Vendor: GIAC

Exam Code: GISF

Exam Name: GIAC Information Security Fundamentals

Version: Demo

QUESTION 1
Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

A. Risk acceptance
B. Risk transfer
C. Risk avoidance
D. Risk mitigation

Correct Answer: B

QUESTION 2
You have successfully installed an IRM server into your environment. This IRM server will be utilized to protect the company's videos, which are available to all employees but contain sensitive data. You log on to the WSS 3.0 server with administrator permissions and navigate to the Operations section. What option should you now choose so that you can input the RMS server name for the WSS 3.0 server to use?

A. Self-service site management
B. Content databases
C. Information Rights Management
D. Define managed paths

Correct Answer: C

QUESTION 3
You work as a security manager for Qualxiss Inc. Your Company involves OODA loop for resolving and deciding over company issues. You have detected a security breach issue in your company.

Which of the following procedures regarding the breach is involved in the observe phase of the OODA loop?

A. Follow the company security guidelines.
B. Decide an activity based on a hypothesis.
C. Implement an action practically as policies.
D. Consider previous experiences of security breaches.

Correct Answer: A

QUESTION 4
How should you configure the Regional Centers' e-mail, so that it is secure and encrypted? (Click the Exhibit button on the toolbar to see the case study.)

A. Use EFS.
B. Use IPSec.
C. Use S/MIME.
D. Use TLS.

Correct Answer: C

QUESTION 5
How long are cookies in effect if no expiration date is set?

A. Fifteen days
B. Until the session ends.
C. Forever

D. One year

Correct Answer: B

QUESTION 6
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

Correct Answer: A

QUESTION 7
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.

Correct Answer: BD

QUESTION 8
Based on the information given in the case study, which two authentication methods should you use to allow customers to access their photos on the Web site? (Click the Exhibit button on the toolbar to see the case study.) Each correct answer represents a part of the solution. Choose two.

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

Correct Answer: BE

QUESTION 9
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

Correct Answer: BCD

QUESTION 10
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

Correct Answer: B

QUESTION 11
You are the project manager of SST project. You are in the process of collecting and distributing performance information including status report, progress measurements, and forecasts. Which of the following process are you performing?

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

Correct Answer: C

QUESTION 12
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning:

nmap -PN -p- -sI IP_Address_of_Company_Server

He analyzes that the server's TCP ports 21, 25, 80, and 111 are open. Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

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

Correct Answer: A

QUESTION 13
Which of the following protocols provides secured transaction of data between two computers?

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

Correct Answer: A

QUESTION 14
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

Correct Answer: D

QUESTION 15
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

Correct Answer: BCD

QUESTION 16
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

Correct Answer: ABE

QUESTION 17
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John? Each correct answer represents a complete solution. Choose all that apply.

A. The virus, used by John, is not in the database of the antivirus program installed on the ser ver.
B. The mutation engine of the virus is generating a new encrypted code.
C. John has created a new virus.
D. John has changed the signature of the virus.

Correct Answer: ABCD

QUESTION 18
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

Correct Answer: D

QUESTION 19

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

Correct Answer: B

QUESTION 20
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

Correct Answer: A

QUESTION 21
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

Correct Answer: D

QUESTION 22
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

Correct Answer: D

QUESTION 23
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 *

Correct Answer: D

QUESTION 24
You are a Consumer Support Technician. You are helping a user troubleshoot computer-related issues.

While troubleshooting the user's computer, you find a malicious program similar to a virus or worm. The program negatively affects the privacy and security of the computer and is capable of damaging the computer. Which of the following alert levels of Windows Defender is set for this program?

A. Low
B. High
C. Severe
D. Medium

Correct Answer: C

QUESTION 25
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)

Correct Answer: D

QUESTION 26
You work as an Exchange Administrator for TechWorld Inc. The company has a Windows 2008 Active Directory-based network. The network contains an Exchange Server 2010 organization. The messaging organization contains one Hub Transport server, one Client Access server, and two Mailbox servers. You are planning to deploy an Edge Transport server in your messaging organization to minimize the attack surface. At which of the following locations will you deploy the Edge Transport server?

A. Active Directory site
B. Intranet
C. Behind the inner firewall of an organization
D. Perimeter network

Correct Answer: D

QUESTION 27
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

Correct Answer: BCD

QUESTION 28
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

Correct Answer: A

QUESTION 29
Availability Management allows organizations to sustain the IT service availability to support the business at a justifiable cost. Which of the following elements of Availability Management is used to perform at an agreed level over a period of time?
Each correct answer represents a part of the solution. Choose all that apply.

A. Maintainability
B. Resilience
C. Error control
D. Recoverability
E. Reliability
F. Security
G. Serviceability

Correct Answer: ABDEFG

QUESTION 30
Your company is going to add wireless connectivity to the existing LAN. You have concerns about the security of the wireless access and wish to implement encryption. Which of the following would be the best choice for you to use?

A. WAP
B. WEP
C. DES
D. PKI

Correct Answer: B

QUESTION 31
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

Correct Answer: C

QUESTION 32
Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

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

Correct Answer: C

QUESTION 33
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

Correct Answer: D

QUESTION 34
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

Correct Answer: D

QUESTION 35
The SALES folder has a file named XFILE.DOC that contains critical information about your company. This folder resides on an NTFS volume. The company's Senior Sales Manager asks you to provide security for that file. You make a backup of that file and keep it in a locked cupboard, and then you deny access on the file for the Sales group. John, a member of the Sales group, accidentally deletes that file. You have verified that John is not a member of any other group.

Although you restore the file from backup, you are confused how John was able to delete the file despite having no access to that file.

What is the most likely cause?

A. The Sales group has the Full Control permission on the SALES folder.
B. The Deny Access permission does not work on files.
C. The Deny Access permission does not restrict the deletion of files.
D. John is a member of another group having the Full Control permission on that file.

Correct Answer: A

QUESTION 36
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

Correct Answer: BD

QUESTION 37
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.

Correct Answer: A

QUESTION 38
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

Correct Answer: D

QUESTION 39
Which of the following monitors program activities and modifies malicious activities on a system?

A. Back door
B. HIDS
C. RADIUS
D. NIDS

Correct Answer: B

QUESTION 40
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.

Correct Answer: D

QUESTION 41
Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Cross-Site Request Forgery
B. Code injection attack
C. Cross-Site Scripting attack
D. Command injection attack

Correct Answer: B

QUESTION 42
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

Correct Answer: A

QUESTION 43
Which of the following does an anti-virus program update regularly from its manufacturer's Web site?

A. Hotfixes
B. Definition
C. Service packs
D. Permissions

Correct Answer: B

QUESTION 44
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.

Correct Answer: D

QUESTION 45
Hardening a system is one of the practical methods of securing a computer system. Which of the following techniques is used for hardening a computer system?

A. Disabling all user accounts
B. Applying egress filtering
C. Applying Access Control List (ACL)
D. Applying a patch to the OS kernel

Correct Answer: D

QUESTION 46
You work as a security manager in Mariotiss Inc. Your enterprise has been facing network and software security threats since a few months. You want to renew your current security policies and management to enhance the safety of your information systems. Which of the following is the best practice to initiate the renewal process from the lowest level with the least managerial effort?

A. Start the Incident handling process.
B. Change the entire security policy.
C. Perform an IT audit.
D. Switch to a new network infrastructure.

Correct Answer: C

QUESTION 47
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

Correct Answer: C

QUESTION 48
You are concerned about outside attackers penetrating your network via your company Web server.

You wish to place your Web server between two firewalls One firewall between the Web server and the outside world The other between the Web server and your network

What is this called?

A. IDS
B. SPI firewall
C. DMZ
D. Application Gateway firewall

Correct Answer: C

QUESTION 49
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)

Correct Answer: D

QUESTION 50
According to the case study, what protocol should be used to protect a customer's privacy and credit card information?
(Click the Exhibit button on the toolbar to see the case study.)

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

Correct Answer: E

QUESTION 51
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.

Correct Answer: C

QUESTION 52
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

Correct Answer: ABC

QUESTION 53
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.

Correct Answer: BC

QUESTION 54
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

Correct Answer: CD

QUESTION 55
Your Company is receiving false and abusive e-mails from the e-mail address of your partner company. When you complain, the partner company tells you that they have never sent any such e-mails. Which of the following types of cyber crimes involves this form of network attack?

A. Cyber squatting
B. Cyber Stalking
C. Man-in-the-middle attack
D. Spoofing

Correct Answer: D

QUESTION 56
You switch on your mobile Bluetooth device to transfer data to another Bluetooth device. Which of the following Information assurance pillars ensures that the data transfer is being performed with the targeted authorized Bluetooth device and not with any other or unauthorized device?

A. Data integrity
B. Confidentiality

C. Authentication
D. Non-repudiation

Correct Answer: C

QUESTION 57
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) Server. Use PPTP without packet filtering for VPN.
B. Use 128-bit encryption for Routing and Remote Access Service(RRAS) Server. Use PPTP without packet filtering for VPN.
C. Use 128-bit encryption for Routing and Remote Access Service(RRAS) Server. Use PPTP with packet filtering for VPN.
D. Use 40-bit encryption for the Routing and Remote Access Service(RRAS) Server. Use PPTP with packet filtering for VPN.

Correct Answer: C

QUESTION 58
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.

Correct Answer: BD

QUESTION 59
Which of the following terms is used for a router that filters traffic before it is passed to the firewall?

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

Correct Answer: A

QUESTION 60
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

Correct Answer: B

QUESTION 61
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

Correct Answer: BC

QUESTION 62
You have decided to implement an intrusion detection system on your network. You primarily are interested in the IDS being able to recognized known attack techniques. Which type of IDS should you choose?

A. Signature Based
B. Passive
C. Active
D. Anomaly Based

Correct Answer: A

QUESTION 63
You want to ensure that everyone who sends you an email should encrypt it. However you do not wish to exchange individual keys with all people who send you emails. In order to accomplish this goal which of the following should you choose?

A. DES
B. AES
C. Symmetric Encryption
D. Public Key encryption

Correct Answer: D

QUESTION 64
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

Correct Answer: C

QUESTION 65
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

Correct Answer: ABC

QUESTION 66
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)

Correct Answer: ACD

QUESTION 67
TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Windows
B. Red Hat
C. Solaris
D. Knoppix

Correct Answer: A

QUESTION 68
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)

Correct Answer: ABC

QUESTION 69
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

Correct Answer: C

QUESTION 70
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.

Correct Answer: D

QUESTION 71
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

Correct Answer: A

QUESTION 72
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.

Correct Answer: A

QUESTION 73
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

Correct Answer: D

QUESTION 74
You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

A. Denial-of-Service
B. Eavesdropping
C. Spoofing
D. Packet manipulation

Correct Answer: A

QUESTION 75
John works as a security manager in Mariotx.Inc. He has been tasked to resolve a network attack issue.

To solve the problem, he first examines the critical information about the attacker's interaction to the network environment. He prepares a past record and behavioral document of the attack to find a direction of the solution. Then he decides to perform an action based on the previous hypothesis and takes the appropriate action against the attack. Which of the following strategies has John followed?

A. Maneuver warfare
B. Control theory
C. SWOT Analysis
D. OODA loop

Correct Answer: D

QUESTION 76
Which of the following service provider classes is used to create a digital signature?

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

Correct Answer: F

QUESTION 77
Which of the following is a pillar of Information Assurance CIA triad?

A. Integrity
B. Affiliation
C. Accessibility
D. Isolation

Correct Answer: A

QUESTION 78
Adam, a novice Web user is getting large amount of unsolicited commercial emails on his email address. He suspects that the emails he is receiving are the Spam. Which of the following steps will he take to stop the Spam?
Each correct answer represents a complete solution. Choose all that apply.

A. Forward a copy of the spam to the ISP to make the ISP conscious of the spam.
B. Send an email to the domain administrator responsible for the initiating IP address.
C. Report the incident to the FTC (The U.S. Federal Trade Commission) by sending a copy of the spam message.
D. Close existing email account and open new email account.

Correct Answer: AC

QUESTION 79
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. Risk analysis
B. Firewall security
C. OODA loop
D. Cryptography

Correct Answer: D

QUESTION 80
You work as an executive manager for Mariotx.Inc. You entered into a business contract with a firm called Helfixnet.Inc. You passed on the contract details to Helfixnet.Inc and also got an acceptance approval. You later find that Helfixnet.Inc is violating the rules of the contract and they claim that they had never entered into any contract with Mariotx.Inc when asked. Which of the following directives of Information Assurance can you apply to ensure prevention from such issues?

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

Correct Answer: B

QUESTION 81
You work in an enterprise as a Network Engineer. Your enterprise has a secure internal network.

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

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

Correct Answer: C

QUESTION 82
The security of a computer against the unauthorized usage largely depends upon the efficiency of the applied access control method. Which of the following statements are true about a computer access control method?
Each correct answer represents a complete solution. Choose all that apply.

A. It can be based upon fingerprint or eye recognition.
B. It can be time-synchronous.
C. It provides security against the virus attacks.
D. It provides security against Eavesdropping.
E. It checks the authenticity of a person.
F. It is used to encrypt a message before transmitting it on a network.

Correct Answer: ABE

QUESTION 83
Which of the following tools is an open source network intrusion prevention and detection system that operates as a network sniffer?

A. IPLog
B. Snort
C. Timbersee
D. Swatch

Correct Answer: B

QUESTION 84
Which of the following factors determine the strength of the encryption?

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

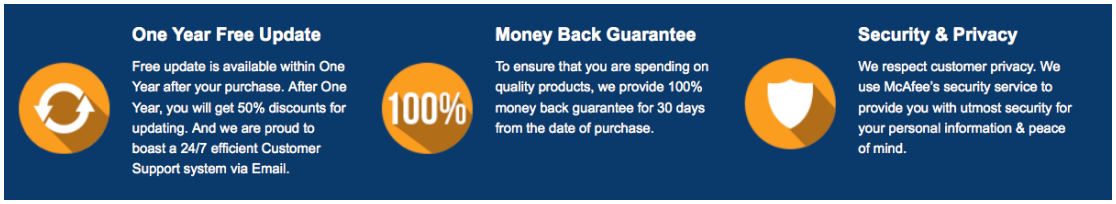
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions