examples of administrative controls?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BC

NEW QUESTION 53
- (Topic 1)
The Project Risk Management knowledge area focuses on which of the following processes?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

NEW QUESTION 57
- (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 61
- (Topic 1)
Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

NEW QUESTION 62
- (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 64
- (Topic 1)
What does Wireless Transport Layer Security (WTLS) provide for wireless devices? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 69
- (Topic 1)
Mark work as a Network Administrator for Roadways Travel Inc. The conmpany 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 71
- (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)
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 78
- (Topic 1)
Which of the following protocols are used by Network Attached Storage (NAS)?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 80
- (Topic 1)
Which of the following provides a credential that can be used by all Kerberos-enabled servers and applications?

A. Remote Authentication Dial In User Service (RADIUS)

B. Internet service provider (ISP)
C. Network Access Point (NAP)
D. Key Distribution Center (KDC)

Answer: D

NEW QUESTION 83
- (Topic 1)
You work as a security manager for hackoxiss Inc. The company consists of a perimeter
network as its internal network. A number of ethical hackers are employed in the company. You are getting complaints that some employees of the company are trying to intrude other systems on the outer network (Internet). In which of the following ways will you secure the internal as well as the outer network?

A. Deny the access of outer users to internal network.
B. Use distributed firewalls.
C. Deny the access of internal users to outer network.
D. Configure ACL on your company's router.

Answer: B

NEW QUESTION 86
- (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 88
- (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 89
- (Topic 1)
You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

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

Answer: D

NEW QUESTION 92
- (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 97
- (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 99
- (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 102
- (Topic 1)
Under the SMART scheme, the Predictive Failure Analysis Technology is used to determine the failure or crash for which of the following parts of a computer system?

A. Operating System
B. Hard Disc drive
C. Software
D. Internet Browser

Answer: B

NEW QUESTION 107
- (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 108
- (Topic 1)
Which of the following provide data confidentiality services by encrypting the data sent between wireless systems?
Each correct answer represents a complete solution. Choose two.

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

Answer: BC

NEW QUESTION 109
- (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 114
- (Topic 1)
Kelly is the project manager of the NNQ Project for her company. This project will last for one year and has a budget of $350,000. Kelly is working with her project team and subject matter experts to begin the risk response planning process. When the project manager begins the plan risk response process, what two inputs will she need?

A. Risk register and the results of risk analysis
B. Risk register and the risk response plan
C. Risk register and the risk management plan
D. Risk register and power to assign risk responses

Answer: C

NEW QUESTION 116
- (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 121
- (Topic 1)
Which of the following are some of the parts of a project plan?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABC

NEW QUESTION 126
- (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 130
- (Topic 1)
Which of the following options cannot be accessed from Windows Update?

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

Answer: D

NEW QUESTION 134
- (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 138
- (Topic 1)
Which of the following is the most secure place to host a server that will be accessed publicly through the Internet?

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

Answer: C

NEW QUESTION 140
- (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 144
- (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 149
- (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 150
- (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 152
- (Topic 1)
Which of the following statements are true about Dsniff?
Each correct answer represents a complete solution. Choose two.

A. It is a virus.
B. It contains Trojans.
C. It is antivirus.
D. It is a collection of various hacking tools.

Answer: BD

NEW QUESTION 156
- (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 160
- (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 164

- (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 165
- (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 169
- (Topic 2)
Which of the following evidences is NOT the potential evidence for Routers?

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

Answer: B

NEW QUESTION 172
- (Topic 2)
Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

NEW QUESTION 173
- (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 178
- (Topic 2)
Which of the following is NOT a phase of the OODA Loop strategy?

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

Answer: B

NEW QUESTION 183
- (Topic 2)
Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

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

Answer: ABD

NEW QUESTION 187
- (Topic 2)
You are the Administrator for a corporate network. You are concerned about denial of service attacks. Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

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

Answer: A

NEW QUESTION 188
- (Topic 2)
Mark works as a Network Administrator for NetTech Inc. The network uses routers from multiple vendors. Mark wants to implement a routing protocol on the company's network that provides VLSM support, scalability and minimal overhead on the network. Which of the following protocols will Mark use to fulfill the requirements?

A. RIPv1
B. EIGRP
C. CDP
D. OSPF

Answer: D

NEW QUESTION 189
- (Topic 2)
Which of the following encryption techniques does digital signatures use?

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

Answer: C

NEW QUESTION 190
- (Topic 2)
Which of the following protocols provides connectionless integrity and data origin authentication of IP packets?

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

Answer: D

NEW QUESTION 191
- (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 195
- (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 198
CORRECT TEXT - (Topic 2)
Fill in the blank with the appropriate value. SHA-1 produces a _____ -bit message digest.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
SHA-1 produces a160-bit message digest

NEW QUESTION 202
- (Topic 2)
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

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

Answer: B

NEW QUESTION 207
- (Topic 2)
Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 209
- (Topic 2)
Which of the following techniques can be used by an administrator while working with the symmetric encryption cryptography? Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 211
- (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 216
- (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 221
- (Topic 2)
You discover that someone has been logging onto your network after office hours. After investigating this you find the login belongs to someone who left the company 12 months ago. What would have been the best method to prevent this?

A. A policy with time of day restrictions.
B. An IDS system.

C. A policy with account expiration.
D. A DMZ firewall.

Answer: C

NEW QUESTION 225
- (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 226
- (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 228
- (Topic 2)
The Incident handling process implemented in an enterprise is responsible to deal with all the incidents regarding the enterprise. Which of the following procedures will be involved by the preparation phase of the Incident handling process?

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

Answer: B

NEW QUESTION 233
- (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 236
- (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 240
- (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 242
- (Topic 2)
You are concerned about an attacker being able to get into your network. You want to make sure that you are informed of any network activity that is outside normal parameters. What is the best way to do this?

A. Utilize protocol analyzers.
B. User performance monitors.
C. Implement signature based antivirus.
D. Implement an anomaly based IDS.

Answer: D

NEW QUESTION 244
- (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 249
- (Topic 2)
A company would like your consulting firm to review its current network and suggest changes that will increase its efficiency and optimize the business processes. To design such a network, you prepare a case study.
Which of the following policies should be implemented through a group policy that is associated with the netperfect.com domain?
(Click the Exhibit button on the toolbar to see the case study.)
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: ABD

NEW QUESTION 254
- (Topic 2)
The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for uCertify Software Systems Pvt. Ltd.?
(Click the Exhibit button on the toolbar to see the case study.)

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

Answer: DEGH

NEW QUESTION 257
- (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 260
- (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 265
- (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 268
- (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 269
- (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 274
- (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 278
- (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 279
- (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 283
- (Topic 2)
Which of the following best describes the identification, analysis, and ranking of risks?

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

Answer: D

NEW QUESTION 284
- (Topic 2)
Which of the following authentication methods uses MD5 hash encoding while transferring credentials over a network?

A. .NET Passport authentication
B. Advanced Digest authentication
C. Integrated Windows authentication
D. Digest authentication

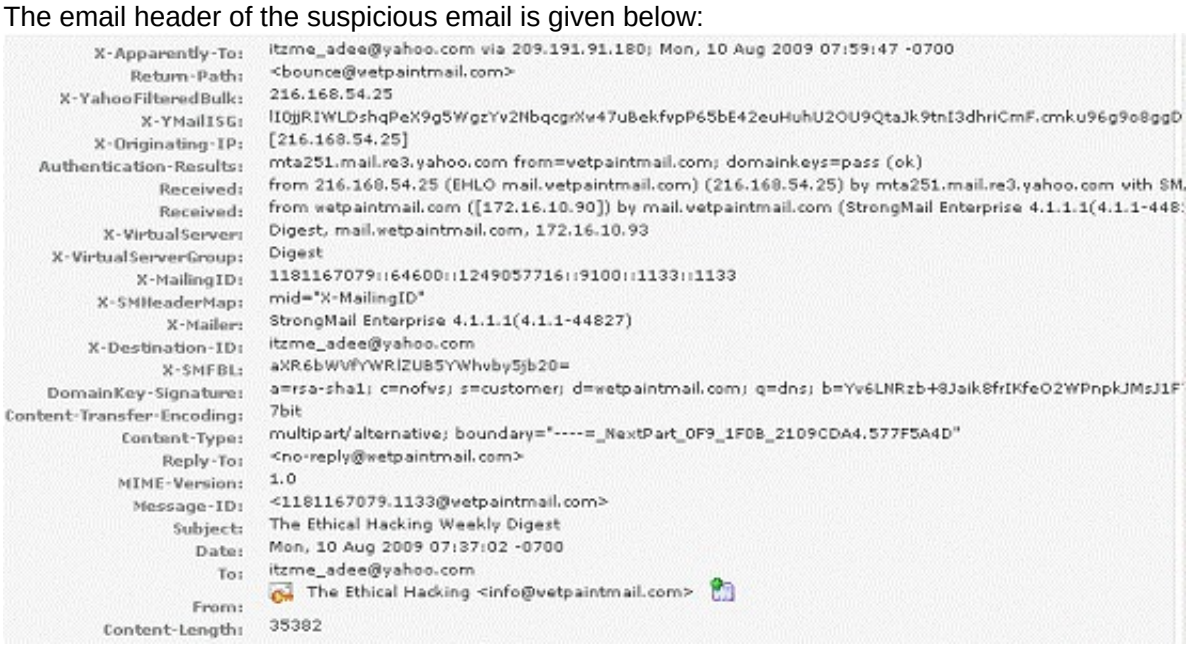
Answer: B

NEW QUESTION 288
- (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 289
- (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 290
- (Topic 2)
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

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

Answer: B

NEW QUESTION 292
- (Topic 2)
Mark works as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains four Windows 2008 member servers and 250 Windows Vista client computers. One of the member servers works as a Web server that hosts an intranet Web site. According to the company security policy, Mark needs to fulfill the following requirements:
* 1. Encryption should be used for authentication of all traffic to the Web site.
* 2. SSL should not be used on the Web server for performance reasons.
* 3. Users should be authenticated using their Active Directory credentials.
In order to fulfill the requirements, Mark has disabled the Anonymous Authentication setting on the server. What else does he have to do?

A. Enable the Anonymous Authentication setting on the server.
B. Enable the Encrypting File System (EFS) on the server.
C. Enable the Digest Authentication setting on the server.
D. Enable the Windows Authentication setting on the server.

Answer: CD

NEW QUESTION 294
- (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 298
- (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 300
- (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 302
- (Topic 2)
Donna is the project manager for her organization. She is preparing a plan to manage changes to the project should changes be requested. Her change management plan defines the process for documenting, tracking, and determining if the changes should be approved or declined. What system is considered the parent of the change control system documented in Donna's plan?

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

Answer: A

NEW QUESTION 305
- (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 309
- (Topic 2)
You and your project team want to perform some qualitative analysis on the risks you have identified and documented in Project Web Access for your project. You would like to create a table that captures the likelihood and affect of the risk on the project. What type of a chart or table would you like to create for the project risks?

A. Risk Breakdown Structure
B. Risk Probability and Impact Matrix
C. Risk Review Table
D. Risk Impact and Affect Matrix

Answer: B

NEW QUESTION 314
- (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 316
- (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 318
- (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 321
- (Topic 2)
Which of the following is an examination of the controls within an Information technology (IT) infrastructure?

A. Risk analysis
B. ITIL
C. ADP audit
D. SMART

Answer: C

NEW QUESTION 322
- (Topic 2)
You want to install a server that can be accessed by external users. You also want to ensure that these users cannot access the rest of the network. Where will you place the server?

A. Intranet
B. Local Area Network

C. Internet
D. Demilitarized Zone
E. Extranet
F. Wide Area Network

Answer: D

NEW QUESTION 324
- (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 326
- (Topic 2)
Which of the following is used to determine whether or not a principal is allowed to perform a requested action?

A. Authentication
B. Security policy
C. Authorization
D. Principal

Answer: C

NEW QUESTION 331
- (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 334
- (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 336
- (Topic 3)
Fred is the project manager for the TCC Company. His company has an internal policy that states each year they will provide free services to a nonprofit organization. Therefore, the company and its employees are not allowed to charge or receive money or gifts from the nonprofit organization they choose to provide free services. This year, the TCC Company offers to provide project management services to the children's hospital for a marketing campaign to raise money. Due to the TCC Company's project management services, the nonprofit agency exceeded previous years fund raising efforts. To show appreciation the nonprofit organization offered to reimburse the project manager for his travel expenses. Which of the following best describes how the project manager should handle the situation?

A. Say thank you and let them pay for the travel, it is the least they can do.
B. Tell the hospital no thank you and explain it is against company policy to accept payment for services provided to their pro bono customers.
C. Say nothing as to not hurt the feelings of the children's hospital.
D. Ask if the hospital could pay for some of the supplies too.

Answer: B

NEW QUESTION 340
- (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 341
- (Topic 3)
You work as the Security Administrator for Prodotxiss Inc. You want to ensure the security of your Wi-Fi enterprise network against the wireless snooping attacks. Which of the following measures will you take over the site network devices of the network?

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

Answer: C

NEW QUESTION 346
- (Topic 3)
You work as the project manager for Bluewell Inc. Your project has several risks that will affect several stakeholder requirements. Which project management plan will define who will be available to share information on the project risks?

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

Answer: B

NEW QUESTION 349
- (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 350
- (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 351
- (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 352
- (Topic 3)
John is a merchant. He has set up a LAN in his office. Some important files are deleted as a result of virus attack. John wants to ensure that it does not happen again. What will he use to protect his data from virus?

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

Answer: A

NEW QUESTION 353

- (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 355
- (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 359
.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questons and Answers in PDF Format

GISF Practice Exam Features:

* GISF Questions and Answers Updated Frequently

* GISF Practice Questions Verified by Expert Senior Certified Staff

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

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