Vendor: GIAC

Exam Code: GISP

Exam Name: GIAC Information Security Professional

Version: Demo

Topic 1, Volume A

QUESTION NO: 1

Which of the following is a technique used to attack an Ethernet wired or wireless network?

A. DNS poisoning
B. Keystroke logging
C. Mail bombing
D. ARP poisoning

Answer: D

QUESTION NO: 2

Which of the following refers to encrypted text?

A. Plaintext
B. Cookies
C. Hypertext
D. Ciphertext

Answer: D

QUESTION NO: 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: A,C

QUESTION NO: 4

Mark works as a Network Administrator for NetTech Inc. He wants users to access only those

resources that are required for them. Which of the following access control models will he use?

A. Role-Based Access Control
B. Discretionary Access Control
C. Mandatory Access Control
D. Policy Access Control

Answer: A

QUESTION NO: 5

Which of the following are methods used for authentication?

Each correct answer represents a complete solution. Choose all that apply.

A. Smart card
B. Biometrics
C. Username and password
D. Magnetic stripe card

Answer: A,B,C,D

QUESTION NO: 6

Which of the following protocols is used to verify the status of a certificate?

A. CEP
B.HTTP
C.OSPF
D.OCSP

Answer: D

QUESTION NO: 7

Fill in the blank with the appropriate value.

Service Set Identifiers (SSIDs) are case sensitive text strings that have a maximum length of

_____characters.

A. 32

Answer: A

QUESTION NO: 8

You work as a Network Administrator for NetTech Inc. The company has a network that consists of 200 client computers and ten database servers. One morning, you find that a hacker is accessing unauthorized data on a database server on the network. Which of the following actions will you take to preserve the evidences?

Each correct answer represents a complete solution. Choose three.

A. Prevent a forensics experts team from entering the server room.
B. Preserve the log files for a forensics expert.
C. Prevent the company employees from entering the server room.
D. Detach the network cable from the database server.

Answer: B,C,D

QUESTION NO: 9

Which of the following heights of fence deters only casual trespassers?

A. 3 to 4 feet
B. 2 to 2.5 feet
C. 8 feet
D. 6 to 7 feet

Answer: A

QUESTION NO: 10

Which of the following statements about *role-based access control (RBAC)* model is true?

A. In this model, a user can access resources according to his role in the organization.
B. In this model, the permissions are uniquely assigned to each user account.
C. In this model, the same permission is assigned to each user account.
D. In this model, the users can access resources according to their seniority.

Answer: A

QUESTION NO: 11

Which of the following statements about a *fiber-optic* cable are true?

Each correct answer represents a complete solution. Choose three.

A. It is immune to electromagnetic interference (EMI).
B. It can transmit undistorted signals over great distances.
C. It has eight wires twisted into four pairs.
D. It uses light pulses for signal transmission.

Answer: A,B,D

QUESTION NO: 12

Which of the following statements about the bridge are true?

Each correct answer represents a complete solution. Choose two.

A. It filters traffic based on IP addresses.
B. It forwards broadcast packets.
C. It assigns a different network address per port.
D. It filters traffic based on MAC addresses.

Answer: B,D

QUESTION NO: 13

Sam works as a Web Developer for McRobert Inc. He wants to control the way in which a Web browser receives information and downloads content from Web sites. Which of the following browser settings will Sam use to accomplish this?

A. Proxy server
B. Security
C. Cookies
D. Certificate

Answer: B

QUESTION NO: 14

Which of the following are used to suppress paper or wood fires?

Each correct answer represents a complete solution. Choose two.

A. Water
B. Kerosene
C. CO2
D. Soda acid

Answer: A,D

QUESTION NO: 15

Which of the following steps can be taken to protect laptops and data they hold?

Each correct answer represents a complete solution. Choose all that apply.

A. Use slot locks with cable to connect the laptop to a stationary object.
B. Keep inventory of all laptops including serial numbers.
C. Harden the operating system.
D. Encrypt all sensitive data.

Answer: A,B,C,D

QUESTION NO: 16

Which of the following attacks involves multiple compromised systems to attack a single target?

A. Brute force attack
B. DDoS attack
C. Dictionary attack
D. Replay attack

Answer: B

QUESTION NO: 17

Which of the following statements about *DMZ* are true?

Each correct answer represents a complete solution. Choose two.

A. It is an anti-virus software that scans the incoming traffic on an internal network.
B. It is the boundary between the Internet and a private network.
C. It contains company resources that are available on the Internet, such as Web servers and FTP servers.
D. It contains an access control list (ACL).

Answer: B,C

QUESTION NO: 18

Which of the following protocols is used to establish a secure TELNET session over TCP/IP?

A. SSL
B. PGP
C. IPSEC
D. SSH

Answer: D

QUESTION NO: 19

Which methods help you to recover your data in the event of a system or hard disk failure?

Each correct answer represents a complete solution. Choose two.

A. Install a RAID system
B. Use data encryption
C. Install and use a tape backup unit
D. Install UPS systems on all important devices

Answer: A,C

QUESTION NO: 20

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as _____.

A. False positive
B. False negative
C. True negative
D. True positive

Answer: A

QUESTION NO: 21

Which of the following statements about *smurf* is true?

A. It is an ICMP attack that involves spoofing and flooding.
B. It is a UDP attack that involves spoofing and flooding.
C. It is a denial of service (DoS) attack that leaves TCP ports open.
D. It is an attack with IP fragments that cannot be reassembled.

Answer: A

QUESTION NO: 22

Which of the following policies is set by a network administrator to allow users to keep their emails and documents for a fixed period of time?

A. Retention policy
B. Password policy
C. Audit policy
D. Backup policy

Answer: A

QUESTION NO: 23

Which of the following statements about *Switched Multimegabit Data Service (SMDS)* are true?

Each correct answer represents a complete solution. Choose two.

A. It is a logical connection between two devices.
B. It uses fixed-length (53-byte) packets to transmit information.
C. It supports speeds of 1.544 Mbps over Digital Signal level 1 (DS-1) transmission facilities.
D. It is a high-speed WAN networking technology used for communication over public data networks

Answer: C,D

QUESTION NO: 24

Which of the following terms refers to the protection of data against unauthorized access?

A. Auditing
B. Recovery
C. Confidentiality
D. Integrity

Answer: C

QUESTION NO: 25

Which of the following is a *remote access protocol* that supports *encryption*?

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

Answer: A

QUESTION NO: 26

Which of the following is the best way of protecting important data against *virus* attack?

A. Updating the anti-virus software regularly.
B. Taking daily backup of data.

C. Using strong passwords to log on to the network.
D. Implementing a firewall.

Answer: A

QUESTION NO: 27

Which of the following functions are performed by a *firewall*?

Each correct answer represents a complete solution. Choose all that apply.

A. It hides vulnerable computers that are exposed to the Internet.
B. It logs traffic to and from the private network.
C. It enhances security through various methods, including packet filtering, circuit-level filtering, and application filtering.
D. It blocks unwanted traffic.

Answer: A,B,C,D

QUESTION NO: 28

Which of the following statements about *Digest authentication* are true?

Each correct answer represents a complete solution. Choose two.

A. In Digest authentication, passwords are sent across a network as clear text, rather than as a has value.
B. Digest authentication is used by wireless LANs, which follow the IEEE 802.11 standard.
C. In Digest authentication, passwords are sent across a network as a hash value, rather than as clear text.
D. Digest authentication is a more secure authentication method as compared to Basic authentication.

Answer: C,D

QUESTION NO: 29

Which of the following types of attacks slows down or stops a server by overloading it with requests?

A. Vulnerability attack
B. Impersonation attack
C. Network attack
D. DoS attack

Answer: D

QUESTION NO: 30

Which of the following is the most secure authentication method?

A. Certificate-based authentication
B. Basic authentication
C. Digest authentication
D. Integrated Windows authentication

Answer: A

QUESTION NO: 31

Which of the following practices come in the category of denial of service attack?

Each correct answer represents a complete solution. Choose three.

A. Sending lots of ICMP packets to an IP address
B. Disrupting services to a specific computer
C. Performing Back door attack on a system
D. Sending thousands of malformed packets to a network for bandwidth consumption

Answer: A,B,D

QUESTION NO: 32

What does the Internet encryption and authentication system named *RSA* stand for?

A. Rivest-Shamir-Adleman
B. Read System Authority
C. Rivest-System-Adleman
D. Remote System Authority

Answer: A

QUESTION NO: 33

Which of the following authentication methods support mutual authentication?

Each correct answer represents a complete solution. Choose two.

A. MS-CHAP v2
B. EAP-TLS
C. EAP-MD5
D. NTLM

Answer: A,B

QUESTION NO: 34

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. Internet

Answer: A

QUESTION NO: 35

Which of the following are the application layer protocols for security?

Each correct answer represents a complete solution. Choose three.

A. Secure Hypertext Transfer Protocol (S-HTTP)
B. Secure Sockets Layer (SSL)
C. Secure Electronic Transaction (SET)
D. Secure Shell (SSH)

Answer: A,C,D

QUESTION NO: 36

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He wants to corrupt an IDS signature database so that performing attacks on the server is made easy and he can observe the flaws in the We-are-secure server. To perform his task, he first of all sends a virus that continuously changes its signature to avoid detection from IDS. Since the new signature of the virus does not match the old signature, which is entered in the IDS signature database, IDS becomes unable to point out the malicious virus. Which of the following IDS evasion attacks is John performing?

A. Session splicing attack
B. Evasion attack
C. Insertion attack
D. Polymorphic shell code attack

Answer: D

QUESTION NO: 37

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Teardrop attack
B. Denial of Service attack
C. Land attack
D. Replay attack

Answer: B

QUESTION NO: 38

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party. Which of the following scanning techniques will John use to accomplish his task?

A. RPC

B. IDLE
C. UDP
D. TCP SYN/ACK

Answer: D

QUESTION NO: 39

Mark has been hired by a company to work as a Network Assistant. He is assigned the task to configure a dial-up connection. He is configuring a laptop. Which of the following protocols should he disable to ensure that the password is encrypted during remote access?

A. SPAP
B. MSCHAP V2
C. PAP
D. MSCHAP

Answer: C

QUESTION NO: 40

Which of the following are *data link layer* components?

Each correct answer represents a complete solution. Choose three.

A. Switches
B. Bridges
C. MAC addresses
D. Hub

Answer: A,B,C

QUESTION NO: 41

Which of the following statements about a *host-based intrusion prevention system (HIPS)* are true?

Each correct answer represents a complete solution. Choose two.

A. It can detect events scattered over the network.
B. It is a technique that allows multiple computers to share one or more IP addresses.
C. It cannot detect events scattered over the network.
D. It can handle encrypted and unencrypted traffic equally.

Answer: C,D

QUESTION NO: 42

You work as a professional Ethical Hacker. You are assigned a project to test the security of www.we-are-secure.com. You are working on the Windows Server 2003 operating system. You suspect that your friend has installed the keyghost keylogger onto your computer. Which of the following countermeasures would you employ in such a situation?

Each correct answer represents a complete solution. Choose all that apply.

A. Use on-screen keyboards and speech-to-text conversion software which can also be useful agains keyloggers, as there are no typing or mouse movements involved.
B. Remove the SNMP agent or disable the SNMP service.
C. Use commercially available anti-keyloggers such as PrivacyKeyboard.
D. Monitor the programs running on the server to see whether any new process is running on the server or not.

Answer: A,C,D

QUESTION NO: 43

Which of the following can be prevented by an organization using job rotation and separation of duties policies?

A. Collusion
B. Eavesdropping
C. Buffer overflow
D. Phishing

Answer: A

QUESTION NO: 44

Which of the following protocols work at the data-link layer?

Each correct answer represents a complete solution. Choose two.

A. NFS
B. SSL
C. ARP
D. PPP

Answer: C,D

QUESTION NO: 45

Which of the following terms refers to the method that allows or restricts specific types of packets from crossing over the *firewall*?

A. Web caching
B. Hacking
C. Packet filtering
D. Spoofing

Answer: C

QUESTION NO: 46

Which of the following encryption methods comes under symmetric encryption algorithm?

Each correct answer represents a complete solution. Choose three.

A. Blowfish
B. DES
C. Diffie-Hellman
D. RC5

Answer: A,B,D

QUESTION NO: 47

Fill in the blank with the appropriate term.

A _____ is a digital representation of information that identifies authorized users on the Internet and intranets.

A. certificate

Answer: A

QUESTION NO: 48

Which of the following defines the communication link between a Web server and Web applications?

A. PGP
B. CGI
C. IETF
D. Firewall

Answer: B

QUESTION NO: 49

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

Answer: A,B,C,D

QUESTION NO: 50

Which of the following are the centralized administration technologies?

Each correct answer represents a complete solution. Choose all that apply.

A. TACACS+
B. RADIUS
C. Media Access control
D. Peer-to-Peer

Answer: A,B

QUESTION NO: 51

Which of the following statements about *active attack* is true?

A. It does not insert false packets into the data stream.
B. It makes the computer's network services unavailable.
C. It inserts false packets into the data stream.
D. It locks out the users' accounts.

Answer: C

QUESTION NO: 52

Which of the following are the ways of sending secure e-mail messages over the Internet?

Each correct answer represents a complete solution. Choose two.

A. PGP
B. IPSec
C. TLS
D. S/MIME

Answer: A,D

QUESTION NO: 53

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

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

Answer: D

QUESTION NO: 54

Which of the following protocols is built in the Web server and browser to encrypt data traveling over the Internet?

A. UDP
B. HTTP
C. SSL
D.IPSec

Answer: C

QUESTION NO: 55

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

A. Cookie
B. Trade secret
C. Utility model
D. Copyright

Answer: B

QUESTION NO: 56

Which of the following statements about *Diffie-Hellman encryption* are true?

Each correct answer represents a complete solution. Choose two.

A. It uses only a private key.

B. It uses both a public key and a private key.
C. It does not authenticate the parties involved.
D. It was developed in 1976.

Answer: B,D

QUESTION NO: 57

Andrew works as a Network Administrator for Infonet Inc. The company's network has a Web server that hosts the company's Web site. Andrew wants to increase the security of the Web site by implementing *Secure Sockets Layer (SSL)*. Which of the following types of encryption does SSL use?

Each correct answer represents a complete solution. Choose two.

A. Secret
B. Asymmetric
C. Synchronous
D. Symmetric

Answer: B,D

QUESTION NO: 58

Which of the following steps are generally followed in computer forensic examinations?

Each correct answer represents a complete solution. Choose three.

A. Acquire
B. Analyze
C. Encrypt
D. Authenticate

Answer: A,B,D

QUESTION NO: 59

John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.

Original cookie values:

ItemID1=2

ItemPrice1=900

ItemID2=1

ItemPrice2=200

Modified cookie values:

ItemID1=2

ItemPrice1=1

ItemID2=1

ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.

Which of the following hacking techniques is John performing?

A. Cross site scripting
B. Man-in-the-middle attack
C. Cookie poisoning
D. Computer-based social engineering

Answer: C

QUESTION NO: 60

Which of the following is the default port for the NetBIOS name service?

A. UDP port 137
B. TCP port 110
C. UDP port 138
D. TCP port 119

Answer: A

QUESTION NO: 61

Which of the following access control models are used in the commercial sector?

Each correct answer represents a complete solution. Choose two.

A. Clark-Wilson model
B. Clark-Biba model
C. Bell-LaPadula model
D. Biba model

Answer: A,D

QUESTION NO: 62

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully performed the following steps of the preattack phase to check the security of the We-are-secure network:

•Gathering information

•Determining the network range

•Identifying active systems

Now, he wants to find the open ports and applications running on the network. Which of the following tools will he use to accomplish his task?

A. ARIN
B. APNIC
C. SuperScan
D. RIPE

Answer: C

QUESTION NO: 63

You work as a Network Administrator for NetTech Inc. When you enter http://66.111.64.227 in the browser's address bar, you are able to access the site. But, you are unable to access the site when you enter http://www.PassGuide.com. What is the most likely cause?

A. The site's Web server has heavy traffic.
B. The site's Web server is offline.
C. WINS server has no NetBIOS name entry for the server.
D. DNS entry is not available for the host name.

Answer: D

QUESTION NO: 64

Which of the following tools is a component of Cisco Adaptive Security Appliance (ASA) and provides an in-depth security design to prevent various types of problems such as viruses, spams, and spyware?

A. Anti-x
B. LIDS
C. Scanlogd
D. KFSensor

Answer: A

QUESTION NO: 65

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2000 domain-based network. Users report that they are unable to log on to the network. Mark finds that accounts are locked out due to multiple incorrect log on attempts. What is the most likely cause of the account lockouts?

A. SYN attack
B. Spoofing
C. PING attack
D. Brute force attack

Answer: D

QUESTION NO: 66

Which of the following are tunneling protocols?

Each correct answer represents a complete solution. Choose two.

A. NNTP
B. SMTP
C. L2TP
D. PPTP

Answer: C,D

QUESTION NO: 67

Which of the following statements about the *One Time Password (OTP)* security system are true?

Each correct answer represents a complete solution. Choose two.

A. It requires a password only once to authenticate users.
B. It requires a new password every time a user authenticates himself.
C. It generates passwords by using either the MD4 or MD5 hashing algorithm.
D. It generates passwords by using Kerberos v5.

Answer: B,C

QUESTION NO: 68

Which of the following are ensured by the concept of integrity in information system security?

Each correct answer represents a complete solution. Choose two.

A. Unauthorized modifications are not made by authorized users.
B. Data modifications are not made by an unauthorized user or process.
C. The intentional or unintentional unauthorized disclosure of a message or important document contents is prevented.
D. The systems are up and running when they are needed.

Answer: A,B

QUESTION NO: 69

You work as a Network Administrator for Net World International. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. There are ten Sales Managers in the company. The company has recently

provided laptops to all its Sales Managers. All the laptops run Windows XP Professional. These laptops will be connected to the company's network through wireless connections. The company's management wants to implement Shared Key *authentication* for these laptops. When you try to configure the network interface card of one of the laptops for Shared Key authentication, you find no such option. What will you do to enable Shared Key authentication?

A. Install PEAP-MS-CHAP v2.
B. Install Service Pack 1.
C. Enable WEP.
D. Install EAP-TLS.

Answer: C

QUESTION NO: 70

You work as a Network Administrator for Infonet Inc. The company's network has an FTP server.

You want to secure the server so that only authorized users can access it. What will you do to accomplish this?

A. Stop the FTP service on the server.
B. Disable anonymous authentication.
C. Disable the network adapter on the server.
D. Enable anonymous authentication.

Answer: B

QUESTION NO: 71

Fill in the blank with the appropriate layer name of the OSI model.

Secure Socket Layer (SSL) operates at the

_____layer of the OSI model.

A. transport

Answer: A

QUESTION NO: 72
Which of the following is a source port forwarder and redirector tool?

A. Fpipe
B. NMAP
C. SuperScan
D. NSLOOKUP

Answer: A

QUESTION NO: 73

Which of the following statements about *Due Care* policy is true?

A. It provides information about new viruses.
B. It is a method used to authenticate users on a network.
C. It identifies the level of confidentiality of information.
D. It is a method for securing database servers.

Answer: C

QUESTION NO: 74

Which of the following methods backs up all changes made since the last full or normal backup?

A. Half backup
B. Incremental backup
C. Differential backup
D. Full backup

Answer: C

QUESTION NO: 75

Which of the following statements about *Discretionary Access Control List (DACL)* is true?

A. It is a rule list containing access control entries.
B. It specifies whether an audit activity should be performed when an object attempts to access a resource.
C. It is a list containing user accounts, groups, and computers that are allowed (or denied) access to the object.

D. It is a unique number that identifies a user, group, and computer account.

Answer: C

QUESTION NO: 76

Which of the following types of attack can be used to break the best physical and logical security mechanism to gain access to a system?

A. Social engineering attack
B. Password guessing attack
C. Mail bombing
D. Cross site scripting attack

Answer: A

QUESTION NO: 77

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

A. Dictionary attack
B. DDoS attack
C. Insertion attack
D. Evasion attack

Answer: B

QUESTION NO: 78

Which of the following languages enable programmers to store *cookies* on client computers?

Each correct answer represents a complete solution. Choose two.

A. Perl
B. DHTML
C. JavaScript
D. HTML

Answer: A,C

QUESTION NO: 79

Which of the following statement about *eavesdropping* is true?

A. It is a type of password guessing attack.
B. It is a way of preventing electronic emissions that are generated from a computer or network.
C. It is known as network saturation attack or bandwidth consumption attack.
D. It is the process of hearing or listening in private conversations.

Answer: D

QUESTION NO: 80

You work as a Database Administrator for Bluewell Inc. The company has a SQL Server 2005 computer. The company asks you to implement a RAID system to provide fault tolerance to a database. You want to implement disk mirroring. Which of the following RAID levels will you use to accomplish the task?

A. RAID-1
B. RAID-10
C. RAID-0
D. RAID-5

Answer: A

QUESTION NO: 81

Which of the following layers of the OSI model provides end-to-end service?

A. The physical layer
B. The application layer
C. The session layer
D. The transport layer

Answer: D

QUESTION NO: 82

These are false reports about non-existent viruses. In these reports, the writer often claims to do impossible things. Due to these false reports, the network administrator shuts down his network, which in turn affects the work of the company. These reports falsely claim to describe an extremely dangerous virus, and declare that the report is issued by a reputed company. These reports are known as _____.

A. Time bombs
B. Virus hoaxes
C. Chain letters
D. Spambots
E. Logic bombs

Answer: B

QUESTION NO: 83

Which of the following statements are true about a Gantt chart?

Each correct answer represents a complete solution. Choose all that apply.

A. It displays the duration of a task.
B. It is easier to plan than PERT.
C. It displays dependencies between activities.
D. The impact of slippage is easily determined.

Answer: A,B,D

QUESTION NO: 84

Which of the following is a network service that stores and organizes information about a network users and network resources and that allows administrators to manage users' access to the resources?

A. Terminal service
B. DFS service
C. SMTP service
D. Directory service

Answer: D

QUESTION NO: 85

Mark the list that mentions the correct levels of classification of the *military data-classification system*.

A.-4

Answer: A

QUESTION NO: 86

Which of the following processes is known as *sanitization*?

A. Physically destroying the media and the information stored on it.
B. Assessing the risk involved in discarding particular information.
C. Verifying the identity of a person, network host, or system process.
D. Removing the content from the media so that it is difficult to restore.

Answer: D

QUESTION NO: 87

Which of the following are used to suppress gasoline and oil fires?

Each correct answer represents a complete solution. Choose three.

A. Water
B. CO2
C. Halon
D. Soda acid

Answer: B,C,D

QUESTION NO: 88

You are responsible for a Microsoft based network. Your servers are all clustered. Which of the following are the likely reasons for the clustering?

Each correct answer represents a complete solution. Choose two.

A. Load balancing
B. Ease of maintenance
C. Failover
D. Reduce power consumption

Answer: A,C

QUESTION NO: 89

Which of the following tools can be used to perform polymorphic shell code attacks?

A. TrueCrypt
B. Fragroute
C. Mendax
D. ADMutate

Answer: D

QUESTION NO: 90

Mark works as a Network Administrator for NetTech Inc. The company has a Windows 2003 domainbased network. The company has two offices in different cities. The offices are connected through the Internet. Both offices have a Windows 2003 server named SERV1 and SERV2 respectively. Mark is required to create a secure connection between both offices. He configures a VPN connection between the offices using the two servers. He uses L2TP for VPN and also configures an IPSec tunnel. Which of the following will he achieve with this configuration?

Each correct answer represents a part of the solution. Choose two.

A. Highest possible encryption for traffic between the offices
B. Encryption for the local files stored on the two servers
C. Extra bandwidth on the Internet connection
D. Mutual authentication between the two servers

Answer: A,D

QUESTION NO: 91

Which of the following statements about *digital signature* is true?

A. Digital signature compresses the message to which it is applied.
B. Digital signature is required for an e-mail message to get through a firewall.
C. Digital signature verifies the identity of the person who applies it to a document.
D. Digital signature decrypts the contents of documents.

Answer: C

QUESTION NO: 92

Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

A. IMAP
B. SNMP
C. SMTP
D. POP3

Answer: A

QUESTION NO: 93

Which of the following refers to going through someone's trash to find out useful or confidential information?

A. Dumpster diving
B. Hacking
C. Phishing
D. Spoofing

Answer: A

QUESTION NO: 94

Which of the following have been developed to address security issues in the e-commerce system?

Each correct answer represents a complete solution. Choose two.

A. Digital cash
B. Encryption frameworks
C. Shopping cart
D. Digital signatures

Answer: B,D

QUESTION NO: 95

Which of the following terms refers to the act of obtaining plain text from cipher text without a cryptographic key?

A. Hacking
B. Algorithm
C. Cryptanalysis
D. Ciphertext

Answer: C

QUESTION NO: 96

Against which of the following does *SSH* provide protection?

Each correct answer represents a complete solution. Choose two.

A. DoS attack
B. Password sniffing
C. Broadcast storm
D. IP spoofing

Answer: B,D

QUESTION NO: 97

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He recommends a disk encryption tool to encrypt the secret files of the We-are-secure server. He presents a report to the We-are-secure authorities as given below:

Which of the following tools is John recommending for disk encryption on the We-are-secure server?

A. CryptoHeaven
B. Stunnel
C. TrueCrypt
D. Magic Lantern

Answer: C

QUESTION NO: 98

Which of the following protocols is used to securely connect to a private network by a remote client using the Internet?

A. PAP
B. PPTP
C. UDP
D. IPSec

Answer: B

QUESTION NO: 99

Which of the following categories of UTP cable has maximum data transfer rate of 155 Mbps?

A. Category 5
B. Category 3
C. Category 7
D. Category 6

Answer: D

QUESTION NO: 100

Perfect World Inc., provides its sales managers access to the company's network from remote locations. The sales managers use laptops to connect to the network. For security purposes, the company's management wants the sales managers to log on to the network using *smart cards* over a remote connection. Which of the following authentication protocols should be used to accomplish this?

A. Challenge Handshake Authentication Protocol (CHAP)
B. Extensible Authentication Protocol (EAP)
C. Open Shortest Path First (OSPF)
D. Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)

Answer: B

QUESTION NO: 101

Which of the following rate systems of the Orange book has no security controls?

A. C-rated
B. D-rated
C. A-rated
D. E-rated

Answer: B

QUESTION NO: 102

Fill in the blank with the appropriate value.

Digital Subscriber Line must be installed within a

_____kilometer radius of the telephone company's access point.

A. 5.5

Answer: A

QUESTION NO: 103
Which of the following refers to the exploitation of a valid computer session to gain unauthorized

access to information or services in a computer system?

A. Piggybacking
B. Hacking
C. Session hijacking
D. Keystroke logging

Answer: C

QUESTION NO: 104

Which of the following type of errors occurs when a legitimate user incorrectly denied access to resources by the Biometrics authentication systems?

A. Type II
B. Type I
C. Type III
D. Type IV

Answer: B

QUESTION NO: 105

Which of the following are the differences between PPTP and L2TP?

Each correct answer represents a complete solution. Choose three.

A. L2TP does not provide any kind of security.
B. PPTP connections use Microsoft Point-to-Point Encryption (MPPE), whereas L2TP uses Data Encryption Standard (DES).
C. L2TP may be used with IPSec, while PPTP stands alone.
D. PPTP is supported by most industry vendors, while L2TP is a proprietary Microsoft standard.

Answer: A,B,C

QUESTION NO: 106

Which of the following statements about *extranet* are true?

Each correct answer represents a complete solution. Choose two.

A. It is an area of a company's Web site, which is only available to selected customers, suppliers, an business partners.
B. It is an area of a company's Web site, which is available to Internet users.
C. It is an arrangement commonly used for business-to-business relationships.
D. It is an arrangement commonly used for a company's employees.

Answer: A,C

QUESTION NO: 107

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. Auditing
C. Security policy
D. Security awareness training

Answer: C,D

QUESTION NO: 108

Which of the following is the process of overwriting all addressable locations on a disk?

A. Sanitization
B. Authentication
C. Spoofing
D. Drive wiping

Answer: D

QUESTION NO: 109

John works as a Network Administrator for We-are-secure Inc. The We-are-secure server is based on Windows Server 2003. One day, while analyzing the network security, he receives an error message that Kernel32.exe is encountering a problem. Which of the following steps should John

take as a countermeasure to this situation?

Each correct answer represents a complete solution. Choose all that apply.

A. He should upgrade his antivirus program.
B. He should download the latest patches for Windows Server 2003 from the Microsoft site, so that he can repair the kernel.
C. He should observe the process viewer (Task Manager) to see whether any new process is running on the computer or not. If any new malicious process is running, he should kill that process.
D. He should restore his Windows settings.

Answer: A,C

QUESTION NO: 110

Which of the following Windows RRAS authentication protocols uses completely unencrypted passwords?

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

Answer: A

QUESTION NO: 111

Which of the following statements about *DMZ* is true?

A. DMZ is a corporate network used as the Internet.
B. DMZ is a firewall that lies in between two corporate networks.
C. DMZ is a network that is not connected to the Internet.
D. DMZ is a network that lies in between a corporate network and the Internet.

Answer: D

QUESTION NO: 112

Which of the following components come under the *network layer* of the OSI model?

Each correct answer represents a complete solution. Choose two.

A. Firewalls
B. Hub
C. Routers
D. MAC addresses

Answer: A,C

QUESTION NO: 113

Which of the following is the default port for *Secure Shell (SSH)*?

A. TCP port 22
B. UDP port 161
C. UDP port 138
D. TCP port 443

Answer: A

QUESTION NO: 114

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trademark
B. Patent
C. Trade secret
D. Copyright

Answer: A

QUESTION NO: 115

Which of the following techniques are used to secure wireless networks?

Each correct answer represents a complete solution. Choose three.

A. MAC address filtering
B. SSID spoofing
C. IP spoofing
D. Closed network

Answer: A,B,D

QUESTION NO: 116

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave *TCP ports* half open?

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

Answer: C

QUESTION NO: 117

Which of the following is a type of intruder detection that involves logging network events to a file for an administrator to review later?

A. Passive detection
B. Event detection
C. Active detection
D. Packet detection

Answer: A

QUESTION NO: 118

Which of the following cables provides maximum security against electronic eavesdropping on a network?

A. Fibre optic cable
B. NTP cable

C. STP cable
D. UTP cable

Answer: A

QUESTION NO: 119

At which of the following layers Structured Query Language (SQL) works?

A. Physical
B. Network
C. Transport
D. Session

Answer: D

QUESTION NO: 120

You work as a Network Administrator of a TCP/IP network. You are having *DNS* resolution problem. Which of the following utilities will you use to diagnose the problem?

A. NSLOOKUP
B. IPCONFIG
C. PING
D. TRACERT

Answer: A

QUESTION NO: 121

Which of the following entities is used by Routers and firewalls to determine which packets should be forwarded or dropped?

A. Rainbow table
B. Rootkit
C. Access control list
D. Backdoor

Answer: C

QUESTION NO: 122

Which of the following are natural environmental threats that an organization faces?

Each correct answer represents a complete solution. Choose two.

A. Storms
B. Floods
C. Strikes
D. Accidents

Answer: A,B

QUESTION NO: 123

Which of the following encryption algorithms are based on block ciphers?

A. RC4
B. RC5
C. Twofish
D. Rijndael

Answer: B,C,D

QUESTION NO: 124

Which of the following are the responsibilities of the owner with regard to data in an information classification program?

Each correct answer represents a complete solution. Choose three.

A. Delegating the responsibility of the data protection duties to a custodian.
B. Determining what level of classification the information requires.
C. Running regular backups and routinely testing the validity of the backup data.
D. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.

Answer: A,B,D

QUESTION NO: 125

What will be the best strategy to prevent employees on a Local Area Network from performing unauthorized activities?

A. Grant the employees minimum permissions that are needed to perform the required tasks.
B. Limit the number of files that any employee can open at any given time.
C. Grant the employees maximum permissions that are needed to perform the required tasks.
D. Store the resources on a hard disk that has NTFS partitions.

Answer: A

QUESTION NO: 126

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided laptops to its sales team members. You have configured access points in the network to enable a wireless network. The company's security policy states that all users using laptops must use smart cards for *authentication*. Which of the following authentication techniques will you use to implement the security policy of the company?

A. IEEE 802.1X using EAP-TLS
B. Pre-shared key
C. IEEE 802.1X using PEAP-MS-CHAP
D. Open system

Answer: A

QUESTION NO: 127

In which of the following scanning techniques does a scanner connect to an FTP server and request that server to start data transfer to the third system?

A. Xmas Tree scanning
B. TCP SYN scanning
C. Bounce attack scanning

D. TCP FIN scanning

Answer: C

QUESTION NO: 128

Which of the following protocols is used to query and modify information stored within the directory services?

A. PPTP
B. ARP
C. PAP
D. LDAP

Answer: D

QUESTION NO: 129

Which of the following does *Certification Authority (CA)* provide in an e-commerce system?

Each correct answer represents a complete solution. Choose two.

A. Credit
B. Trust
C. Transparency
D. Identification

Answer: B,D

QUESTION NO: 130

In which of the following attacks does an attacker send a spoofed TCP SYN packet in which the target's IP address is filled in both the source and destination fields?

A. Jolt DoS attack
B. Ping of death attack
C. Teardrop attack
D. Land attack

Answer: D

QUESTION NO: 131

Which of the following terms is used for securing an operating system from an attack?

A. System hacking
B. System hardening
C. System mirroring
D. System indexing

Answer: B

QUESTION NO: 132

Which of the following access control models uses a role based method to determine access rights and permission?

A. Discretionary access control
B. Roaming access control
C. Nondiscretionary access control
D. Mandatory access control

Answer: C

QUESTION NO: 133

Which of the following ports is the default port for *Layer 2 Tunneling Protocol (L2TP)* ?

A. UDP port 1701
B. UDP port 161
C. TCP port 443
D. TCP port 110

Answer: A

QUESTION NO: 134

Which of the following is a process of monitoring data packets that travel across a network?

A. Packet sniffing
B. Authentication
C. Network binding
D. Encryption

Answer: A

QUESTION NO: 135

Which of the following statements about service pack are true?

Each correct answer represents a complete solution. Choose two.

A. It is a medium by which product updates are distributed.
B. It is a term used for securing an operating system.
C. It is a term generally related to security problems in a software.
D. It is a collection of Fixes and Patches in a single product.

Answer: A,D

QUESTION NO: 136

Fill in the blank with the appropriate value.

Primary Rate Interface (PRI) of an ISDN connection contains

_____B channels and _____D channel.

A. 23,1

Answer: A

QUESTION NO: 137

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He writes the following snort rule:

This rule can help him protect the We-are-secure server from the _____.

A. Chernobyl virus
B. I LOVE YOU virus
C. Melissa virus
D. Nimda virus

Answer: D

QUESTION NO: 138

Which of the following rate systems of Orange book has mandatory protection of the Trusted Computing Base (TCB)?

A. B-rated system
B. A-rated system
C. D-rated system
D. C-Rated system

Answer: A

QUESTION NO: 139

Which of the following rated systems of the Orange book has mandatory protection of the TCB?

A. B-rated
B. A-rated
C. D-rated
D. C-rated

Answer: A

QUESTION NO: 140

Which of the following standards is used in wireless local area networks (WLANs)?

A. IEEE 802.4
B. IEEE 802.11b

C. IEEE 802.5
D. IEEE 802.3

Answer: B

QUESTION NO: 141

Which of the following is an entry in an object's discretionary access control list (DACL) that grants permissions to a user or group?

A. Access control list (ACL)
B. Discretionary access control entry (DACE)
C. Security Identifier (SID)
D. Access control entry (ACE)

Answer: D

QUESTION NO: 142

Which of the following database types is a collection of tables that are linked by their primary keys?

A. Relational database management system
B. Object-oriented database management system
C. Hierarchical database management system
D. File-oriented database management system

Answer: A

QUESTION NO: 143

You work as a Network Administrator for NetTech Inc. The company's network has a Windows 2000 domain-based network. You want to prevent malicious e-mails from entering the network from the non-existing domains. What will you do to accomplish this?

A. Disable DNS recursive queries on the DNS server.
B. Enable DNS recursive queries on the DNS server.
C. Enable DNS reverse lookup on the e-mail server.

D. Disable DNS reverse lookup on the e-mail server.

Answer: C

QUESTION NO: 144

Which of the following is used to implement a procedure to control inbound and outbound traffic on a network?

A. Sam Spade
B. NIDS
C. ACL
D. Cookies

Answer: C

QUESTION NO: 145

Which of the following standards works at the *presentation layer*?

Each correct answer represents a complete solution. Choose all that apply.

A. ASCII
B. MPEG
C. TIFF
D. JPEG

Answer: A,B,C,D

QUESTION NO: 146

Which of the following statements about *Network Address Translation (NAT)* are true?

Each correct answer represents a complete solution. Choose two.

A. It allows the computers in a private network to share a global, ISP assigned address to connect to the Internet.
B. It reduces the need for globally unique IP addresses.
C. It allows external network clients access to internal services.

D. It provides added security by using Internet access to deny or permit certain traffic from the Bastion Host.

Answer: A,B

QUESTION NO: 147

Which of the following types of halon is found in portable extinguishers and is stored as a liquid?

A. Halon 11
B. Halon 1301
C. Halon 1211
D. Halon-f

Answer: C

QUESTION NO: 148

You work as a Network Administrator for NetTech Inc. To ensure the security of files, you encrypt data files using *Encrypting File System (EFS)*. You want to make a backup copy of the files and maintain security settings. You can backup the files either to a network share or a floppy disk. What will you do to accomplish this?

A. Copy the files to a network share on a FAT32 volume.
B. Copy the files to a network share on an NTFS volume.
C. Place the files in an encrypted folder. Then, copy the folder to a floppy disk.
D. Copy the files to a floppy disk that has been formatted using Windows 2000 Professional.

Answer: B

QUESTION NO: 149

You work as a Network Administrator for NetTech Inc. Your computer has the Windows 2000 Server operating system. You want to harden the security of the server. Which of the following changes are required to accomplish this?

Each correct answer represents a complete solution. Choose two.

A. Rename the Administrator account.

B. Remove the Administrator account.
C. Disable the Guest account.
D. Enable the Guest account.

Answer: A,C

Topic 2, Volume B

QUESTION NO: 150

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using the TFN and Trin00 tools to test the security of the We-aresecure server, so that he can check whether the server is vulnerable or not. Using these tools, which of the following attacks can John perform to test the security of the We-are- secure server?

A. Reply attack
B. Cross site scripting attack
C. DDoS attack
D. Brute force attack

Answer: C

QUESTION NO: 151

Which of the following statements about *IEEE 802.1X* standard are true?

Each correct answer represents a complete solution. Choose two.

A. It uses the Point-to-Point Tunneling Protocol (PPTP) that works on Ethernet, Token Ring, or wireless LANs to exchange messages for the authentication process.
B. It uses the Extensible Authentication Protocol (EAP) that works on Ethernet, Token Ring, or wireless LANs to exchange messages for the authentication process.
C. It provides an authentication framework for wireless LANs.
D. It provides the highest level of VPN security.

Answer: B,C

QUESTION NO: 152

Which of the following needs to be documented to preserve evidences for presentation in court?

A. Incident response policy
B. Separation of duties
C. Chain of custody
D. Account lockout policy

Answer: C

QUESTION NO: 153

Fill in the blank with the appropriate value.

SHA-1 produces a

_____-bit message digest.

A. 160

Answer: A

QUESTION NO: 154

Which of the following statements about *asymmetric encryption* are true?

Each correct answer represents a complete solution. Choose two.

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

Answer: A,C

QUESTION NO: 155

Which of the following refers to a computer that must be secure because it is accessible from the Internet and is vulnerable to attacks?

A. LMHOSTS
B. Bastion host
C. Firewall
D. Gateway

Answer: B

QUESTION NO: 156

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 cuts down dial-up charges.
C. It is used for automated assignment of IP addresses to a TCP/IP client in the domain.
D. It uses a single registered IP address for multiple connections to the Internet.

Answer: A,D

QUESTION NO: 157

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. Integrity
D. Confidentiality

Answer: B,C,D

QUESTION NO: 158

Which of the following services is provided by the *message authentication code (MAC)* ?

A. Data recovery
B. Integrity

C. Fault tolerance
D. Key recovery

Answer: B

QUESTION NO: 159

Which of the following statements best describes *VeriSign*?

A. It is a signature verification utility.
B. It is a certification authority.
C. It is an encryption technology.
D. It is an authentication server.

Answer: B

QUESTION NO: 160

Which of the following protocols is responsible for the resolution of IP addresses to media access control (MAC) addresses?

A. ARP
B. PPP
C. ICMP
D. HTTP

Answer: A

QUESTION NO: 161

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the preattack phase successfully:

•Information gathering

•Determination of network range

•Identification of active systems

•Location of open ports and applications

Now, which of the following tasks should he perform next?

A. Install a backdoor to log in remotely on the We-are-secure server.
B. Map the network of We-are-secure Inc.
C. Fingerprint the services running on the we-are-secure network.
D. Perform OS fingerprinting on the We-are-secure network.

Answer: D

QUESTION NO: 162

You work as a Network Administrator for NetTech Inc. Employees in remote locations connect to the company's network using Remote Access Service (RAS). Which of the following will you use to protect the network against unauthorized access?

A. Bridge
B. Antivirus software
C. Gateway
D. Firewall

Answer: D

QUESTION NO: 163

Which of the following statements about a *perimeter network* are true?

Each correct answer represents a complete solution. Choose three.

A. It has a connection to the Internet through an external firewall and a connection to an internal network through an interior firewall.
B. It has a connection to a private network through an external firewall and a connection to an internal network through an interior firewall.
C. It is also known as a demilitarized zone or DMZ.
D. It prevents access to the internal corporate network for outside users.

Answer: A,C,D

QUESTION NO: 164

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

A. Spam
B. Artistic license
C. Patent
D. Phishing

Answer: C

QUESTION NO: 165

You are using a Windows-based sniffer named ASniffer to record the data traffic of a network. You have extracted the following IP Header information of a randomly chosen packet from the sniffer's log:

45 00 00 28 00 00 40 00 29 06 43 CB D2 D3 82 5A 3B 5E AA 72

Which of the following TTL decimal values and protocols are being carried by the IP Header of this packet?

A. 16, ICMP
B. 41, TCP
C. 16, UDP
D. 41, UDP

Answer: B

QUESTION NO: 166

Which of the following attacks is specially used for cracking a password?

A. DoS attack
B. PING attack
C. Dictionary attack
D. Vulnerability attack

Answer: C

QUESTION NO: 167

Peter works as a Network Administrator for Net World Inc. The company wants to allow remote users to connect and access its private network through a dial-up connection via the Internet. All the data will be sent across a public network. For security reasons, the management wants the data sent through the Internet to be encrypted. The company plans to use a Layer 2 Tunneling Protocol (L2TP) connection. Which communication protocol will Peter use to accomplish the task?

A. Microsoft Point-to-Point Encryption (MPPE)
B. Pretty Good Privacy (PGP)
C. Data Encryption Standard (DES)
D. IP Security (IPSec)

Answer: D

QUESTION NO: 168

In which of the following cryptographic attacking techniques does an attacker obtain encrypted messages that have been encrypted using the same encryption algorithm?

A. Ciphertext only attack
B. Chosen ciphertext attack
C. Known plaintext attack
D. Chosen plaintext attack

Answer: A

QUESTION NO: 169

Which of the following are based on malicious code?

Each correct answer represents a complete solution. Choose two.

A. Worm
B. Biometrics
C. Denial-of-Service (DoS)

D. Trojan horse

Answer: A,D

QUESTION NO: 170

Which of the following devices performs protocol and format translations?

A. Switch
B. Modem
C. Gateway
D. Repeater

Answer: C

QUESTION NO: 171

Which of the following processes is known as *Declassification*?

A. Verifying the identity of a person, network host, or system process.
B. Physically destroying the media and the information stored on it.
C. Assessing the risk involved in making a confidential document available to public.
D. Removing the content from the media so that it is difficult to restore.

Answer: C

QUESTION NO: 172

Which of the following components come under the *physical layer* of the OSI model?

Each correct answer represents a complete solution. Choose all that apply.

A. Wall jacks
B. Hubs
C. Switches
D. Fiber cabling
E. RJ-45 connectors

Answer: A,B,D,E

QUESTION NO: 173

Which of the following is ensured by the concept of availability in information system security?

A. Data modifications are not made by an unauthorized user or process.
B. The intentional or unintentional unauthorized disclosure of a message or important document contents is prevented.
C. The systems are up and running when they are needed.
D. Unauthorized modifications are not made by authorized users.

Answer: C

QUESTION NO: 174

Which of the following is an authentication protocol?

A. LDAP
B. PPTP
C. TLS
D. Kerberos

Answer: D

QUESTION NO: 175

Which of the following security models dictates that subjects can only access objects through applications?

A. Biba-Clark model
B. Bell-LaPadula
C. Biba model
D. Clark-Wilson

Answer: D

QUESTION NO: 176

Which of the following protocols work at the *Application layer* of an OSI model?

Each correct answer represents a complete solution. Choose three.

A. Secure Hypertext Transfer Protocol (S-HTTP)
B. Address Resolution Protocol (ARP)
C. Post Office Protocol version 3 (POP3)
D. Trivial File Transfer Protocol (TFTP)

Answer: A,C,D

QUESTION NO: 177

Which of the following statements about *system hardening* are true?

Each correct answer represents a complete solution. Choose two.

A. It is used for securing the computer hardware.
B. It can be achieved by locking the computer room.
C. It is used for securing an operating system.
D. It can be achieved by installing service packs and security updates on a regular basis.

Answer: C,D

QUESTION NO: 178

Which of the following are considered *Bluetooth* security violations?

Each correct answer represents a complete solution. Choose two.

A. Social engineering
B. Bluesnarfing
C. SQL injection attack
D. Bluebug attack
E. Cross site scripting attack

Answer: B,D

QUESTION NO: 179

Which of the following are intrusion detection device?

A. Fingerprint reader
B. Smart card reader
C. Retinal scanner
D. CCTV

Answer: D

QUESTION NO: 180

Which of the following statements about *biometric* authentication is true?

A. A user provides his user name and password for authentication.
B. A user uses a smart card for authentication.
C. A sensor scans some physical characteristics of a user and sends that information to the authentication server.
D. A user is issued a device that is used for authentication.

Answer: C

QUESTION NO: 181

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

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

Answer: A,B

QUESTION NO: 182

Which of the following protocols are used to provide secure communication between a client and a server over the Internet?

Each correct answer represents a part of the solution. Choose two.

A. HTTP
B. SSL
C. SNMP
D. TLS

Answer: B,D

QUESTION NO: 183

Which of the following statements are true about worms?

Each correct answer represents a complete solution. Choose all that apply.

A. Worms can exist inside files such as Word or Excel documents.
B. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
C. One feature of worms is keystroke logging.
D. Worms replicate themselves from one system to another without using a host file.

Answer: A,B,D

QUESTION NO: 184

Which of the following types of evidence is considered as the best evidence?

A. A copy of the original document
B. A computer-generated record
C. Information gathered through the witness's senses
D. The original document

Answer: D

QUESTION NO: 185

You work as a Network Administrator for Rick International. The company has a TCP/IP-based network. A user named Kevin wants to set an *SSH* terminal at home to connect to the company's network. You have to configure your company's router for it. By default, which of the following

standard ports does the SSH protocol use for connection?

A. 21
B. 443
C. 80
D. 22

Answer: D

QUESTION NO: 186

Which of the following IP addresses are *private addresses*?

Each correct answer represents a complete solution. Choose all that apply.

A. 10.0.0.3
B. 192.168.15.2
C. 192.166.54.32
D. 19.3.22.17

Answer: A,B

QUESTION NO: 187

What is the hash value length of the Secure Hash Algorithm (SHA-1)?

A. 164-bit
B. 320-bit
C. 128-bit
D. 160-bit

Answer: D

QUESTION NO: 188

Which of the following viruses masks itself from applications or utilities to hide itself by detection of anti-virus software?

A. Macro virus
B. E-mail virus
C. Stealth virus
D. Polymorphic virus

Answer: C

QUESTION NO: 189

You work as a Network Administrator for Net Perfect Inc. The company has a Windows 2000, TCP/IP-based class C network consisting of 200 hosts. The network uses private IP addressing. A computer on the network is connected to the Internet. The management plans to increase the number of hosts to 300. The management also wants all hosts to be able to access the Internet through the existing connection. Which of the following steps will you take to accomplish this?

Each correct answer represents a part of the solution. Choose two.

A. Implement NAT.
B. Upgrade your class C network to a class B network.
C. Add a router to your network.
D. Add a bridge to your network.
E. Apply for more IP addresses for your LAN.

Answer: A,B

QUESTION NO: 190

Which of the following statements about *RSA algorithm* are true?

Each correct answer represents a complete solution. Choose two.

A. It is a block cipher in which plain text and cipher text are integers between 0 and n-1.
B. It is a stream cipher in which plain text and cipher text are integers between 0 and n-1.
C. It is an asymmetric algorithm.
D. It is a symmetric algorithm.

Answer: A,C

QUESTION NO: 191

Which of the following terms refers to the process in which headers and trailers are added around user data?

A. Encryption
B. Encapsulation
C. Authentication
D. Authorization

Answer: B

QUESTION NO: 192

Fill in the blank with the appropriate value.

International Data Encryption Algorithm (IDEA) operates on 64-bit blocks using a _____-bit key.

A. 128

Answer: A

QUESTION NO: 193

Which of the following are types of *social engineering* attacks?

Each correct answer represents a complete solution. Choose two.

A. An unauthorized person gains entrance to the building where the company's database server resides and accesses the server by pretending to be an employee.
B. An unauthorized person inserts an intermediary software or program between two communicating hosts to listen to and modify the communication packets passing between the two hosts.
C. An unauthorized person calls a user and pretends to be a system administrator in order to get the user's password.
D. An unauthorized person modifies packet headers by using someone else's IP address to hide his identity.

Answer: A,C

QUESTION NO: 194

Which of the following is the default port for *TACACS*?

A. UDP port 49
B. TCP port 443
C. TCP port 25
D. TCP port 80

Answer: A

QUESTION NO: 195

Which of the following is generally practiced by the police or any other recognized governmental authority?

A. SMB signing
B. Phishing
C. Spoofing
D. Wiretapping

Answer: D

QUESTION NO: 196

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

A. Chain of custody
B. Evidence access policy
C. Chain of evidence
D. Incident response policy

Answer: A

QUESTION NO: 197

Which of the following are the primary components of a *discretionary access control (DAC)* model?

Each correct answer represents a complete solution. Choose two.

A. User's group
B. Access rights and permissions
C. File and data ownership
D. Smart card

Answer: B,C

QUESTION NO: 198

Which of the following ensures that a sender cannot deny sending a message?

A. Authentication
B. Snooping
C. Spoofing
D. Non repudiation

Answer: D

QUESTION NO: 199

Which of the following protocols work at the network layer?

Each correct answer represents a complete solution. Choose three.

A. OSPF
B. SPX
C. IGMP
D. RIP

Answer: A,C,D

QUESTION NO: 200

Which of the following is executed when a predetermined event occurs?

A. Worm
B. Trojan horse
C. Logic bomb
D. MAC

Answer: C

QUESTION NO: 201

Which of the following types of computers is used for attracting potential intruders?

A. Honey pot
B. Bastion host
C. Data pot
D. Files pot

Answer: A

QUESTION NO: 202

You work as a Network Administrator for Infonet Inc. The company uses *Wired Equivalent Privacy (WEP)* for wireless security. Who among the following can authenticate from the access point of the network?

A. Only users within the company.
B. Anyone can authenticate.
C. Only users with the correct WEP key.
D. Only the administrator.

Answer: C

QUESTION NO: 203

Which of the following terms is used for the process of securing a system or a device on a network infrastructure?

A. Sanitization
B. Cryptography

C. Hardening
D. Authentication

Answer: C

QUESTION NO: 204

Which of the following statements about *Dynamic Host Configuration Protocol (DHCP)* are true?

Each correct answer represents a complete solution. Choose two.

A. It is used to provide host name resolution in a TCP/IP-based network.
B. It is used to dynamically assign IP addresses to computers.
C. It reduces the complexity of managing network client IP address configuration.
D. It reduces the risk of a denial of service (DoS) attack.

Answer: B,C

QUESTION NO: 205

Which of the following two components does Kerberos *Key Distribution Center (KDC)* consist of?

Each correct answer represents a complete solution. Choose two.

A. Data service
B. Account service
C. Ticket-granting service
D. Authentication service

Answer: C,D

QUESTION NO: 206

Which of the following is used for *secure financial transactions* over the Internet?

A. VPN
B. ATM
C. SSL
D. SET

Answer: D

QUESTION NO: 207

Which of the following encryption algorithms are based on stream ciphers?

Each correct answer represents a complete solution. Choose two.

A. RC4
B. FISH
C. Blowfish
D. Twofish

Answer: A,B

QUESTION NO: 208

Which of the following is the most secure policy for a *firewall*?

A. Passing all packets unless they are explicitly rejected.
B. Enabling all internal interfaces.
C. Blocking all packets unless they are explicitly permitted.
D. Disabling all external interfaces.

Answer: C

QUESTION NO: 209

Which of the following is an attack with IP fragments that cannot be reassembled?

A. Teardrop attack
B. Dictionary attack
C. Password guessing attack
D. Smurf attack

Answer: A

QUESTION NO: 210

You work as a Web Developer for WebCrunch Inc. You create a web site that contains information about the company's products and services. The web site is to be used by the company's suppliers only. Which of the following options will you use to specify the nature of access to the web site?

A. Intranet
B. Internet and Intranet
C. Internet
D. Extranet

Answer: D

QUESTION NO: 211

Which of the following statements about *buffer overflow* are true?

Each correct answer represents a complete solution. Choose two.

A. It is a situation that occurs when a storage device runs out of space.
B. It can terminate an application.
C. It can improve application performance.
D. It is a situation that occurs when an application receives more data than it is configured to accept

Answer: B,D

QUESTION NO: 212

Which of the following ports is used by a *BOOTP* server?

A. UDP port 389
B. UDP port 67
C. TCP port 80
D. TCP port 110

Answer: B

QUESTION NO: 213

Which of the following protocols uses TCP port 22 as the default port and operates at the application layer?

A. Secure Sockets Layer (SSL)
B. Secure Shell (SSH)
C. Post Office Protocol version 3 (POP3)
D. Trivial File Transfer Protocol (TFTP)

Answer: B

QUESTION NO: 214

Which of the following protocols multicasts messages and information among all member devices in an IP multicast group?

A. ARP
B. TCP
C. ICMP
D. IGMP

Answer: D

QUESTION NO: 215

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

A. EAP
B. CHAP
C. MS-CHAP v2
D. PAP

Answer: A

QUESTION NO: 216

Which of the following performs packet screening for security on the basis of port numbers?

A. Switch
B. DNS
C. Hub
D. Firewall

Answer: D

QUESTION NO: 217

Which of the following are man-made threats that an organization faces?

Each correct answer represents a complete solution. Choose three.

A. Frauds
B. Strikes
C. Employee errors
D. Theft

Answer: A,C,D

QUESTION NO: 218

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

Each correct answer represents a complete solution. Choose all that apply.

A. Dig
B. NSLookup
C. DSniff
D. Host

Answer: A,B,D

QUESTION NO: 219

Which of the following security models deal only with integrity?

Each correct answer represents a complete solution. Choose two.

A. Biba
B. Bell-LaPadula
C. Biba-Wilson
D. Clark-Wilson

Answer: A,D

QUESTION NO: 220

In which of the following IDS evasion attacks does an attacker send a data packet such that IDS accepts the data packet but the host computer rejects it?

A. Fragmentation overlap attack
B. Evasion attack
C. Fragmentation overwrite attack
D. Insertion attack

Answer: D

QUESTION NO: 221

Which of the following services does Internet Information Server (IIS) provide along with HTTP?

Each correct answer represents a complete solution. Choose three.

A. SMTP
B. FTP
C.PPTP
D.NNTP

Answer: A,B,D

QUESTION NO: 222

Which of the following are the responsibilities of a custodian with regard to data in an information classification program?

Each correct answer represents a complete solution. Choose three.

A. Running regular backups and routinely testing the validity of the backup data
B. Performing data restoration from the backups when necessary
C. Controlling access, adding and removing privileges for individual users
D. Determining what level of classification the information requires

Answer: A,B,C

QUESTION NO: 223

Which of the following statements about Microsoft *hotfix* are true?

Each correct answer represents a complete solution. Choose two.

A. It is the term used by Microsoft for major service pack releases.
B. It is generally related to security problems.
C. It is a collection of files used by Microsoft for software updates released between major service pack releases.
D. It is generally related to the problems of a Web server's performance.

Answer: B,C

QUESTION NO: 224

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He notices that UDP port 137 of the We-are-secure server is open. Assuming that the Network Administrator of We-are-secure Inc. has not changed the default port values of the services, which of the following services is running on UDP port 137?

A. HTTPS
B. HTTP
C. TELNET

D. NetBIOS

Answer: D

QUESTION NO: 225

Which of the following tools is used for breaking digital watermark?

A. TRACERT
B. Trin00
C. Fpipe
D. 2Mosaic

Answer: D

QUESTION NO: 226

Which of the following are used to suppress electrical and computer fires?

Each correct answer represents a complete solution. Choose two.

A. Halon
B. Soda acid
C. CO2
D. Water

Answer: A,C

QUESTION NO: 227

Which of the following are the major tasks of risk management?

Each correct answer represents a complete solution. Choose two.

A. Building Risk free systems
B. Assuring the integrity of organizational data
C. Risk control
D. Risk identification

Answer: C,D

QUESTION NO: 228

Which of the following records is the first entry in a DNS database file?

A. SRV
B. CNAME
C. MX
D. SOA

Answer: D

QUESTION NO: 229

Which of the following groups represents the most likely source of an asset loss through the inappropriate use of computers?

A. Employees
B. Hackers
C. Visitors
D. Customers

Answer: A

QUESTION NO: 230

Which of the following types of coaxial cable is used for cable TV and cable modems?

A. RG-62
B. RG-59
C. RG-8
D. RG-58

Answer: B

QUESTION NO: 231

Which of the following is the process of finding weaknesses in cryptographic algorithms and obtaining the plaintext or key from the ciphertext?

A. Cryptanalysis
B. Kerberos
C. Cryptographer
D. Cryptography

Answer: A

QUESTION NO: 232

Which of the following is used by the *Diffie-Hellman encryption* algorithm?

A. Password
B. Access control entry
C. Key exchange
D. Access control list

Answer: C

QUESTION NO: 233

Which of the following provides secure online payment services?

A. CA
B. IEEE
C. ACH
D. ICSA

Answer: C

QUESTION NO: 234

John works as an Ethical Hacker for PassGuide Inc. He wants to find out the ports that are open in PassGuide's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP SYN
B. TCP SYN/ACK
C. TCP FIN
D. Xmas tree

Answer: A

QUESTION NO: 235

Which of the following statements about the Instant messaging programs are true?

Each correct answer represents a complete solution. Choose all that apply.

A. Most of the programs have no encryption facility.
B. They allow effective and efficient communication and immediate receipt of reply.
C. They provide secure password management.
D. They can bypass corporate firewalls.

Answer: A,B,D

QUESTION NO: 236

Which of the following tools is used to flood the local network with random MAC addresses?

A. NETSH
B. NMAP
C. Port scanner
D. Macof

Answer: D

QUESTION NO: 237

Mark works as a Webmaster for Infonet Inc. He sets up an e-commerce site. He wants to accept online payments through credit cards on this site. He wants the credit card numbers to be encrypted. What will Mark do to accomplish the task?

To Read the **Whole Q&As**, please purchase the **Complete Version** from **Our website**.

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

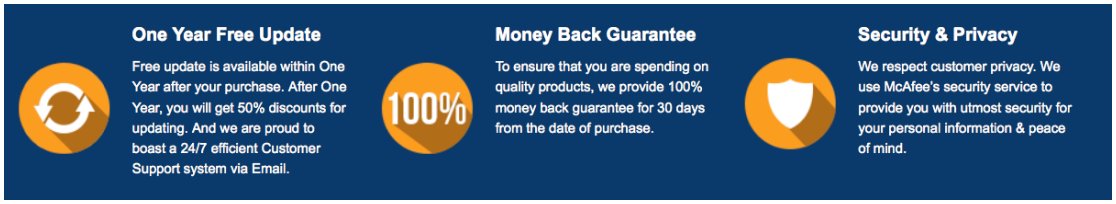
★ Average **99.9%** Success Rate

★ 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

Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.

Copyright © 2004-2015, All Rights Reserved.