Question #1 *Topic 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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Which of the following refers to encrypted text?

A. Plaintext

B. Cookies

C. Hypertext

D. Ciphertext

Suggested Answer: *D*

DrChats 4 years, 6 months ago

D is right

upvoted 1 times

Question #3 *Topic 1*

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).

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

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

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

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

A. CEP

B. HTTP

C. OSPF

D. OCSP

Suggested Answer: *D*

martino88 2 years, 11 months ago

OCSP (Online Certificate Status Protocol) is one of two common schemes used to maintain the security of a server and other network resources. An older method, which OCSP has superseded in some scenarios, is known as a certificate revocation list (CRL).

upvoted 1 times

Question #7 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate value.

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

Suggested Answer: *32*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 1*

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.

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

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.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 1*

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.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 1*

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.

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

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).

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

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

A. SSL

B. PGP

C. IPSEC

D. SSH

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

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

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

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.

Suggested Answer: *A*

sergio_sark 3 years, 4 months ago

It is not possible to visualize the beginning of the question

upvoted 1 times

Question #22 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

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

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

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

A. Auditing

B. Recovery

C. Confidentiality

D. Integrity

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

?

A. PPP

B. SNMP

C. UDP

D. SLIP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

?

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.

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

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.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

Which of the following is the most secure authentication method?

A. Certificate-based authentication

B. Basic authentication

C. Digest authentication

D. Integrated Windows authentication

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

stand for?

A. Rivest-Shamir-Adleman

B. Read System Authority

C. Rivest-System-Adleman

D. Remote System Authority

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

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

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

SIMULATION -

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.

Suggested Answer: *Internet*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

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)

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 1*

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 SYCK

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 1*

components?

Each correct answer represents a complete solution. Choose three.

A. Switches

B. Bridges

C. MAC addresses

D. Hub

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 1*

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.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 1*

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.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 1*

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

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 1*

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

Suggested Answer: *C*
The Firewall mechanism of operation is inspecting and filtering packets by policy.

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 1*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate term.

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

Suggested Answer: *certificate*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 1*

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

A. PGP

B. CGI

C. IETF

D. Firewall

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 1*

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

A. The 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.

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 1*

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

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 1*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 1*

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.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 1*

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
. 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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 1*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 1*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 1*

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

I dentifying 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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 1*

Which of the following are tunneling protocols?
Each correct answer represents a complete solution. Choose two.

A. NNTP

B. SMTP

C. L2TP

D. PPTP

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 1*

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 1*

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.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 1*

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 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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 1*

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 1*

SUMULATION -

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.

Suggested Answer: *transport*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 1*

Which of the following is a source port forwarder and redirector tool?

A. Fpipe

B. NMAP

C. SuperScan

D. NSLOOKUP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 1*

on client computers?
Each correct answer represents a complete solution. Choose two.

A. Perl

B. DHTML

C. JavaScript

D. HTML

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 1*

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.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 1*

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

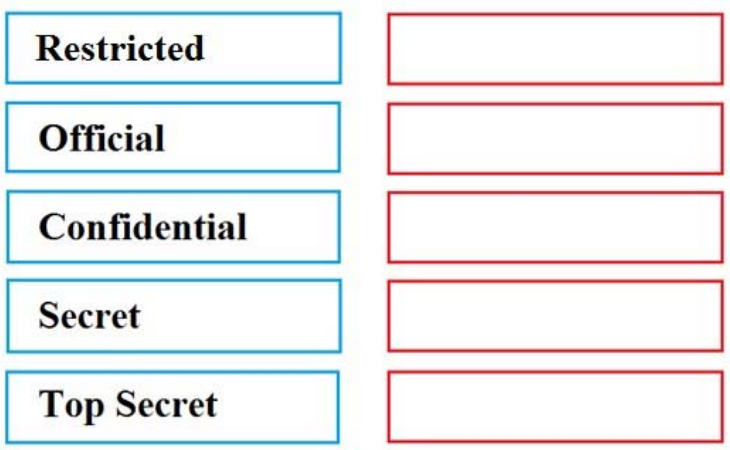
Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 1*

.

Select and Place:



Suggested Answer:

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 1*

?

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 1*

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

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 1*

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

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 1*

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

A. TrueCrypt

B. Fragroute

C. Mendax

D. ADMutate

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 1*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 1*

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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #95 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 1*

provide protection?
Each correct answer represents a complete solution. Choose two.

A. DoS attack

B. Password sniffing

C. Broadcast storm

D. IP spoofing

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He 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:
⇨ It creates a virtual encrypted disk within a file and mounts it as a real disk.
⇨ It provides the following encryption algorithms:
⇨ AES-256
⇨ Serpent
⇨ Twofish

Mode of operation: XTS -
⇨ It can also encrypt a partition or drive where an operations system is installed.
⇨ It provides two levels of plausible deniability in case an enemy forces it to reveal the password:
⇨ Hidden volume and hidden operating system
⇨ 2nd layer of encryption for sensitive contents.
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

Suggested Answer: *C*
authorities as given below:

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 1*

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 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)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 1*

SIMULATION -

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.

Suggested Answer: *5.5*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #105 *Topic 1*

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.

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 1*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #107 *Topic 1*

Which of the following are the examples of administrative controls?
Each correct answer represents a complete solution. Choose all that apply.

A. Data Backup

B. Auditing

C. Security policy

D. Security awareness training

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 1*

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

A. Sanitization

B. Authentication

C. Spoofing

D. Drive wiping

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 1*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 1*

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

A. PAP

B. MS-CHAP

C. CHAP

D. MS-CHAP v2

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 1*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 1*

of the OSI model?
Each correct answer represents a complete solution. Choose two.

A. Firewalls

B. Hub

C. Routers

D. MAC addresses

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #113 *Topic 1*

?

A. TCP port 22

B. UDP port 161

C. UDP port 138

D. TCP port 443

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 1*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #116 *Topic 1*

half open?

A. Spoofing

B. PING attack

C. SYN attack

D. Hacking

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #117 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #118 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #119 *Topic 1*

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

A. Physical

B. Network

C. Transport

D. Session

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #120 *Topic 1*

resolution problem. Which of the following utilities will you use to diagnose the problem?

A. NSLOOKUP

B. IPCONFIG

C. PING

D. TRACERT

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #121 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #122 *Topic 1*

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

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 1*

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

A. RC4

B. RC5

C. Twofish

D. Rijndael

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #124 *Topic 1*

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.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #125 *Topic 1*

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.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #126 *Topic 1*

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
. 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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #127 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #128 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #129 *Topic 1*

provide in an e-commerce system?
Each correct answer represents a complete solution. Choose two.

A. Credit

B. Trust

C. Transparency

D. Identification

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #130 *Topic 1*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #131 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #132 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #133 *Topic 1*

?

A. UDP port 1701

B. UDP port 161

C. TCP port 443

D. TCP port 110

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #134 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #135 *Topic 1*

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.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #136 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate value.

Primary Rate Interface (PRI) of an ISDN connection contains _____ B channels and _____ D channel.

Suggested Answer: *23,1*

Currently there are no comments in this discussion, be the first to comment!

Question #137 *Topic 1*

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:

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-IIS cmd.exe access"; flow:to_server,established;
content:"cmd.exe"; nocase; classtype:web-application-attack;
sid:1002; rev:6;)
```

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #138 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #139 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #140 *Topic 1*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #141 *Topic 1*

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)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #142 *Topic 1*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #143 *Topic 1*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #144 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #145 *Topic 1*

?

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

A. ASCII

B. MPEG

C. TIFF

D. JPEG

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #146 *Topic 1*

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.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #147 *Topic 1*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #148 *Topic 1*

. 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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #149 *Topic 1*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 2*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 2*

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 2*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate value.

SHA-1 produces a _____ -bit message digest.

Suggested Answer: *160*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 2*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 2*

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.

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 2*

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

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 2*

?

A. Data recovery

B. Integrity

C. Fault tolerance

D. Key recovery

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 2*

?

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.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 2*

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.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 2*

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.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 2*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 2*

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

A. DoS attack

B. PING attack

C. Dictionary attack

D. Vulnerability attack

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 2*

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)

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 2*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 2*

Which of the following devices performs protocol and format translations?

A. Switch

B. Modem

C. Gateway

D. Repeater

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 2*

?

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 2*

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

Suggested Answer: *ABDE*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 2*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 2*

Which of the following is an authentication protocol?

A. LDAP

B. PPTP

C. TLS

D. Kerberos

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 2*

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)

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 2*

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.

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 2*

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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 2*

Which of the following are intrusion detection device?

A. Fingerprint reader

B. Smart card reader

C. Retinal scanner

D. CCTV

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 2*

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 2*

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)

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 2*

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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 2*

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.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #36 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #37 *Topic 2*

?

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

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #38 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #39 *Topic 2*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #40 *Topic 2*

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.

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #41 *Topic 2*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #42 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #43 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate value.

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

Suggested Answer: *128*

Currently there are no comments in this discussion, be the first to comment!

Question #44 *Topic 2*

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.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #45 *Topic 2*

?

A. UDP port 49

B. TCP port 443

C. TCP port 25

D. TCP port 80

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #46 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #47 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #48 *Topic 2*

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

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #49 *Topic 2*

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

A. Authentication

B. Snooping

C. Spoofing

D. Non repudiation

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #50 *Topic 2*

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

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #51 *Topic 2*

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

A. Worm

B. Trojan horse

C. Logic bomb

D. MAC

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #52 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #53 *Topic 2*

for wireless security. Who among the following can
network?

A. Only users within the company.

B. Anyone can authenticate.

C. Only users with the correct WEP key.

D. Only the administrator.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #54 *Topic 2*

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

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #55 *Topic 2*

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #56 *Topic 2*

consist of?
Each correct answer represents a complete solution. Choose two.

A. Data service

B. Account service

C. Ticket-granting service

D. Authentication service

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #57 *Topic 2*

over the Internet?

A. VPN

B. ATM

C. SSL

D. SET

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #58 *Topic 2*

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

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #59 *Topic 2*

?

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.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #60 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #61 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #62 *Topic 2*

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

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #63 *Topic 2*

server?

A. UDP port 389

B. UDP port 67

C. TCP port 80

D. TCP port 110

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #64 *Topic 2*

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)

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #65 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #66 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #67 *Topic 2*

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

A. Switch

B. DNS

C. Hub

D. Firewall

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #68 *Topic 2*

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

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #69 *Topic 2*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #70 *Topic 2*

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

Suggested Answer: *AD*

Currently there are no comments in this discussion, be the first to comment!

Question #71 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #72 *Topic 2*

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

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #73 *Topic 2*

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

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #74 *Topic 2*

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.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #75 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #76 *Topic 2*

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

A. TRACERT

B. Trin00

C. Fpipe

D. 2Mosaic

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #77 *Topic 2*

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

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #78 *Topic 2*

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

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #79 *Topic 2*

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

A. SRV

B. CNAME

C. MX

D. SOA

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #80 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #81 *Topic 2*

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

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #82 *Topic 2*

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

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #83 *Topic 2*

algorithm?

A. Password

B. Access control entry

C. Key exchange

D. Access control list

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #84 *Topic 2*

Which of the following provides secure online payment services?

A. CA

B. IEEE

C. ACH

D. ICSA

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #85 *Topic 2*

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 SYCK

C. TCP FIN

D. Xmas tree

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #86 *Topic 2*

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.

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #87 *Topic 2*

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

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #88 *Topic 2*

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?

A. Use PGP.

B. Use HTTP.

C. Use MIME.

D. Use SET.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #89 *Topic 2*

Which of the following layers protocols handles file transfer and network management?

A. Application

B. Transport

C. Presentation

D. Session

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #90 *Topic 2*

SIMULATION -

Fill in the blank with the appropriate value.

Twofish symmetric key block cipher operates on 128-bits block size using key sizes up to_____ bits.

Suggested Answer: *256*

Currently there are no comments in this discussion, be the first to comment!

Question #91 *Topic 2*

Which of the following protects from electrical and magnetic induction that causes interference to the power voltage?

A. Power regulator

B. Shielded line

C. Firewall

D. Smoke detector

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #92 *Topic 2*

Which of the following features of a switch helps to protect network from MAC flood and MAC spoofing?

A. Port security

B. Multi-Authentication

C. Quality of Service (QoS)

D. MAC Authentication Bypass

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #93 *Topic 2*

Which of the following are the common roles with regard to data in an information classification program?
Each correct answer represents a complete solution. Choose all that apply.

A. User

B. Owner

C. Custodian

D. Security auditor

E. Editor

Suggested Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Question #94 *Topic 2*

are true?

Each correct answer represents a complete solution. Choose two.

A. It uses symmetric key pairs.

B. It uses asymmetric key pairs.

C. It provides security using data encryption and digital signature.

D. It is a digital representation of information that identifies users.

Suggested Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Question #95 *Topic 2*

In which of the following does a Web site store information such as user preferences to provide customized services to users?

A. ActiveX control

B. Keyword

C. Protocol

D. Cookie

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #96 *Topic 2*

Which of the following classes of IP addresses allows a maximum of 2,097,152 networks?

A. Class C

B. Class B

C. Class D

D. Class A

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #97 *Topic 2*

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company.
To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Email spoofing

B. Social engineering

C. Web ripping

D. Steganography

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #98 *Topic 2*

Which of the following is a program that monitors data packets traveling across a network?

A. Sniffer

B. Smurf

C. Hacker

D. BitLocker

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #99 *Topic 2*

At which of the following layers of the Open System Interconnection (OSI) model the Internet Control Message Protocol (ICMP) and the Internet Group
Management Protocol (IGMP) work?

A. The Physical layer

B. The Network layer

C. The Data-Link layer

D. The Presentation layer

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #100 *Topic 2*

You work as a Network Administrator for Net Soft Inc. You are designing a data backup plan for your company's network. The backup policy of the company requires high security and easy recovery of data. Which of the following options will you choose to accomplish this?

A. Take a full backup daily and use six-tape rotation.

B. Take a full backup on Monday and an incremental backup on each of the following weekdays. Keep Monday's backup offsite.

C. Take a full backup on Monday and a differential backup on each of the following weekdays. Keep Monday's backup offsite.

D. Take a full backup daily with the previous night's tape taken offsite.

E. Take a full backup daily with one tape taken offsite weekly.

F. Take a full backup on alternate days and keep rotating the tapes.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #101 *Topic 2*

Which of the following ports is used by a BOOTP client?

A. UDP port 67

B. UDP port 53

C. UDP port 69

D. UDP port 68

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #102 *Topic 2*

You work as a Network Administrator for NetTech Inc. The company's network is connected to the Internet.
For security, you want to restrict unauthorized access to the network with minimum administrative effort.
You want to implement a hardware-based solution. What will you do to accomplish this?

A. Connect a brouter to the network.

B. Implement firewall on the network.

C. Connect a router to the network.

D. Implement a proxy server on the network.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #103 *Topic 2*

Which of the following conditions the line to keep voltage steady and clean?

A. Power regulator

B. Demilitarized zone (DMZ)

C. Transponder

D. Smoke detector

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #104 *Topic 2*

Which of the following refers to a condition in which a computer repeatedly sends ICMP echo requests to another host?

A. Broadcast storm

B. SYN attack

C. Spoofing

D. PING attack

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #105 *Topic 2*

A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing?
Each correct answer represents a complete solution. Choose all that apply.

A. ToneLoc

B. THC-Scan

C. Wingate

D. NetStumbler

Suggested Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #106 *Topic 2*

fire?

A. Combustible metals fire

B. Paper or wood fire

C. Oil fire

D. Electronic or computer fire

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #107 *Topic 2*

cables?

A. Light

B. Infrared

C. Electrical current

D. Radio wave

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #108 *Topic 2*

operate?

A. Data-link layer

B. Physical layer

C. Session layer

D. Network layer

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #109 *Topic 2*

Which of the following concepts represent the three fundamental principles of information security?
Each correct answer represents a complete solution. Choose three.

A. Integrity

B. Privacy

C. Confidentiality

D. Availability

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #110 *Topic 2*

John works as a contract Ethical Hacker. He has recently got a project to do security checking for www.we-are-secure.com. He wants to find out the operating system of the we-are-secure server in the information gathering step. Which of the following commands will he use to accomplish the task?
Each correct answer represents a complete solution. Choose two.

A. nc 208.100.2.25 23

B. nc -v -n 208.100.2.25 80

C. nmap -v -O 208.100.2.25

D. nmap -v -O www.we-are-secure.com

Suggested Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Question #111 *Topic 2*

?

A. PPP

B. L2TP

C. PPTP

D. SLIP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #112 *Topic 2*

Which of the following provides high availability of data?

A. RAID

B. Anti-virus software

C. Backup

D. EFS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #113 *Topic 2*

session keys are available in which of the following lengths?

A. 64-bit and 128-bit.

B. 40-bit and 64-bit.

C. 128-bit and 1,024-bit.

D. 40-bit and 128-bit.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #114 *Topic 2*

Which of the following protocols is used to provide security for wireless local area networks (WLANs)?

A. WEP

B. EAP

C. NAT

D. TLS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #115 *Topic 2*

plan for
it. Client computers with different operating systems will access the Web server. How will you configure the Web server so that it is secure and only authenticated users are able to access it?
Each correct answer represents a part of the solution. Choose two.

A. Use the EAP protocol.

B. Use the SSL protocol.

C. Use Basic authentication.

D. Use encrypted authentication.

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #116 *Topic 2*

are true?
Each correct answer represents a complete solution. Choose two.

A. It is used to securely store public and private keys for log on , e-mail signing and encryption, and file encryption.

B. It is a device that routes data packets between computers in different networks.

C. It is a device that contains a microprocessor and permanent memory.

D. It is a device that works as an interface between a computer and a network.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #117 *Topic 2*

In which of the following security tests does the security testing team simulate as an employee or other person with an authorized connection to the organization's network?

A. Remote dial-up network

B. Remote network

C. Stolen equipment

D. Local network

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #118 *Topic 2*

Which of the following types of activities can be audited for security?
Each correct answer represents a complete solution. Choose three.

A. Data downloading from the Internet

B. File and object access

C. Network logons and logoffs

D. Printer access

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #119 *Topic 2*

are true?
Each correct answer represents a complete solution. Choose three.

A. It typically executes at a higher speed than a block cipher.

B. It typically executes at a slower speed than a block cipher.

C. It divides a message into blocks for processing.

D. It divides a message into bits for processing.

E. It is a symmetric key cipher.

Suggested Answer: *ADE*

Currently there are no comments in this discussion, be the first to comment!

Question #120 *Topic 2*

?

Each correct answer represents a complete solution. Choose three.

A. Identifying the risk

B. Assessing the impact of potential threats

C. Finding an economic balance between the impact of the risk and the cost of the countermeasure

D. Identifying the accused

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #121 *Topic 2*

?

Each correct answer represents a complete solution. Choose three.

A. Authentication

B. Data encryption

C. Authorization

D. Accounting

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #122 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He copies the whole structure of the
We-are-secure Web site to the local disk and obtains all the files on the Web site. Which of the following techniques is he using to accomplish his task?

A. TCP FTP proxy scanning

B. Eavesdropping

C. Web ripping

D. Fingerprinting

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #123 *Topic 2*

Which of the following is required to be backed up on a domain controller to recover Active Directory?

A. Installed third party application's folders

B. User's personal data

C. Operating System files

D. System state data

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #124 *Topic 2*

SIMULATION -

Fill in the blanks with the appropriate values.

International Data Encryption Algorithm (IDEA) is a _____ -bit block cipher that uses a _____-bit key.

Suggested Answer: *64,128*

Currently there are no comments in this discussion, be the first to comment!

Question #125 *Topic 2*

threat?

Each correct answer represents a complete solution. Choose three.

A. Password policies

B. Vulnerability assessments

C. Data classification

D. Data encryption

Suggested Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Question #126 *Topic 2*

Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

A. Packaging

B. Spoofing

C. Eavesdropping

D. Shielding

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #127 *Topic 2*

.

Which of the following will you use to accomplish this?

A. IPSec

B. PGP

C. PPTP

D. NTFS

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #128 *Topic 2*

Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Denial-of-Service (DoS) attack

B. Impersonation attack

C. Vulnerability attack

D. Man-in-the-middle attack

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #129 *Topic 2*

You work in a company that accesses the Internet frequently. This makes the company's files susceptible to attacks from unauthorized access. You want to protect your company's network from external attacks. Which of the following options will help you in achieving your aim?

A. HTTP

B. FTP

C. Firewall

D. Gopher

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #130 *Topic 2*

Which of the following works at the network layer and hides the local area network IP address and topology?

A. Hub

B. MAC address

C. Network address translation (NAT)

D. Network interface card (NIC)

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #131 *Topic 2*

is true?

A. It is a computer that is used to resolve the NetBIOS name to an IP address.

B. It is a computer that is used to resolve the host name to an IP address.

C. It is a computer that is accessible from the Internet to collect information about internal networks.

D. It is a computer that must be made secure because it is accessible from the Internet and hence is more vulnerable to attacks.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #132 *Topic 2*

Which of the following is the main reason for implementing CCTV as part of the physical arrangement?

A. Authenticating users

B. Securing data

C. Increasing guard visibility

D. Preventing criminal activities

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #133 *Topic 2*

Which of the following is a reason to implement security logging on a DNS server?

A. For measuring a DNS server's performance

B. For recording the number of queries resolved

C. For preventing malware attacks on a DNS server

D. For monitoring unauthorized zone transfer

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #134 *Topic 2*

Which of the following occurs when a packet is sent from a source computer to a destination computer?

A. Broadcast transmission

B. Unicast transmission

C. Multicast transmission

D. Baseband transmission

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #135 *Topic 2*

You work as a Network Administrator for McRoberts Inc. The company has a TCP-based network, which is connected to the Internet. Users use their Web browsers to connect to Web servers and to view different Web pages. Which of the following protocols ensures a secure connection between a Web browser and a Web server?

A. L2TP

B. SSL

C. IPSec

D. PPTP

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #136 *Topic 2*

program execute?

A. Router

B. Client and Web server

C. Client

D. Web server

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #137 *Topic 2*

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

A. Packet sniffing

B. Packet filtering

C. Shielding

D. Password guessing

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #138 *Topic 2*

Which of the following is used to allow or deny access to network resources?

A. ACL

B. System hardening

C. Spoofing

D. NFS

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #139 *Topic 2*

Which of the following VPN protocols offer encryption?
Each correct answer represents a complete solution. Choose two.

A. L2F

B. PPTP

C. L2TP

D. IPSec

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #140 *Topic 2*

Which of the following is used by attackers to obtain an authenticated connection on a network?

A. Denial-of-Service (DoS) attack

B. Replay attack

C. Man-in-the-middle attack

D. Back door

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #141 *Topic 2*

Which of the following are politically motivated threats that an organization faces?
Each correct answer represents a complete solution. Choose all that apply.

A. Power distribution outages

B. Civil disobedience

C. Riot

D. Terrorist attacks

E. Vandalism

Suggested Answer: *BCDE*

Currently there are no comments in this discussion, be the first to comment!

Question #142 *Topic 2*

is true?

A. It hides the public network from internal hosts.

B. It hides internal hosts from the public network.

C. It uses public IP addresses on an internal network.

D. It translates IP addresses into user friendly names.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #143 *Topic 2*

Which of the following protocols provides maintenance and error reporting function?

A. ICMP

B. IGMP

C. PPP

D. UDP

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #1 *Topic 3*

?

A. It is used to track user accounts for file and object access, logon attempts, etc.

B. It is used to prevent unauthorized access to network resources.

C. It is used to protect the network against virus attacks.

D. It is used to secure the network or the computers on the network.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 3*

Which of the following statements about the integrity concept of information security management are true?
Each correct answer represents a complete solution. Choose three.

A. It determines the actions and behaviors of a single individual within a system

B. It ensures that unauthorized modifications are not made to data by authorized personnel or processes.

C. It ensures that modifications are not made to data by unauthorized personnel or processes.

D. It ensures that internal information is consistent among all subentities and also consistent with th real-world, external situation.

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 3*

Which of the following OSI model layers handles translation of data into standard format, data compression, and decompression?

A. Application

B. Physical

C. Presentation

D. Session

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 3*

fire?

A. Cooking oil fire

B. Electrical fire

C. Wooden fire

D. Combustible metal fire

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 3*

provides file-level security?

A. CDFS

B. FAT

C. NTFS

D. FAT32

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 3*

Which of the following is an open source network intrusion detection system?

A. Sourcefire

B. NETSH

C. Macof

D. Snort

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #7 *Topic 3*

?

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

A. Support for file and folder level permissions.

B. Support for dual-booting.

C. Support for Encrypting File System (EFS).

D. Support for audio files.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #8 *Topic 3*

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Patent

B. Snooping

C. Copyright

D. Utility model

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #9 *Topic 3*

Which of the following books deals with confidentiality?

A. Brown Book

B. Red Book

C. Purple Book

D. Orange Book

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 3*

Which of the following can provide security against man-in-the-middle attack?

A. Strong data encryption during travel

B. Strong authentication method

C. Firewall

D. Anti-virus programs

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 3*

Which of the following are the levels of military data classification system?
Each correct answer represents a complete solution. Choose all that apply.

A. Top Secret

B. Sensitive

C. Public

D. Unclassified

E. Secret

F. Confidential

Suggested Answer: *ABDEF*

Currently there are no comments in this discussion, be the first to comment!

Question #12 *Topic 3*

A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Privacy law

B. Trademark law

C. Security law

D. Copyright law

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 3*

Which of the following protects against unauthorized access to confidential information via encryption and works at the network layer?

A. IPSec

B. NAT

C. Firewall

D. MAC address

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 3*

Which of the following types of fiber optic cable is generally used in WANs and powered by laser light?

A. Multi-mode fiber

B. Single-mode fiber

C. Dual-mode fiber

D. Duplex-mode fiber

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #15 *Topic 3*

Which of the following protocols is used as the directory access protocol?

A. HDAP

B. NNTP

C. FTP

D. LDAP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #16 *Topic 3*

Which of the following command-line utilities queries the DNS server to check whether or not the zone database contains the correct information?

A. IPCONFIG

B. TELNET

C. NSLOOKUP

D. NETSTAT

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 3*

are true?
Each correct answer represents a complete solution. Choose two.

A. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site.

B. It uses TCP port 80 as the default port.

C. It uses TCP port 443 as the default port.

D. It is a protocol used to provide security for a database server in an internal network.

Suggested Answer: *AC*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 3*

Which of the following terms is synonymous with the willful destruction of another person's property?

A. Hacking

B. Vandalism

C. Spoofing

D. Phishing

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 3*

Which of the following protocols is used for sending e-mail messages between e-mail servers?

A. IGMP

B. SNMP

C. ICMP

D. SMTP

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 3*

Samantha works as an Ethical Hacker for we-are-secure Inc. She wants to test the security of the weare- secure server for DoS attacks. She sends large number of ICMP ECHO packets to the target computer. Which of the following DoS attacking techniques will she use to accomplish the task?

A. Land attack

B. Ping flood attack

C. Smurf dos attack

D. Teardrop attack

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 3*

Which of the following allows an administrator to find weak passwords on the network?

A. Rainbow table

B. Back door

C. Worm

D. Access control list

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 3*

Which of the following is the most common method used by attackers to identify wireless networks?

A. Back door

B. Packet filtering

C. Packet sniffing

D. War driving

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 3*

to notify the names of active directory elements?
Each correct answer represents a complete solution. Choose three.

A. DC

B. OU

C. FN

D. CN

Suggested Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 3*

Which of the following tools can be used by a user to hide his identity?
Each correct answer represents a complete solution. Choose all that apply.

A. War dialer

B. IPchains

C. Anonymizer

D. Proxy server

E. Rootkit

Suggested Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 3*

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

A. Corroborating

B. Circumstantial

C. Direct

D. Incontrovertible

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 3*

Which of the following statements about Network Address Translation (NAT) are true?
Each correct answer represents a complete solution. Choose three.

A. It hides the internal IP addressing scheme.

B. It protects network from the password guessing attacks.

C. It is used to connect private networks to the public Internet.

D. It shares public Internet addresses with a large number of internal network clients.

Suggested Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 3*

Which of the following handles a relatively wide range of frequencies, which may be divided into channels or frequency bins?

A. Broadband transmission

B. Multicast transmission

C. Baseband transmission

D. Unicast transmission

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 3*

Which of the following records everything a person types using the keyboard?

A. Line conditioner

B. Firewall

C. Port scanner

D. Keystroke logger

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 3*

Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Policy Access Control

B. Mandatory Access Control

C. Role-Based Access Control

D. Discretionary Access Control

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 3*

Which of the following terms refers to a momentary low voltage?

A. Blackout

B. Spike

C. Noise

D. Sag

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 3*

Which of the following is the best method to stop vulnerability attacks on a Web server?

A. Implementing the latest virus scanner

B. Using strong passwords

C. Configuring a firewall

D. Installing service packs and updates

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 3*

Which of the following is the most secure method of authentication?

A. Biometrics

B. Smart card

C. Anonymous

D. Username and password

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 3*

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

⇨ It displays the signal strength of a wireless network, MAC address, SISD, channel details, etc.

⇨ It is commonly used for the following purposes:

a. War driving

b. Detecting unauthorized access points

c. Detecting causes of interference on a WLAN

d. WEP ICV error tracking

e. Making Graphs and Alarms on 802.11 Data, including Signal Strength

This tool is known as _____.

A. Kismet

B. NetStumbler

C. Absinthe

D. THC-Scan

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 3*

Which of the following are the phases of the Certification and Accreditation (C&A) process?
Each correct answer represents a complete solution. Choose two.

A. Auditing

B. Initiation

C. Detection

D. Continuous Monitoring

Suggested Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 3*

Which of the following is the method of hiding data within another media type such as graphic or document?

A. Spoofing

B. Cryptanalysis

C. Steganography

D. Packet sniffing

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!