GIAC

Exam Questions GISF

GIAC Information Security Fundamentals

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

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

Answer: B

NEW QUESTION 2
- (Topic 1)
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)
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)
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 5
- (Topic 1)
Which of the following are the goals of the cryptographic systems? Each correct answer represents a complete solution. Choose three.

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

Answer: BCD

NEW QUESTION 6
- (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 7
- (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 8
- (Topic 1)
Victor wants to use Wireless Zero Configuration (WZC) to establish a wireless network connection using his computer running on Windows XP operating system. Which of the following are the most likely threats to his computer?
Each correct answer represents a complete solution. Choose two.

A. Attacker can use the Ping Flood DoS attack if WZC is used.
B. Attacker by creating a fake wireless network with high power antenna cause Victor's computer to associate with his network to gain access.
C. Information of probing for networks can be viewed using a wireless analyzer and may be used to gain access.
D. It will not allow the configuration of encryption and MAC filterin
E. Sending information is not secure on wireless network.

Answer: BC

NEW QUESTION 9
- (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 10
- (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 10
- (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 15
- (Topic 1)
Which of the following statements about asymmetric encryption are true? Each correct answer represents a complete solution. Choose two.

A. Asymmetric encryption is faster as compared to symmetric encryption.
B. Asymmetric encryption uses a public key and a private key pair for data encryption.
C. In asymmetric encryption, only one key is needed to encrypt and decrypt data.
D. In asymmetric encryption, the public key is distributed and the private key is available only to the recipient of the message.

Answer: BD

NEW QUESTION 18

- (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 19
- (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 20
- (Topic 1)
Which of the following types of virus is capable of changing its signature to avoid detection?

A. Stealth virus
B. Boot sector virus
C. Macro virus
D. Polymorphic virus

Answer: D

NEW QUESTION 24
- (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 28
CORRECT TEXT - (Topic 1)
Fill in the blank with the appropriate layer name.
The Network layer of the OSI model corresponds to the ______ layer of the TCP/IP model.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Internet

NEW QUESTION 31
- (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 34
- (Topic 1)
Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?

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

Answer: B

NEW QUESTION 38
- (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 43
- (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 45
- (Topic 1)
You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Install a DMZ firewall
B. Enable verbose logging on the firewall
C. Install a host-based IDS
D. Install a network-based IDS

Answer: D

NEW QUESTION 49
- (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 53
- (Topic 1)
Which of the following objects in an Active Directory serve as security principles? Each correct answer represents a part of the solution. Choose all that apply.

A. User accounts
B. Organizational units (OUs)
C. Computer accounts
D. Groups

Answer: ACD

NEW QUESTION 54
- (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 58
- (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 61
- (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 66
- (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 67
- (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 72
- (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 74
- (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 76
- (Topic 1)
Which of the following are core TCP/IP protocols that can be implemented with Windows NT to connect computers and internetworks?
Each correct answer represents a complete solution. Choose all that apply.

A. Address Resolution Protocol (ARP)
B. Network Link Protocol (NWLink)
C. User Datagram Protocol (UDP)
D. Internet Control Message Protocol (ICMP)

Answer: ACD

NEW QUESTION 80
- (Topic 1)
Which of the following techniques are used after a security breach and are intended to limit the extent of any damage caused by the incident?

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

Answer: A

NEW QUESTION 82
- (Topic 1)
Tom works as the project manager for BlueWell Inc. He is working with his project to ensure timely and appropriate generation, retrieval, distribution, collection, storage, and ultimate disposition of project information. What is the process in which Tom is working?

A. Stakeholder expectation management
B. Stakeholder analysis
C. Work performance measurement
D. Project communication management

Answer: D

NEW QUESTION 83
- (Topic 1)
You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

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

Answer: A

NEW QUESTION 88
- (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 92
- (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 93
- (Topic 1)
You are the Security Consultant and have been contacted by a client regarding their encryption and hashing algorithms. Their in-house network administrator tells you that their current hashing algorithm is an older one with known weaknesses and is not collision resistant. Which algorithm are they most likely using for hashing?

A. PKI
B. MD5
C. SHA
D. Kerberos

Answer: B

NEW QUESTION 94
- (Topic 1)
Which of the following techniques allows an attacker to take network traffic coming towards a host at one port and redirect it from that host to another host?

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

Answer: D

NEW QUESTION 95
- (Topic 1)
Which of the following protocols is used to provide remote monitoring and administration to network management machines on the network? The management machines will use this protocol to collect information for network monitoring. At times, the protocol can also be used for remote configuration.

A. NNTP
B. Telnet
C. SSH
D. SNMP

Answer: D

NEW QUESTION 99
- (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 104
- (Topic 1)
You work as a Network Administrator for Net World Inc. The company has a TCP/IP-based network.
You have configured an Internet access router on the network. A user complains that he is unable to access a resource on the Web. You know that a bad NAT table entry is causing the issue. You decide to clear all the entries on the table. Which of the following commands will you use?

A. show ip dhcp binding
B. ipconfig /flushdns
C. ipconfig /all
D. clear ip nat translation *

Answer: D

NEW QUESTION 106
- (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 110
- (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 114
- (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 117
- (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 122
- (Topic 1)
Which of the following are the differences between routed protocols and routing protocols?
Each correct answer represents a complete solution. Choose two.

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

Answer: BC

NEW QUESTION 125
- (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 129
- (Topic 1)
A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

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

Answer: D

NEW QUESTION 134
- (Topic 1)
Which of the following is prepared by the business and serves as a starting point for producing the IT Service Continuity Strategy?

A. Disaster Invocation Guideline
B. Business Continuity Strategy
C. Index of Disaster-Relevant Information
D. Availability/ ITSCM/ Security Testing Schedule

Answer: B

NEW QUESTION 138
- (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 139
- (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 144
- (Topic 2)
Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

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

Answer: C

NEW QUESTION 147
- (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 149
- (Topic 2)
You are the project manager of a new project to install new hardware for your organization's computer network. You have never worked with networking software or hardware before so you enroll in a class to learn more about the technology you'll be managing in your project. This is an example of which one of the following?

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

Answer: B

NEW QUESTION 152
- (Topic 2)
Which of the following types of cipher encrypts alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword?

A. Block cipher
B. Transposition cipher
C. Vigen re cipher
D. Stream cipher

Answer: C

NEW QUESTION 157
- (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 159
- (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 163
- (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 166
- (Topic 2)
You work as a Network Administrator for Infosec Inc. You find that not only have security applications running on the server, including software firewalls, anti-virus programs, and anti-spyware programs been disabled, but anti-virus and anti-spyware definitions have also been deleted. You suspect that this situation has arisen due to malware infection. Which of the following types of malware is the most likely cause of the issue?

A. Whack-A-Mole
B. FireKiller 2000
C. Beast
D. SubSeven

Answer: B

NEW QUESTION 167
- (Topic 2)
The TCP/IP protocol suite uses _____ to identify which service a certain packet is destined for.

A. Subnet masks
B. IP addresses
C. MAC addresses
D. Port numbers

Answer: D

NEW QUESTION 170
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 173
- (Topic 2)
Which of the following are used as primary technologies to create a layered defense for giving protection to a network?
Each correct answer represents a complete solution. Choose all that apply.

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

Answer: BCD

NEW QUESTION 174
- (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 176
- (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 179
- (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 182
- (Topic 2)
Mark is implementing security on his e-commerce site. He wants to ensure that a customer sending a message is really the one he claims to be. Which of the following techniques will he use to ensure this?

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

Answer: D

NEW QUESTION 185
- (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 189
- (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 191
- (Topic 2)
You have created a Web site, which will be used for e-commerce. You want to ensure that the transactions are highly secured. For this purpose, you have to create a system to verify the identity of a potential customer. Which of the following security techniques will you use?

A. Asymmetric encryption
B. Symmetric encryption
C. Spoofing
D. Digital certificate

Answer: D

NEW QUESTION 192

- (Topic 2)
Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

A. PING attack
B. Spoofing
C. Hacking
D. SYN attack

Answer: D

NEW QUESTION 195
- (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 199
- (Topic 2)
Your computer continues to operate even if its disk drive has failed. This ability is known as _____.

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

Answer: B

NEW QUESTION 203
- (Topic 2)
Peter is a merchant. He uses symmetric encryption to send confidential messages to different users of his Web site. Which of the following is the other name for asymmetric encryption?

A. Session key encryption
B. Public key encryption
C. Secret key encryption
D. Shared key encryption

Answer: B

NEW QUESTION 208
- (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 210
- (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 213
- (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 215
- (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 219
- (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 224
- (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 229
- (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 232
- (Topic 2)
You work as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. You are troubleshooting a computer of a user who is working on Windows Vista.
He reports that his sensitive data is being accessed by someone because of security vulnerability in the component of Windows Vista. Which of the following features of Windows Security Center will you configure to save the user's data?

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

Answer: C

NEW QUESTION 235
- (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 238
- (Topic 2)
Bluetooth uses the ______ specification in the _____ band with FHSS technology.

A. IEEE 802.11, 2.4-2.5 GHz
B. IEEE 802.11, 1.4-2.5 GHz
C. IEEE 802.15, 1.5-2.0 GHz
D. IEEE 802.15, 2.4-2.5 GHz

Answer: D

NEW QUESTION 243
- (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 247
- (Topic 2)
Which of the following combines the characteristics of a bridge and a router?

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

Answer: B

NEW QUESTION 250
- (Topic 2)
Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

A. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer
B. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer
C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer
D. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

Answer: D

NEW QUESTION 251
- (Topic 2)
Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

A. Sensitive
B. Unclassified
C. Confidential
D. Public
E. Secret
F. Private

Answer: ACDF

NEW QUESTION 253
- (Topic 2)
Which of the following types of firewalls forms a session flow table?

A. Proxy server firewall
B. Packet filtering firewall

C. Stateless packet filtering firewall
D. Stateful packet filtering firewall

Answer: D

NEW QUESTION 257
- (Topic 2)
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Status Accounting
B. Configuration Item Costing
C. Configuration Identification
D. Configuration Verification and Auditing

Answer: B

NEW QUESTION 260
- (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 263
- (Topic 2)
You work as the Network Administrator of TechJobs. You implement a security policy, to be in effect at all times, on the client computer in your network. While troubleshooting, assistant administrators often change security settings on the network. You want the security policy to be reapplied after changes have been made. How can you automate this task? (Click the Exhibit button on the toolbar to see the case study.)

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

Answer: D

NEW QUESTION 266
- (Topic 2)
Which of the following categories of the network management model is used to detect and log network problems or device failures?

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

Answer: A

NEW QUESTION 270
- (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 273
- (Topic 2)
Which term best describes an e-mail that contains incorrect and misleading information or warnings about viruses?

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

Answer: E

NEW QUESTION 275
- (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 277
- (Topic 2)
You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project?
Each correct answer represents a complete solution. Choose all that apply.

A. It provides the risk analysis of project configurations.
B. It provides object, orient, decide and act strategy.
C. It provides the versions for network devices.
D. It provides a live documentation of the project.

Answer: CD

NEW QUESTION 280
- (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 283
- (Topic 2)
Which of the following is the best approach to conflict resolution?

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

Answer: B

NEW QUESTION 285
- (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 287
- (Topic 3)
Rick works as a Network Administrator for Fimbry Hardware Inc. Based on the case study, which network routing strategy will he implement for the company? (Click the Exhibit button
on the toolbar to see the case study.)

A. He will implement OSPF on all the router interfaces.
B. He will implement RIP v1 on all the router interfaces.
C. He will implement the IGMP on all the router interface.
D. He will implement RIP v2 on all the router interfaces.
E. He will implement static routes for the routers.

Answer: E

NEW QUESTION 289
- (Topic 3)
You are the project manager for a software technology company. You and the project team have identified that the executive staff is not fully committed to the project. Which of the following best describes the risk?

A. Residual risks
B. Trend analysis
C. Schedule control
D. Organizational risks

Answer: D

NEW QUESTION 291
- (Topic 3)
Which of the following logs contains events pertaining to security as defined in the Audit policy?

A. DNS server log
B. Application log
C. System log
D. Directory Service log
E. Security log
F. File Replication Service log

Answer: E

NEW QUESTION 292
- (Topic 3)
Which of the following types of attack can guess a hashed password?

A. Teardrop attack
B. Evasion attack
C. Denial of Service attack
D. Brute force attack

Answer: D

NEW QUESTION 293
- (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 298
- (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 299
- (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 302

- (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 304
- (Topic 3)
You are the Network Administrator for a software development company. Your company creates various utilities and tools. You have noticed that some of the files your company creates are getting deleted from systems. When one is deleted, it seems to be deleted from all the computers on your network. Where would you first look to try and diagnose this problem?

A. Antivirus log
B. System log
C. IDS log
D. Firewall log

Answer: A

NEW QUESTION 308
- (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 309
- (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 311
- (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 315
......