EC-COUNCIL.312-38.v2026-02-04.q327

Exam Code:	312-38
Exam Name:	EC-Council Certified Network Defender CND
Certification Provider:	EC-COUNCIL
Free Question Number:	327
Version:	v2026-02-04
# of views:	185
# of Questions views:	3270
https://www.freepdfdumps.com/EC-COUNCIL.312-38.v2026-02-04.q327.html	

NEW QUESTION: 1
Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?
A. Session hijacking
B. Phishing
C. Smurf
D. Spoofing
Answer: (SHOW ANSWER)

NEW QUESTION: 2
Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denial-of-service, or unauthorized changes to system hardware, software, or data?
A. Disaster Recovery Plan
B. Crisis Communication Plan
C. Cyber Incident Response Plan
D. Occupant Emergency Plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
Which of the following is a management process that provides a framework for promoting quick recovery and the capability for an effective response to protect the interests of its brand, reputation, and stakeholders?
A. Incident handling
B. Patch management
C. Log analysis
D. Business Continuity Management

Answer: (SHOW ANSWER)

NEW QUESTION: 4
Which of the following tool is used for passive attacks to capture network traffic?
A. None
B. Intrusion detection system
C. Sniffer
D. Intrusion prevention system
E. warchalking
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
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. Not broadcasting the SSID
C. WPA encryption
D. WEP encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 6
Drag and drop the Response management plans to match up with their respective purposes.

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:

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

Disaster recovery plan

Crisis communication plan

Contingency plan

Continuity of operation plan

Business recovery plan

Business continuity plan

NEW QUESTION: 7
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 -o
B. netstat -ao
C. netstat -an
D. netstat -a
Answer: C (LEAVE A REPLY)

NEW QUESTION: 8
Fill in the blank with the appropriate term. _____ 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.
Answer:
Disaster recovery

NEW QUESTION: 9
Which of the following OSI layers defines the electrical and physical specifications for devices?
A. Presentation layer
B. Physical layer
C. Transport layer
D. Data link layer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 10
Which of the following tools is an open source protocol analyzer that can capture traffic in real time?
A. Snort
B. Netresident
C. Wireshark
D. NetWitness
Answer: C (LEAVE A REPLY)

NEW QUESTION: 11
The GMT enterprise is working on their internet and web usage policies. GMT would like to control internet bandwidth consumption by employees. Which group of policies would this belong to?
A. Enterprise Information Security Policy
B. Network Services Specific Security Policy
C. Issue Specific Security Policy

D. System Specific Security Policy

Answer: B (LEAVE A REPLY)

The control of internet bandwidth consumption by employees falls under the Network Services Specific Security Policy. This category of policy is designed to manage and secure the services that are provided over the network, which includes internet access and usage. It encompasses the rules and procedures that govern how network services, such as bandwidth, are allocated and used within an organization. By implementing such policies, GMT enterprise aims to ensure that the network's bandwidth is utilized effectively and in alignment with the company's operational requirements and objectives.

NEW QUESTION: 12

John works as a C programmer. He develops the following C program:

His program is vulnerable to a _____ attack.

A. SQL injection

B. Denial-of-Service

C. Buffer overflow

D. Cross site scripting

Answer: C (LEAVE A REPLY)

This program takes a user-supplied string and copies it into 'buffer1', which can hold up to 10 bytes of data. If a user sends more than 10 bytes, it would result in a buffer overflow.

NEW QUESTION: 13

Which of the following is susceptible to a birthday attack?

A. Integrity

B. Digital signature

C. Authentication

D. Authorization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 14
Which of the following attacks comes under the category of an active attack?
A. Replay attack
B. Wireless footprinting
C. Passive Eavesdropping
D. Traffic analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 15
Which characteristic of an antenna refers to how directional an antennas radiation pattern is?
A. Typical gain
B. Polarization
C. Directivity
D. Radiation pattern
Answer: D (LEAVE A REPLY)

NEW QUESTION: 16
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 private information on the Internet
B. To prevent a user from sending a message to another user with the name of a third person
C. To protect information from loss and deliver it to its destination properly
D. To protect information from unwanted editing, accidentally or intentionally by unauthorized users
Answer: (SHOW ANSWER)

NEW QUESTION: 17
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. Virus
B. The reactive IDS
C. None
D. The polymorphic virus
E. Honey Pot
Answer: (SHOW ANSWER)

NEW QUESTION: 18
What is the IT security team responsible for effectively managing the security of the organization's IT infrastructure, called?
A. Grey Team
B. Red Team
C. Blue Team
D. Yellow Team
Answer: C (LEAVE A REPLY)
In the context of cybersecurity, the Blue Team refers to the group responsible for defending an organization's IT infrastructure. This team's primary focus is on internal security measures, maintaining defensive protocols, and ensuring that the organization's systems and data are protected against cyber threats. They are tasked with the effective management of security controls, incident response, and the overall maintenance of the organization's cybersecurity posture.

NEW QUESTION: 19
Which of the following statement holds true in terms of containers?
A. Container requires more memory space
B. Each container runs in its own OS
C. Container is fully isolated; hence, more secure
D. Process-level isolation happens; a container in hence less secure
Answer: (SHOW ANSWER)
Containers are designed to be lightweight, running directly within the host's kernel without the need for a guest operating system. This means they share the same OS kernel but maintain separate user spaces. While this architecture provides process-level isolation, it does not offer the same level of security as a fully isolated virtual machine (VM). VMs include a full copy of an operating system, a virtual copy of the hardware that the OS requires to run, and provide complete isolation from the host system. Containers, on the other hand, are less secure because if the host OS is compromised, all containers could potentially be compromised. The Certified Network Defender (CND) program emphasizes understanding the security implications of

different technologies, including containers, and the importance of implementing appropriate security measures to protect network resources.

NEW QUESTION: 20
Which of the following tools is a free portable tracker that helps the user to trace the laptop if it is stolen?
A. Adeona
B. bridle
C. SAINT
D. Nessus
E. None
Answer: A (LEAVE A REPLY)

NEW QUESTION: 21
According to the company's security policy, all access to any network resources must use Windows Active Directory Authentication. A Linux server was recently installed to run virtual servers and it is not using Windows Authentication. What needs to happen to force this server to use Windows Authentication?
A. Edit the ADLIN file.
B. Edit the shadow file.
C. Remove the /var/bin/localauth.conf file.
D. Edit the PAM file to enforce Windows Authentication
Answer: D (LEAVE A REPLY)
To enforce Windows Active Directory Authentication on a Linux server, the Pluggable Authentication Modules (PAM) configuration files must be edited. PAM provides a way to develop programs that are independent of authentication scheme. These files, located in /etc/pam.d/, dictate how a Linux system handles authentication for various services. To integrate Windows Active Directory with a Linux server, specific PAM modules like pam_krb5 or pam_winbind can be used. These modules allow the Linux system to communicate with the Active Directory server for authentication purposes. The process typically involves installing necessary packages, joining the Linux server to the AD domain, and configuring the PAM files to use AD for authentication.

NEW QUESTION: 22
Which of the following representatives of the incident response team takes forensic backups of systems that are the focus of an incident?
A. Legal representative
B. Information security representative
C. Technical representative
D. Lead investigator
Answer: C (LEAVE A REPLY)

NEW QUESTION: 23
An attacker has access to password hashes of a windows 7 computer. Which of the following attacks can the attacker use to reveal the passwords?
A. XSS
B. Rainbow table
C. Brute force
D. Dictionary attacks
Answer: (SHOW ANSWER)
In the context of password hashes on a Windows 7 computer, a Rainbow Table attack is a feasible method an attacker might use to reveal passwords. This type of attack utilizes precomputed tables known as rainbow tables that contain hash values for every possible combination of characters. An attacker with access to password hashes can use these tables to look up the corresponding plaintext passwords. The effectiveness of rainbow tables stems from their ability to reverse cryptographic hash functions, which are used to store passwords securely. Since Windows 7 uses NTLM hashes, which are known to be vulnerable to rainbow table attacks, this method is particularly relevant.

NEW QUESTION: 24
Which of the following commands can be used to disable unwanted services on Debian, Ubuntu and other Debian-based Linux distributions?
A. # chkconfig [service name]off
B. # chkconfig [service name] -del
C. # service [service name] stop
D. # update-rc.d -f [service name] remove
Answer: D (LEAVE A REPLY)
In Debian-based Linux distributions, such as Ubuntu, the update-rc.d command is used to add and remove services from the startup sequence. To disable a service, the -f option (which stands for `force') is used along with the remove parameter to remove the service from the startup sequence. This prevents the service from starting automatically during the system boot.

NEW QUESTION: 25
Fill in the blank with the appropriate term.
A _____ is a translation device or service that is often controlled by a separate Media Gateway Controller, which provides the call control and signaling functionality.
Answer:
Media gateway

NEW QUESTION: 26
Which of the following network monitoring techniques requires extra monitoring software or hardware?
A. Non-router based

B. Switch based
C. Hub based
D. Router based
Answer: (SHOW ANSWER)
Switch-based network monitoring requires additional monitoring software or hardware because switches operate at the data link layer of the OSI model and do not inherently provide monitoring capabilities. To monitor traffic through a switch, network administrators must use port mirroring or a network tap, which involves configuring the switch to send a copy of the network packets to a monitoring device. This allows the monitoring device to analyze the traffic passing through the switch without interfering with the network's normal operation. This technique is essential for deep packet inspection, intrusion detection systems, and for gaining visibility into the traffic between devices in a switched network.

NEW QUESTION: 27
_____ is a structured and continuous process which integrates information security and risk management activities into the system development life cycle (SDLC).
A. COBIT Framework
B. NIST Risk Management Framework
C. ERM Framework
D. COSO ERM Framework
Answer: (SHOW ANSWER)
The NIST Risk Management Framework (RMF) is a structured process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle (SDLC). It provides a disciplined and structured process that integrates information security and risk management activities into the SDLC. The RMF is designed to help organizations manage the security of their information systems by guiding them through a step-by-step process that includes categorizing information systems, selecting and implementing appropriate security controls, assessing the effectiveness of the controls, authorizing information system operation, and continuously monitoring the security state of the system.

NEW QUESTION: 28
Henry, head of network security at Gentech, has discovered a general report template that someone has reserved only for the CEO. Since the file has to be editable, viewable, and deletable by everyone, what permission value should he set?
A. 700
B. 777
C. 755
D. 600
Answer: B (LEAVE A REPLY)
To allow a file to be editable, viewable, and deletable by everyone, Henry needs to set the file permissions to the most permissive value. In Linux and Unix systems, file permissions are

represented by three sets of three bits, each set representing permissions for the owner, the group, and others.
The permission value of 777 means:
The first digit (7) grants read (4), write (2), and execute (1) permissions to the owner. The second digit (7) grants read, write, and execute permissions to the group. The third digit (7) grants read, write, and execute permissions to others. Setting the permissions to 777 ensures that everyone (owner, group, and others) can read, write, and execute the file. This aligns with the requirement for the file to be editable, viewable, and deletable by everyone.

NEW QUESTION: 29
Which of the following policies to help define what users can and should do to use the network and organization of computer equipment?
A. IT policy
B. general policy
C. None
D. user policy
E. remote access policy
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
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: C (LEAVE A REPLY)
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.

NEW QUESTION: 31
Which of the following protocols is used to report an error in datagram processing?
A. BGP
B. DHCP
C. ICMP

D. ARP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 32
Which of the following networks interconnects devices centered on an individual person's workspace?
A. WWAN
B. WPAN
C. WMAN
D. WLAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 33
Which of the following is a method of authentication that uses physical characteristics?
A. Biometrics
B. ACL
C. Honeypot
D. COMSEC
Answer: (SHOW ANSWER)

NEW QUESTION: 34
How many layers are present in the TCP/IP model?
A. 10
B. 4
C. 7
D. 5
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
Lyle is the IT director for a medium-sized food service supply company in Nebrask a. Lyle's company employs over 300 workers, half of which use computers. He recently came back from a security training seminar on logical security. He now wants to ensure his company is as secure as

possible. Lyle has many network nodes and workstation nodes across the network. He does not have much time for implementing a network-wide solution. He is primarily concerned about preventing any external attacks on the network by using a solution that can drop packets if they are found to be malicious. Lyle also wants this solution to be easy to implement and be network-wide. What type of solution would be best for Lyle?

A. A NEPT implementation would be the best choice.

B. To better serve the security needs of his company, Lyle should use a HIDS system.

C. Lyle would be best suited if he chose a NIPS implementation

D. He should choose a HIPS solution, as this is best suited to his needs.

Answer: C (LEAVE A REPLY)

Lyle's requirements indicate the need for a network-wide solution that is easy to implement and capable of dropping malicious packets to prevent external attacks. A Network Intrusion Prevention System (NIPS) is designed to be deployed across the network to inspect traffic and take action based on predefined security policies, such as dropping malicious packets. NIPS solutions are generally easier to manage and deploy compared to Host Intrusion Prevention Systems (HIPS), which require installation on individual endpoints. Moreover, NIPS can provide a centralized security solution for all the network nodes and workstation nodes that Lyle is concerned about, making it a suitable choice for his medium-sized company.

NEW QUESTION: 36

Which RAID level does not provide data redundancy?

A. RAID level 0

B. RAID level 1

C. RAID level 50

D. RAID level 10

Answer: A (LEAVE A REPLY)

RAID level 0, also known as striping, involves splitting data evenly across two or more disks without parity information, redundancy, or fault tolerance. This means that if one drive fails, the entire array fails, resulting in total data loss. RAID 0 is typically used to increase performance, as it allows for faster read and write operations by using multiple disks simultaneously. However, because it does not duplicate data across the disks, it does not provide any form of data redundancy.

NEW QUESTION: 37

Daniel is monitoring network traffic with the help of a network monitoring tool to detect any abnormalities. What type of network security approach is Daniel adopting?

A. Preventative

B. Reactive

C. Retrospective

D. Defense-in-depth

Answer: B (LEAVE A REPLY)

Daniel is adopting a Reactive network security approach. This approach involves monitoring network traffic to detect any abnormalities or intrusions as they occur. The goal of reactive security is to identify and respond to threats in real-time. It is a part of the broader defense strategy that includes Protect, Detect, Respond, and Predict, where `Detect' aligns with the reactive approach. By using network monitoring tools, Daniel is able to observe the network for any signs of compromise or unusual activity and then take appropriate action to mitigate the threat.

NEW QUESTION: 38
David, a network and system admin, encrypted all the files in a Windows system that supports NTFS file system using Encrypted File Systems (EFS). He then backed up the same files into another Windows system that supports FAT file system. Later, he found that the backup files were not encrypted. What could be the reason for this?
A. EFS could only encrypt the files that follow NTFS
B. FAT files cannot be encrypted
C. EFS is not the encryption system used in Windows
D. Copied files loses their encryption
Answer: A (LEAVE A REPLY)
The Encrypting File System (EFS) is a feature of the NTFS file system that provides encryption at the file system level. It is designed to work specifically with NTFS and does not support the FAT file system. When files encrypted with EFS are copied or backed up to a volume that uses the FAT file system, the encryption is lost because FAT does not support EFS encryption. This is why David found that the backup files were not encrypted after transferring them to a system that supports the FAT file system.

NEW QUESTION: 39
Which of the following attacks, the attacker cannot use the software, which is trying a number of key combinations in order to obtain your password?
A. Smurf attack
B. Shock brutal force
C. None
D. Buffer overflow
E. Zero-day attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
Which of the following OSI layers is sometimes called the syntax layer?
A. Physical layer
B. Application layer
C. Presentation layer
D. Data link layer

Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
In which of the following transmission modes is data sent and received alternatively?
A. Full-duplex mode
B. Bridge mode
C. Half-duplex mode
D. Simplex mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
Which firewall technology can filter application-specific commands such as GET and POST requests?
A. Application proxy
B. Circuit-level gateways
C. Stateful multi-layer inspection
D. Application-level gateways
Answer: D (LEAVE A REPLY)
Application-level gateways, also known as proxy firewalls, operate at the application layer of the OSI model and can filter traffic based on application-specific commands such as HTTP GET and POST requests. These firewalls examine the content of the traffic and make decisions based on the specifics of the application protocol. They can allow or deny traffic based on the actual commands being sent, providing a high level of security by ensuring that only valid types of transactions are completed.

NEW QUESTION: 43
Which of the following is a type of scam that entices a user to disclose personal information?
A. Spamming
B. Phishing
C. Smurfing
D. Sniffing
Answer: (SHOW ANSWER)

NEW QUESTION: 44
In an Ethernet peer-to-peer network, which of the following cables is used to connect two computers, using RJ-45 connectors and Category-5 UTP cable?
A. Parallel
B. Loopback
C. Crossover
D. Serial
Answer: (SHOW ANSWER)

NEW QUESTION: 45
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 a NIDS implementation.
B. Fred's boss wants Fred to monitor a NIPS system.
C. Fred's boss wants to implement a HIPS solution.
D. Fred's boss wants to implement a HIDS solution.
Answer: A (LEAVE A REPLY)
The solution described is a Network Intrusion Detection System (NIDS). A NIDS is designed to monitor and analyze network traffic for all computers on a network without affecting the traffic flow.
It gathers information on potential security threats and alerts the network administrator--in this case, Fred--without taking direct action to block the traffic. This aligns with the requirement of Fred's boss for a solution that monitors network traffic and gathers information without impacting it. Unlike a Network Intrusion Prevention System (NIPS), which actively blocks potential threats, or Host-based Intrusion Detection/Prevention Systems (HIDS/HIPS), which are installed on individual hosts, a NIDS operates at the network level to monitor traffic across all systems.

NEW QUESTION: 46
Eric is receiving complaints from employees that their systems are very slow and experiencing odd issues including restarting automatically and frequent system hangs. Upon investigating, he is convinced the systems are infected with a virus that forces systems to shut down automatically after period of time. What type of security incident are the employees a victim of?
A. Scans and probes
B. Malicious Code
C. Denial of service
D. Distributed denial of service
Answer: (SHOW ANSWER)
The symptoms described by the employees, such as systems being very slow, restarting automatically, and experiencing frequent hangs, are indicative of a security incident involving malicious code. Malicious code refers to software or scripts designed to cause harm to a computer system, network, or server. In this case, the virus that forces systems to shut down

automatically after a period of time is a type of malicious code. It disrupts the normal functioning of the system, leading to decreased performance and unexpected behavior.

NEW QUESTION: 47
Bryson is the IT manager and sole IT employee working for a federal agency in Californi a. The agency was just given a grant and was able to hire on 30 more employees for a new extended project. Because of this, Bryson has hired on two more IT employees to train up and work. Both of his new hires are straight out of college and do not have any practical IT experience. Bryson has spent the last two weeks teaching the new employees the basics of computers, networking, troubleshooting techniques etc. To see how these two new hires are doing, he asks them at what layer of the OSI model do Network Interface Cards (NIC) work on. What should the new employees answer?
A. NICs work on the Session layer of the OSI model.
B. The new employees should say that NICs perform on the Network layer.
C. They should tell Bryson that NICs perform on the Physical layer
D. They should answer with the Presentation layer.
Answer: C (LEAVE A REPLY)
Network Interface Cards (NICs) operate at the Physical layer of the OSI model. This layer is responsible for the actual physical connection between devices. It transmits individual bits from one node to the next and is involved in the electrical, mechanical, procedural, and functional aspects of activating, maintaining, and deactivating physical connections. It's also where hardware like cables, switches, and NICs come into play.

NEW QUESTION: 48
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: 49
Brendan wants to implement a hardware based RAID system in his network. He is thinking of choosing a suitable RAM type for the architectural setup in the system. The type he is interested in provides access times of up to 20 ns. Which type of RAM will he select for his RAID system?
A. NVRAM
B. SDRAM
C. NAND flash memory
D. SRAM
Answer: D (LEAVE A REPLY)
SRAM, or Static Random-Access Memory, is known for its low access time, typically around 20 ns, which makes it suitable for applications requiring high speed, such as cache memory in computers or, in this case, a RAID system. SRAM is faster than DRAM because it does not need to be refreshed as often, which is why it's used where speed is critical. Although SRAM is more expensive and has less density compared to other types of RAM, its speed advantage makes it the preferred choice for Brendan's RAID system requirements.

NEW QUESTION: 50
Which among the following is used by anti-malware systems and threat intelligence platforms to spot and stop malicious activities at an initial stage?
A. Indicators of compromise
B. Indicators of attack
C. Key risk indicators
D. Indicators of exposure
Answer: (SHOW ANSWER)

NEW QUESTION: 51
Which phase of incident response process involves collection of incident evidence and sending them to forensic department for further investigation?
A. Incident recording and assignment
B. Eradication
C. Incident containment

D. Preparation for incident response
Answer: D (LEAVE A REPLY)

NEW QUESTION: 52
Who is responsible for executing the policies and plans required for supporting the information technology and computer systems of an organization?
A. Chief Information Officer (CIO)
B. Business and functional managers
C. Senior management
D. IT security practitioners
Answer: A (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: 53
John has successfully remediated the vulnerability of an internal application that could have caused a threat to the network. He is scanning the application for the existence of a remediated vulnerability, this process is called a_____and it has to adhere to the_____
A. Verification, Security Policies
B. Mitigation, Security policies
C. Vulnerability scanning, Risk Analysis
D. Risk analysis, Risk matrix
Answer: A (LEAVE A REPLY)
The process of scanning an application for the existence of a remediated vulnerability is known as verification. This step is crucial to ensure that the vulnerability has been properly addressed and that the application is no longer susceptible to the previously identified threat. Verification must adhere to the organization's security policies, which provide the framework and guidelines for all security-related activities. These policies ensure that the verification process is conducted in a manner that is consistent with the organization's overall security posture and compliance requirements.

NEW QUESTION: 54
Which of the following is a centralized collection of honeypots and analysis tools?
A. Production honeypot
B. Honeyfarm
C. Research honeypot
D. Honeynet

Answer: B (LEAVE A REPLY)

NEW QUESTION: 55
Which of the following wireless networks provides connectivity over distance up to 20 feet?
A. WMAN
B. WPAN
C. WWAN
D. WLAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 56
Fill in the blank with the appropriate term.
_____ is a prime example of a high-interaction honeypot.
Answer:
Honeynet

NEW QUESTION: 57
Bankofamerica Enterprise is working on an internet and usage policy in a way to control the internet demand. What group of policy does this belong to?
A. Enterprise Information Security Policy
B. Issue Specific Security Policy
C. Network Services Specific Security Policy
D. System Specific Security Policy
Answer: B (LEAVE A REPLY)
The development of an internet and usage policy by Bankofamerica Enterprise to control internet demand falls under the category of Issue Specific Security Policy (ISSP). ISSPs are tailored to address specific areas of technology, requiring frequent updates due to changes in the technology or the environment. They provide guidelines on the acceptable use of the company's internet services, outline the consequences of policy violations, and ensure that the internet resources are not misused.

NEW QUESTION: 58
Fill in the blank with the appropriate word. The primary goal of _____ risk analysis is to determine the proportion of effect and theoretical response.
Answer:
qualitative

NEW QUESTION: 59
Identify the method involved in purging technique of data destruction.
A. Degaussing
B. Wiping

C. Incineration
D. Overwriting
Answer: D (LEAVE A REPLY)
The purging technique of data destruction is aimed at making data recovery infeasible using logical methods, which directly target the data at the memory level. Overwriting is a prevalent technique for purging, where data is destroyed by being overwritten with unintelligible characters like 0s and 1s. This method ensures that the original data cannot be recovered.

NEW QUESTION: 60
Which component of the data packets is encrypted in Transport mode encryption of an IPsec server?
A. Payload
B. Header
C. Header and Payload
D. Encryption is not used in IPsec server
Answer: (SHOW ANSWER)
In Transport mode encryption of an IPsec server, only the payload of the data packet is encrypted. This mode is designed to encrypt the message within an IP packet, while the header remains unencrypted. Transport mode is used for end-to-end communication between a client and a server, where the server can interpret the headers to route the packet to the correct application or process.

NEW QUESTION: 61
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: 62
Which of the following is a high-speed network that connects computers, printers, and other network devices together?
A. MAN
B. LAN
C. CAN
D. WAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 63
Fill in the blank with the appropriate term. _____is a powerful and low-interaction open source honeypot.
Answer:
Honeyd

NEW QUESTION: 64
Which field is not included in the TCP header?
A. Acknowledgment number
B. Sequence number
C. Source port
D. Source IP address
Answer: (SHOW ANSWER)
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: 65
Which OSI layer does a Network Interface Card (NIC) work on?

A. Physical layer
B. Presentation layer
C. Network layer
D. Session layer
Answer: A (LEAVE A REPLY)
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 data. 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 addresses.

NEW QUESTION: 66
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. ICANN
C. ITU
D. ANSI
Answer: (SHOW ANSWER)

NEW QUESTION: 67
Paul is a network security technician working on a contract for a laptop manufacturing company in Chicago. He has focused primarily on securing network devices, firewalls, and traffic traversing in and out of the network. He just finished setting up a server a gateway between the internal private network and the outside public network. This server will act as a proxy, limited amount of services, and will filter packets. What is this type of server called?
A. Bastion host
B. Edge transport server
C. SOCKS hsot
D. Session layer firewall
Answer: A (LEAVE A REPLY)
The server described in the question is known as a Bastion host. A Bastion host is a special-purpose computer on a network specifically designed and configured to withstand attacks. It is typically placed in a network's demilitarized zone (DMZ) and acts as a proxy server, offering limited services and filtering packets to protect the internal private network from the public network. It is hardened due to its exposure to potential attacks and usually hosts a single application, like a proxy server, while all other services are removed or limited to reduce the threat surface.

NEW QUESTION: 68
Which of the following TCP/IP state transitions represents no connection state at all?
A. Closing
B. Close-wait
C. Fin-wait-1
D. Closed
Answer: D (LEAVE A REPLY)

NEW QUESTION: 69
Who offers formal experienced testimony in court?
A. Evidence documenter
B. Attorney
C. Expert witness
D. Incident analyzer
Answer: (SHOW ANSWER)
The individual who offers formal experienced testimony in court is known as an Expert Witness. This person is typically engaged due to their specialized knowledge, skills, or experience in a particular field, which is relevant to the case at hand. They provide informed opinions and insights to help the court understand complex matters that are beyond the general knowledge of the layperson. Unlike other witnesses, an expert witness is allowed to offer opinions and draw conclusions based on the facts presented in the case.

NEW QUESTION: 70
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. RARP
B. DHCP
C. PIM
D. ARP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 71
Michelle is a network security administrator working at a multinational company. She wants to provide secure access to corporate data (documents, spreadsheets, email, schedules, presentations, and other enterprise data) on mobile devices across organizations networks without being slowed down and also wants to enable easy and secure sharing of information between devices within an enterprise. Based on the above-mentioned requirements, which among the following solution should Michelle implement?
A. MDM

B. MAM
C. MCM
D. MEM
Answer: (SHOW ANSWER)
Incident management enables an organization to analyze, identify, and rectify hazards and prevent future recurrence in business continuity management. It involves a systematic process that manages the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized. It is an integral part of an organization's business continuity and disaster recovery plan, focusing on the immediate response to incidents, establishing protocols for communication, and promoting swift recovery actions.

NEW QUESTION: 72
Which of the following protocols is used for exchanging routing information between two gateways in a network of autonomous systems?
A. IGMP
B. ICMP
C. EGP
D. OSPF
Answer: C (LEAVE A REPLY)
EGP stands for Exterior Gateway Protocol. It is used for exchanging routing information between two gateways in a network of autonomous systems. This protocol depends upon periodic polling with proper acknowledgements to confirm that network connections are up and running, and to request for routing updates. Each router requests its neighbor at an interval of 120 to 480 seconds, for sending the routing table updates. The neighbor host then responds by sending its routing table. EGP-2 is the latest version of EGP.
Answer option B is incorrect. Internet Control Message Protocol (ICMP) is a maintenance protocol that allows routers and host computers to swap basic control information when data is sent from one computer to another. It is generally considered a part of the IP layer. It allows the computers on a network to share error and status information. An ICMP message, which is encapsulated within an IP datagram, is very useful to troubleshoot the network connectivity and can be routed throughout the Internet.
Answer option A is incorrect. Internet Group Management Protocol (IGMP) is a communication protocol that multicasts messages and information among all member devices in an IP multicast group. However, multicast traffic is sent to a single MAC address but is processed by multiple hosts. It can be effectively used for gaming and showing online videos. IGMP is vulnerable to network attacks.
Answer option D is incorrect. Open Shortest Path First (OSPF) is a routing protocol that is used in large networks. Internet Engineering Task Force (IETF) designates OSPF as one of the Interior Gateway Protocols. A host uses OSPF to obtain a change in the routing table and to immediately multicast updated information to all the other hosts in the network.

NEW QUESTION: 73
Which of the following is an open source implementation of the syslog protocol for Unix?
A. syslog-os
B. syslog Unix
C. syslog-ng
D. Unix-syslog
Answer: (SHOW ANSWER)

NEW QUESTION: 74
Which of the following protocols is described as a connection-oriented and reliable delivery transport layer protocol?
A. IP
B. SSL
C. TCP
D. UDP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
Which of the following is one of the most commonly used implementations of RAID?
A. RAID 5
B. RAID 1
C. RAID 3
D. RAID 2
Answer: A (LEAVE A REPLY)

NEW QUESTION: 76
Fill in the blank with the appropriate term. The _____ is used for routing voice conversations over the Internet. It is also known by other names such as IP Telephony, Broadband Telephony, etc.
Answer:
VoIP

NEW QUESTION: 77
Which of the following statements best describes the consequences of a disaster recovery test?
A. If no deficiencies were found during the test, so the plan is probably perfect.
B. The test results should be kept secret.
C. If no deficiencies were found during the test, the test was probably erroneous.
D. The plan should not change any of the test results would be.
E. None
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
Which of the following is a mechanism that helps in ensuring that only the intended and authorized recipients are able to read data?
A. Confidentiality
B. Authentication
C. Data availability
D. Integrity
Answer: A (LEAVE A REPLY)

NEW QUESTION: 79
Which of the following IEEE standards provides specifications for wireless ATM systems?
A. 802.11a
B. 802.5
C. 802.1
D. 802.3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
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: 81
Which of the following is a data destruction technique that protects the sensitivity of information against a laboratory attack where an unauthorized individual uses signal processing recovery tools in a laboratory environment to recover the information?
A. Purging
B. Disposal
C. Destroying
D. Clearing
Answer: A (LEAVE A REPLY)
Purging is a data destruction technique designed to protect the sensitivity of information against laboratory attacks. In such attacks, unauthorized individuals may use advanced signal processing recovery tools to recover previously stored information. Purging involves removing the stored data in a way that it cannot be reconstructed by any means, including laboratory techniques. This process often includes degaussing, which demagnetizes the magnetic field of storage media, thereby making data recovery virtually impossible.

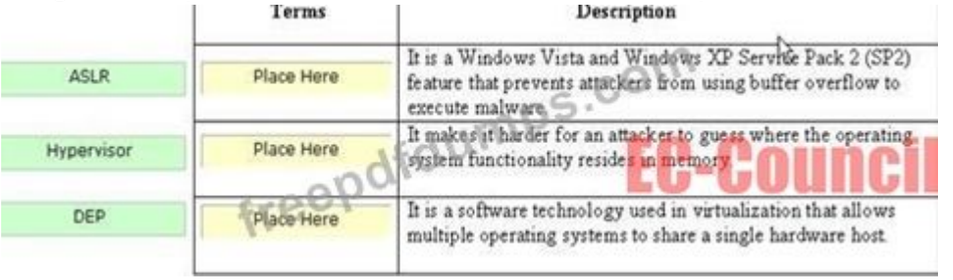
NEW QUESTION: 82
Fill in the blank with the appropriate word. The _____risk analysis process analyzes the effect of a risk event deriving a numerical value.
Answer:
quantitative

NEW QUESTION: 83
Consider a scenario consisting of a tree network. The root Node N is connected to two man nodes N1 and N2. N1 is connected to N11 and N12. N2 is connected to N21 and N22. What will happen if any one of the main nodes fail?
A. Failure of the main node affects all other child nodes at the same level irrespective of the main node.
B. Does not cause any disturbance to the child nodes or its tranmission
C. Failure of the main node will affect all related child nodes connected to the main node
D. Affects the root node only
Answer: (SHOW ANSWER)
In a tree network, each node is connected in a hierarchical manner, with the root node at the top. If a main node (such as N1 or N2) fails, all the child nodes connected to it (N11, N12 for N1 and N21, N22 for N2) will be affected because the tree structure relies on the connectivity of the parent node to its children. The failure of a main node will disrupt the transmission path from the

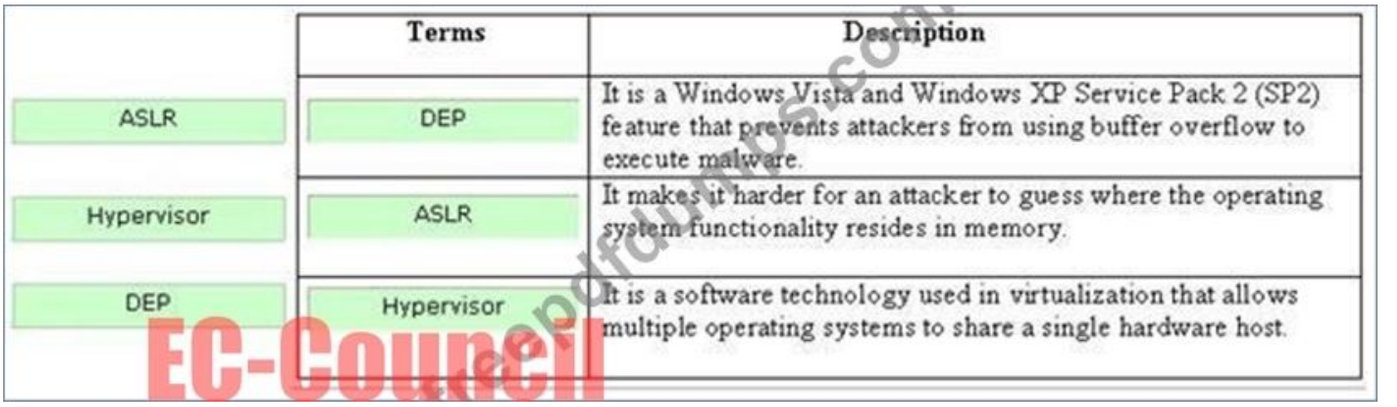
root to the child nodes, leading to a loss of connectivity for those child nodes. This is consistent with the principles of network resilience and fault tolerance as outlined in the EC-Council's Certified Network Defender (CND) program, which emphasizes the importance of each node in maintaining the network's overall integrity.

NEW QUESTION: 84

Drag and drop the terms to match with their descriptions.



Answer:



NEW QUESTION: 85

The IR team and the network administrator have successfully handled a malware incident on the network. The team is now preparing countermeasure guideline to avoid a future occurrence of the malware incident.

Which of the following countermeasure(s) should be added to deal with future malware incidents? (Select all that apply)

A. Complying with the company's security policies

B. Implementing strong authentication schemes

C. Implementing a strong password policy

D. Install antivirus software

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

The countermeasures to deal with future malware incidents involve a multi-layered approach that includes:

Complying with the company's security policies: Ensuring that all security policies are followed can prevent malware incidents by maintaining a secure network environment. Implementing strong authentication schemes: Strong authentication can prevent unauthorized access, reducing the risk of malware being introduced by attackers. Implementing a strong password policy:

Robust password policies can deter attackers by making it more difficult to gain access through brute force or other password-related attacks. Install antivirus software: Antivirus software is essential for detecting, preventing, and removing malware from the network.
These measures align with the Certified Network Defender (CND) program's emphasis on a defense-in-depth strategy, which includes protecting endpoints, data, and networks, as well as continuous threat monitoring and response.

NEW QUESTION: 86
Phishing-like attempts that present users a fake usage bill of the cloud provider is an example of a:
A. Cloud to service attack surface
B. User to service attack surface
C. User to cloud attack surface
D. Cloud to user attack surface
Answer: D (LEAVE A REPLY)
Phishing attempts that target users with fake usage bills from a cloud provider are examples of a cloud to user attack surface. This type of attack surface refers to the potential vulnerabilities and entry points that exist between the cloud service provider and the user. In this scenario, the attacker is exploiting the trust relationship between the user and the cloud service provider by presenting a fraudulent bill, hoping the user will reveal sensitive information or make a payment based on the fake bill.

NEW QUESTION: 87
How can one identify the baseline for normal traffic?
A. When the SYN flag appears at the beginning and the FIN 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 FIN flag appears at the beginning and the SYN flag appears at the end of the connection
Answer: A (LEAVE A REPLY)
In TCP/IP networking, establishing a connection typically starts with a SYN (synchronize) flag and ends with a FIN (finish) flag. This is part of the normal TCP three-way handshake and connection termination process:
SYN (Synchronize): Initiates a connection.
SYN-ACK (Synchronize-Acknowledge): Acknowledges the SYN and responds with a SYN. ACK (Acknowledge): Acknowledges the SYN-ACK, establishing the connection.
FIN (Finish): Terminates the connection.

Observing a SYN flag at the beginning and a FIN flag at the end of the connection indicates a normal, properly terminated TCP session, establishing a baseline for normal traffic patterns.

NEW QUESTION: 88
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: (SHOW ANSWER)
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: 89
Which of the following protocols is used for E-mail?
A. SMTP
B. TELNET
C. MIME
D. SSH
Answer: A (LEAVE A REPLY)

NEW QUESTION: 90
Which of the following protocols is a method of implementing virtual private networks?
A. PPTP
B. IRDP
C. OSPF
D. DHCP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 91
Arman transferred some money to his friend's account using a net banking service. After a few hours, his friend informed him that he hadn't received the money yet. Arman logged on to the bank's website to investigate and discovered that the amount had been transferred to an unknown account instead. The bank, upon receiving Arman's complaint, discovered that someone had established a station between Arman's and the bank server's communication

system. The station intercepted the communication and inserted another account number replacing his friend's account number. What is such an attack called?

A. Privilege Escalation

B. DNS Poisoning

C. Man-in-the-Middle Attack

D. DNS Cache Poisoning

Answer: (SHOW ANSWER)

The scenario described is a classic example of a Man-in-the-Middle (MitM) attack. In this type of cyberattack, the attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. The attacker has inserted themselves between the two parties, in this case, Arman and the bank's server, and has intercepted the communication to redirect the funds to a different account. This type of attack can occur in various forms, such as eavesdropping on or altering the communication over an insecure network service, but it is characterized by the attacker's ability to intercept and modify the data being exchanged without either legitimate party noticing.

NEW QUESTION: 92

Peter works as a network administrator at an IT company. He wants to avoid exploitation of the cloud, particularly Azure services. Which of the following is a group of PowerShell scripts designed to help the network administrator understand how attacks happen and help them protect the cloud?

A. POSH-Sysmon

B. MicroBurst

C. SecurityPolicyDsc

D. Sysmon

Answer: B (LEAVE A REPLY)

MicroBurst is a collection of PowerShell scripts designed to help network administrators understand how attacks occur and to protect cloud environments, particularly Azure services. These scripts aid in detecting vulnerabilities, simulating attacks, and implementing defensive measures to secure the cloud infrastructure.

NEW QUESTION: 93

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. Cain

B. PsPasswd

C. AirSnort

D. Kismet

Answer: (SHOW ANSWER)

NEW QUESTION: 94

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. INFORM

B. RESPONSE

C. TRAPS

D. SET

Answer: C (LEAVE A REPLY)

In SNMP (Simple Network Management Protocol), the TRAPS command is used by SNMP agents to notify SNMP managers about certain events occurring within the network. TRAPS are unsolicited messages sent from an SNMP agent to the SNMP manager, alerting it of a significant event, such as a system reboot, link failure, or high CPU usage. Unlike INFORM requests, which are acknowledged messages ensuring that the notification was received, TRAPS do not require an acknowledgment from the SNMP manager, making them less reliable but faster and more suitable for alerting in real- time scenarios.

NEW QUESTION: 95

Nancy is working as a network administrator for a small company. Management wants to implement a RAID storage for their organization. They want to use the appropriate RAID level for their backup plan that will satisfy the following requirements:

1. It has a parity check to store all the information about the data in multiple drives
2. Help reconstruct the data during downtime.
3. Process the data at a good speed.
4.Should not be expensive.

The management team asks Nancy to research and suggest the appropriate RAID level that best suits their requirements. What RAID level will she suggest?

A. RAID 0

B. RAID 10

C. RAID 3
D. RAID 1
Answer: C (LEAVE A REPLY)
RAID 3 is a level of RAID that uses striping with a dedicated parity disk. This means that data is spread across multiple disks, and parity information is stored on one dedicated disk. RAID 3 allows for good read and write speeds and can reconstruct data if one drive fails, thanks to the parity information. It is also a cost-effective solution because it requires only one additional disk for parity, regardless of the size of the array. This makes it suitable for environments where data throughput and fault tolerance are important but budget constraints are a consideration.

NEW QUESTION: 96
You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from certain region. You suspect a DoS incident on the network.
What will be your first reaction as a first responder?
A. Disable Virus Protection
B. Make an initial assessment
C. Communicate the incident
D. Avoid Fear, Uncertainty and Doubt
Answer: (SHOW ANSWER)
As a first responder to a suspected DoS incident, the initial step is to make an assessment of the situation. This involves analyzing the network traffic using tools like Wireshark to confirm the nature of the traffic and determine if it is indeed a DoS attack. The assessment will help in understanding the scope and impact of the incident and is crucial for deciding the subsequent steps in the response process.

NEW QUESTION: 97
Which of the following protocols supports source-specific multicast (SSM)?
A. DNS
B. BGMP
C. ARP
D. DHCP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement? Each correct answer represents a complete solution. Choose two.
A. Using WPA encryption
B. Not broadcasting SSID
C. MAC filtering the router

D. Using WEP encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 99
Which of the following routing metrics refers to the length of time that is required to move a packet from source to destination through the internetwork?
A. Routing delay
B. Bandwidth
C. Load
D. Path length
Answer: A (LEAVE A REPLY)

NEW QUESTION: 100
Steven's company has recently grown from 5 employees to over 50. Every workstation has a public IP address and navigated to the Internet with little to no protection. Steven wants to use a firewall. He also wants IP addresses to be private addresses, to prevent public Internet devices direct access to them. What should Steven implement on the firewall to ensure this happens?
A. Steven should use a Demilitarized Zone (DMZ)
B. Steven should use Open Shortest Path First (OSPF)
C. Steven should use IPsec
D. Steven should enabled Network Address Translation(NAT)
Answer: (SHOW ANSWER)
Steven should implement Network Address Translation (NAT) on the firewall to ensure that the IP addresses of the workstations are private and not directly accessible from the public Internet. NAT translates the private IP addresses of the workstations to a public IP address before they are sent out to the Internet, and vice versa for incoming traffic. This not only hides the internal IP addresses but also allows multiple devices to share a single public IP address, which is essential as the company grows.

NEW QUESTION: 101
Which of the following is a digital telephone/telecommunication network that carries voice, data, and video over an existing telephone network infrastructure?
A. X.25
B. PPP
C. ISDN
D. Frame relay
Answer: (SHOW ANSWER)

NEW QUESTION: 102
Which of the following is a mandatory password-based and key-exchange authentication protocol?

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

NEW QUESTION: 103
You work for a professional computer hacking forensic investigator DataEnet Inc. To explore the e-mail information about an employee of the company. The suspect an employee to use the online e-mail systems such as Hotmail or Yahoo. Which of the following folders on the local computer you are going to check to accomplish the task? Each correct answer represents a complete solution. Choose all that apply.
A. cookies folder
B. Temporary Internet Folder
C. History Folder
D. download folder
Answer: (SHOW ANSWER)

NEW QUESTION: 104
Which of the following technologies can be used to leverage zero-trust model security?
A. Network function virtualization (NFV)
B. Software-defined networking (SDN)
C. Software-defined perimeter (SDP)
D. Network virtualization (NV)
Answer: C (LEAVE A REPLY)
The zero-trust model is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access. The Software Defined Perimeter (SDP) aligns with this model by creating a dynamic, context-aware, and secure boundary around network resources. SDP controls access to resources based on identity, authentication, and authorization, ensuring that only authenticated and authorized users or systems can access the services they require. This approach minimizes the attack surface by hiding network resources from unauthorized or unauthenticated users, which is a core principle of zero-trust security.

NEW QUESTION: 105
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 spoofing

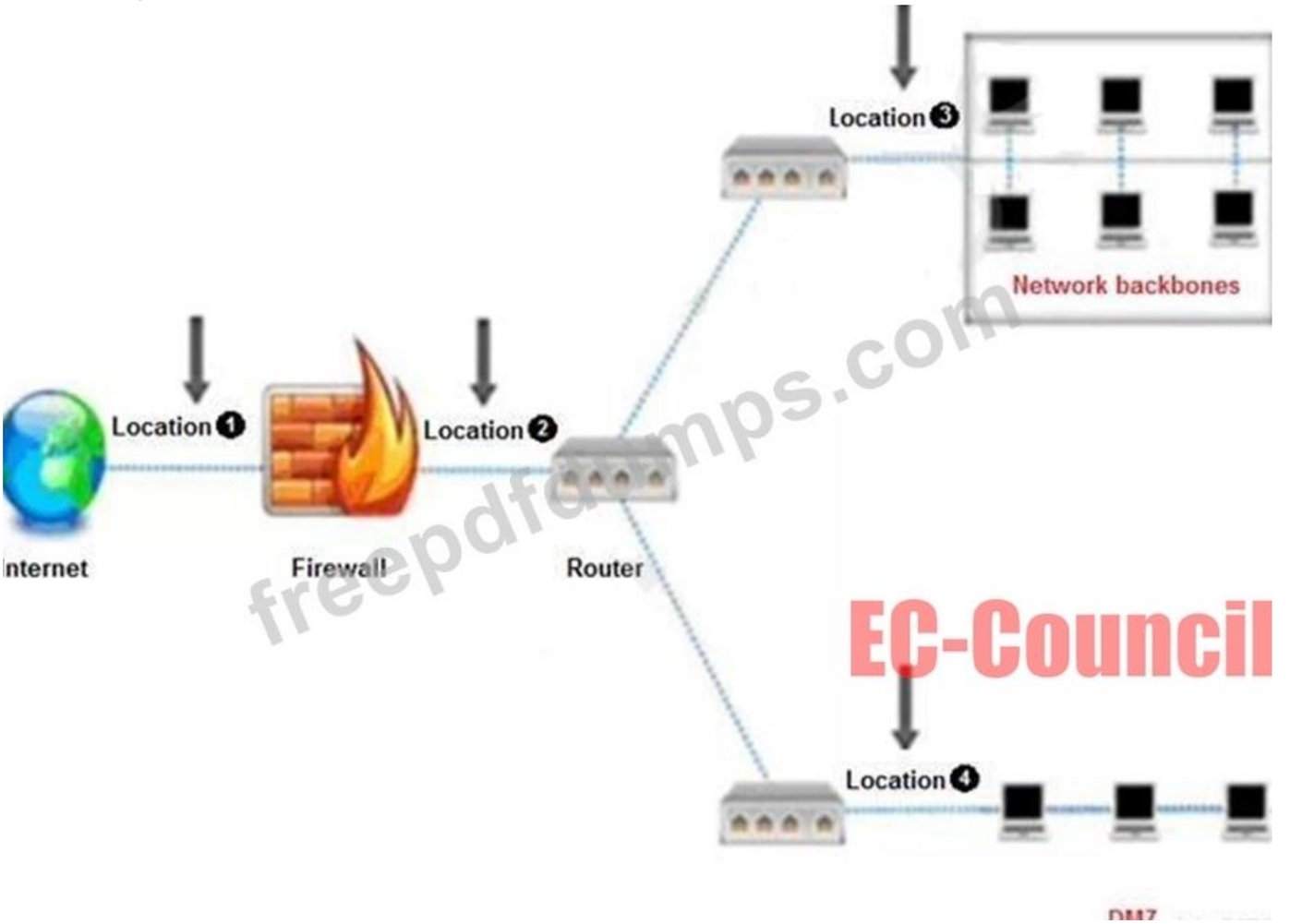
C. E-mail storm
D. E-mail spam
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
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. Nmap
D. Netstat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 107
Which of the following data security technology can ensure information protection by obscuring specific areas of information?
A. Data retention
B. Data encryption
C. Data hashing
D. Data masking
Answer: D (LEAVE A REPLY)
Data masking, also known as data obfuscation, is the process of hiding original data with modified content (characters or other data). This technique is used to protect sensitive information while maintaining a functional substitute for occasions when the real data is not required. For example, in a test database environment, data masking can be used to create a version of the data that is safe for developers to use without exposing sensitive information.
Unlike encryption, which can be reversed with the correct key, data masking is meant to be non-reversible and maintains the format of the data so that it can be used without decryption.

NEW QUESTION: 108
An administrator wants to monitor and inspect large amounts of traffic and detect unauthorized attempts from inside the organization, with the help of an IDS. They are not able to recognize the

exact location to deploy the IDS sensor. Can you help him spot the location where the IDS sensor should be placed?



A. Location 2
B. Location 3
C. Location 4
D. Location 1
Answer: B (LEAVE A REPLY)
In the context of Certified Network Defender (CND), an IDS sensor should be placed at a location where it can effectively monitor and inspect traffic to detect unauthorized attempts. Location 3, which is situated after the firewall but before the network backbone, is ideal for this purpose. At this location, the IDS can analyze traffic that has passed through the firewall, allowing it to focus on potentially harmful traffic that could affect the internal network. It provides visibility into both incoming and outgoing traffic, enabling comprehensive monitoring and detection of any unauthorized or malicious activity.

NEW QUESTION: 109
John is the Vice-President of a BPO. He wants to implement a policy allowing employees to use and manage devices purchased by the organization but restrict the use of the device for business use only. Which among the following policies does John want to implement?
A. COPE policy

B. CYOD policy
C. BYOD policy
D. COBO policy
Answer: B (LEAVE A REPLY)
John wants to implement a policy that allows employees to use and manage devices purchased by the organization but restricts the use of the device for business use only. This is known as a COBO (Company Owned, Business Only) policy. Under a COBO policy, the company provides the devices to the employees and maintains control over them, ensuring that they are used solely for business purposes.

NEW QUESTION: 110
Which of the following is a distance vector routing protocols? Each correct answer represents a complete solution. Choose all that apply.
A. IGRP
B. IS-IS
C. OSPF
D. REST IN PEACE
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 111
Identify the firewall technology that monitors the TCP handshake between the packets to determine whether a requested session is legitimate.
A. Packet Filtering Firewall
B. Stateful Multilayer Inspection
C. Circuit Level Gateway
D. Network Address Translation
Answer: B (LEAVE A REPLY)
Stateful Multilayer Inspection firewalls monitor the state of active connections and determine which network packets to allow through the firewall. They are designed to inspect the TCP handshake, which is the initial connection setup process between two hosts in a network. By monitoring this handshake, the firewall can determine whether a requested session is legitimate. This technology allows the firewall to not only filter packets based on predefined rules but also to ensure that the packets are part of an established and approved connection.

NEW QUESTION: 112
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. IGMP
B. SNMP
C. ICMP
D. BGP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following standards is a proposed enhancement to the 802.11a and 802.11b wireless LAN (WLAN) specifications that offers quality of service (QoS) features, including the prioritization of data, voice, and video transmissions?
A. 802.11e
B. 802.11h
C. 802.11n
D. 802.15
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
WPA encryption in a wireless network uses _____ encryption protocol and a/an _____ integrity check.
A. EAP, CRC-32
B. CCMP, CRC-32
C. CCMP, AES-based
D. TKIP, 64-bit MIC
Answer: D (LEAVE A REPLY)

NEW QUESTION: 115
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: 116
Which of the following techniques is used for drawing symbols in public places for advertising an open Wi-Fi wireless network?
A. War dialing

B. War driving
C. Spamming
D. Warchalking
Answer: D (LEAVE A REPLY)

NEW QUESTION: 117
Fill in the blank with the appropriate term. A _____ is a set of tools that take Administrative control of a computer system without authorization by the computer owners and/or legitimate managers.
Answer:
rootkit

NEW QUESTION: 118
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

NEW QUESTION: 119
You are responsible for network functions and logical security throughout the corporation. Your company has over 250 servers running Windows Server 2012, 5000 workstations running Windows 10, and 200 mobile users working from laptops on Windows 8. Last week 10 of your company's laptops were stolen from a salesman, while at a conference in Barcelon a. These laptops contained proprietary company information. While doing a damage assessment, a news story leaks about a blog post containing information about the stolen laptops and the sensitive information. What built-in Windows feature could you have implemented to protect the sensitive information on these laptops?
A. You should have used 3DES.
B. You should have implemented the Distributed File System (DFS).
C. If you would have implemented Pretty Good Privacy (PGP).
D. You could have implemented the Encrypted File System (EFS)
Answer: (SHOW ANSWER)
The Encrypted File System (EFS) is a feature of the NTFS file system available in Windows that provides filesystem-level encryption. It allows for the transparent encryption of files, protecting confidential data from attackers who might gain physical access to the computers. EFS uses a combination of symmetric key encryption and public key technology to protect files. The symmetric key, known as the File Encryption Key (FEK), is used to encrypt the file data, and then the FEK itself is encrypted with a public key associated with the user's identity and stored with the file. This ensures that only authorized users can decrypt the encrypted files. EFS is particularly

suitable for protecting sensitive data on laptops that might be lost or stolen, as it ensures that the data remains inaccessible without the appropriate encryption key.

NEW QUESTION: 120
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: 121
Which of the following provides a set of voluntary recommended cyber security features to include in network-capable IoT devices?
A. FGMA
B. GLBA
C. GCMA
D. NIST
Answer: D (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: 122
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. Assessment of Risk
B. Analysis of Vulnerabilities
C. Analysis of Threats
D. Identification of Critical Information
E. Application of Appropriate OPSEC Measures
Answer: (SHOW ANSWER)

NEW QUESTION: 123
You are Network Administrator Investment Bank. You're worried about people breeching network and can steal information before you can detect and shut down access. Which of the following is the best way to deal with this issue?
A. Implement a honey pot.
B. To implement the network is based on antivirus.
C. None
D. To implement a strong password policy.
E. To implement a strong firewall.
Answer: (SHOW ANSWER)

NEW QUESTION: 124
Which of the following is true regarding any attack surface?
A. Decrease in vulnerabilities decreases the attack surface
B. Increase in vulnerabilities decreases the attack surface
C. Decrease in risk exposures increases the attack surface
D. Decrease in vulnerabilities increases the attack surface
Answer: (SHOW ANSWER)
The attack surface of a system refers to the sum of all potential points where an unauthorized user can try to enter or extract data from that system. It encompasses all the vulnerabilities, including software flaws, unsecured network ports, and unprotected system endpoints. Therefore, when vulnerabilities are decreased, the attack surface is reduced because there are fewer opportunities for an attacker to exploit. This is a fundamental concept in network security, as reducing the attack surface is a critical step in protecting systems against unauthorized access and potential breaches.

NEW QUESTION: 125

Which Internet access policy starts with all services blocked and the administrator enables safe and necessary services individually, which provides maximum security and logs everything, such as system and network activities?

A. Internet access policy

B. Paranoid policy

C. Permissive policy

D. Prudent policy

Answer: B (LEAVE A REPLY)

The Paranoid policy is an Internet access policy that begins with the premise that all services are blocked by default. Under this policy, the administrator must explicitly enable each service that is deemed safe and necessary. This approach ensures maximum security as it minimizes the potential attack surface by not allowing any services unless they have been vetted and approved. Additionally, this policy typically involves extensive logging of all system and network activities, which can be crucial for monitoring, auditing, and forensic purposes.

NEW QUESTION: 126

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: 127

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 Debian-based Linux OSes?

A. sudo apt-get upgrade

B. sudo apt-get dist-update

C. sudo apt-get dist-upgrade

D. sudo apt-get update

Answer: C (LEAVE A REPLY)

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: 128

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. 802.11i

C. 802.11a

D. 802.11e

Answer: (SHOW ANSWER)

NEW QUESTION: 129

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

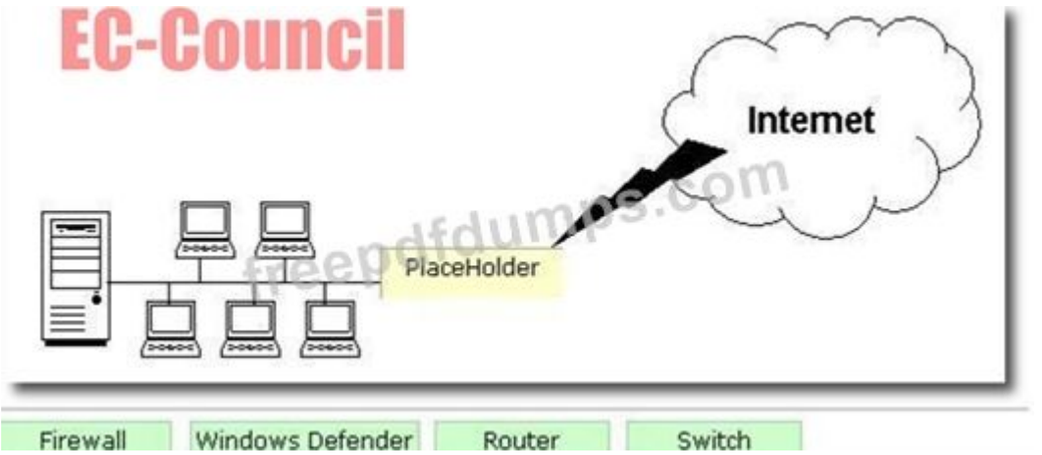
C. Additive increase/multiplicative-decrease

D. Sliding Window

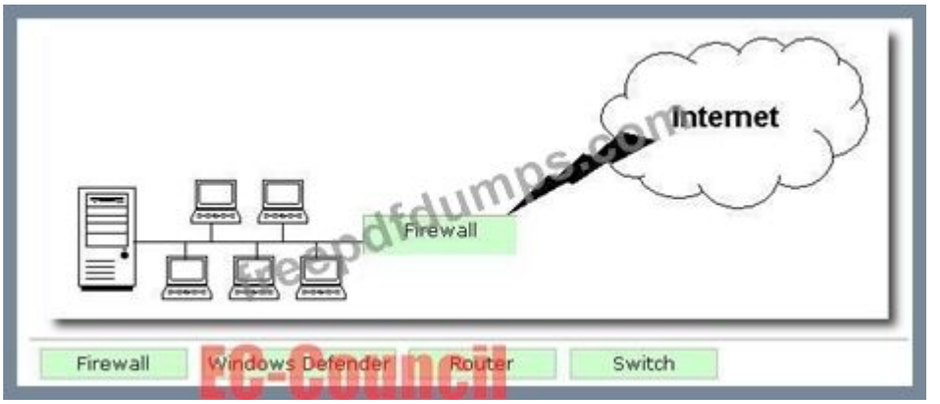
Answer: (SHOW ANSWER)

NEW QUESTION: 130

George works as a Network Administrator for Blue Soft Inc. The company uses Windows Vista operating system. The network of the company is continuously connected to the Internet. What will George use to protect the network of the company from intrusion?



Answer:



NEW QUESTION: 131

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

NEW QUESTION: 132

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

A. spoofing

B. None

C. Zero-day attack

D. website defacement

E. Buffer overflow

Answer: (SHOW ANSWER)

NEW QUESTION: 133

Which of the following is an IPSec protocol that can be used alone in combination with Authentication Header (AH)?

A. PPTP

B. PPP

C. L2TP
D. ESP
Answer: (SHOW ANSWER)

NEW QUESTION: 134
Fill in the blank with the appropriate term. _____ is typically carried out by a remote attacker attempting to gain information or access to a network on which it is not authorized or allowed.
Answer:
Network reconnaissance

NEW QUESTION: 135
What is used for drawing symbols in public places following techniques of advertising an open Wi-Fi network?
A. None
B. spam
C. wardriving
D. war call
E. warchalking
Answer: E (LEAVE A REPLY)

NEW QUESTION: 136
Geon Solutions INC., had only 10 employees when it started. But as business grew, the organization had to increase the amount of staff. The network administrator is finding it difficult to accommodate an increasing number of employees in the existing network topology. So the organization is planning to implement a new topology where it will be easy to accommodate an increasing number of employees. Which network topology will help the administrator solve the problem of needing to add new employees and expand?
A. Bus
B. Star
C. Ring
D. Mesh
Answer: B (LEAVE A REPLY)
The star topology is the most suitable for accommodating an increasing number of employees because it allows for easy addition of new nodes or computers without disrupting the existing network. In a star topology, each node is independently connected to a central hub. If a new employee is added, they can be connected to the hub without affecting the other nodes. This topology also simplifies troubleshooting, as each connection can be individually assessed without taking down the entire network. Furthermore, the star topology is known for its scalability and robustness, making it ideal for a growing company like Geon Solutions INC.

NEW QUESTION: 137
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==9 && ((!(icmp.code==9))
B. (icmp.type==8 && ((!(icmp.code==8))
C. (icmp.type==12) | | (icmp.type==15| |(icmp.type==17)
D. (icmp.type==14) | | (icmp.type==15| |(icmp.type==17)
Answer: B (LEAVE A REPLY)
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 B. 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: 138
The Circuit-level gateway firewall technology functions at which of the following OSI layer?
A. Transport layer
B. Data-link layer
C. Session layer
D. Network layer
Answer: C (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 applications.

NEW QUESTION: 139
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. The type of scan she is usinq is called a NULL scan.

B. Cindy is using a half-open scan to find live hosts on her network.

C. Cindy is attempting to find live hosts on her company's network by using a XMAS scan.

D. She is utilizing a RST scan to find live hosts that are listening on her network.

Answer: B (LEAVE A REPLY)

The technique Cindy is using is known as a half-open scan, or SYN scan. This method involves sending SYN packets, which are the initial step in establishing a TCP connection, to various hosts to determine if the ports are listening. If a host responds with a SYN/ACK, it indicates that the port is open and ready to establish a connection. Cindy then sends an RST packet to terminate the session before the connection is fully established. This type of scan is useful for mapping out live hosts on a network without completing the TCP three-way handshake, thus avoiding the creation of a full connection and reducing the likelihood of detection by intrusion detection systems.

NEW QUESTION: 140

On which of the following OSI layers does the Pretty Good Privacy (PGP) work?

A. Application

B. Data Link

C. Network

D. Transport

Answer: (SHOW ANSWER)

Pretty Good Privacy (PGP) is an encryption program that provides confidentiality, integrity, and authentication for data communication. PGP operates at the Application layer of the OSI model. This is because it is used to encrypt and decrypt texts, emails, files, directories, and whole disk partitions and to enhance the security of email communications. PGP provides these services by utilizing cryptographic privacy and authentication through a hybrid approach that combines symmetric and asymmetric encryption, which is implemented at the Application layer.

NEW QUESTION: 141

Which encryption algorithm is used by WPA3 encryption?

A. RC4

B. AES-CCMP

C. AES-GCMP 256

D. RC4, TKIP

Answer: (SHOW ANSWER)

WPA5 is not a standard term used in the industry, and there seems to be a confusion or typo in the question. However, based on the context of Wi-Fi security and encryption, the closest relevant standard is WPA3, which uses AES-GCMP 256 as its encryption algorithm. WPA3 is the successor to WPA2 and provides enhanced security features. It uses the Advanced Encryption Standard (AES) with Galois/Counter Mode Protocol (GCMP) 256-bit encryption, which offers a higher level of security than the previous encryption methods used in WPA2, such as AES-CCMP. AES-GCMP 256 provides robust protection against various attacks and is designed to work efficiently on a wide range of devices, including those with limited processing capabilities.

NEW QUESTION: 142
In _____ method, windows event logs are arranged in the form of a circular buffer.
A. Non-Wrapping method
B. Out-of Band Method
C. Overwriting Method
D. Wrapping method
Answer: (SHOW ANSWER)

NEW QUESTION: 143
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. Analog modem
B. Cable modem
C. Digital modem
D. DSL
Answer: (SHOW ANSWER)

NEW QUESTION: 144
Which of the following helps in blocking all unauthorized inbound and/or outbound traffic?
A. Firewall
B. IPS
C. IDS
D. Sniffer
Answer: (SHOW ANSWER)

NEW QUESTION: 145
Which IEEE standard does wireless network use?
A. 802.11
B. 802.18
C. 802.9
D. 802.10
Answer: A (LEAVE A REPLY)

The IEEE 802.11 standard is the set of protocols that defines the implementation of wireless local area network (WLAN) communication in the medium access control (MAC) and physical layer (PHY) specifications. It is the foundational standard for wireless networking technologies, commonly known as Wi-Fi. This standard allows for wireless communication between devices by establishing common frequencies and methods of data transmission.

NEW QUESTION: 146
Which of the following entities is responsible for cloud security?
A. Cloud consumer
B. Cloud provider
C. Both cloud consumer and provider
D. Cloud broker
Answer: (SHOW ANSWER)
In the context of cloud security, the responsibility is shared between the cloud provider and the cloud consumer. This is known as the shared responsibility model. The cloud provider is responsible for securing the infrastructure that runs all of the services offered in the cloud. On the other hand, the cloud consumer is responsible for managing the security of their data, applications, and operating systems that they run on the cloud infrastructure. The specific responsibilities can vary depending on the service model being used (IaaS, PaaS, SaaS), but the underlying principle is that both parties have a role to play in ensuring the security of cloud services.

NEW QUESTION: 147
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. Link layer
B. Internet layer
C. Application layer
D. Transport layer
Answer: D (LEAVE A REPLY)

NEW QUESTION: 148
Which of the following layers refers to the higher-level protocols used by most applications for network communication?
A. Internet layer
B. Application layer
C. Transport layer
D. Link layer
Answer: B (LEAVE A REPLY)

NEW QUESTION: 149
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. Function point analysis
B. expert assessment
C. The Delphi technique
D. Program Evaluation Technique (PERT)
Answer: A,B,C (LEAVE A REPLY)

NEW QUESTION: 150
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: 151
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. Bus topology
D. Ring topology
Answer: B (LEAVE A REPLY)

NEW QUESTION: 152
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: (SHOW ANSWER)
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: 153
Sam wants to implement a network-based IDS in the network. Sam finds out the one IDS solution which works is based on patterns matching. Which type of network-based IDS is Sam implementing?
A. Behavior-based IDS
B. Anomaly-based IDS
C. Stateful protocol analysis
D. Signature-based IDS
Answer: D (LEAVE A REPLY)
Sam is implementing a Signature-based Intrusion Detection System (IDS). This type of IDS uses predefined patterns of traffic, known as signatures, to identify and flag potential security threats. These signatures are based on known attack patterns and anomalies that have been identified from past incidents. When network traffic matches a signature within the IDS, an alert is generated, indicating a possible security event or breach. Signature-based IDS is effective in detecting known threats but may not be as effective in identifying new, previously unknown attacks.

NEW QUESTION: 154
A VPN Concentrator acts as a bidirectional tunnel endpoint among host machines. What are the other f unction(s) of the device? (Select all that apply)
A. Provides access memory, achieving high efficiency
B. Assigns user addresses
C. Enables input/output (I/O) operations
D. Manages security keys
Answer: B,D (LEAVE A REPLY)
A VPN Concentrator is a network device designed to manage VPN traffic for multiple users. It acts as a bidirectional tunnel endpoint among host machines and has several key functions. Firstly, it assigns user addresses to enable individual identification within the network. Secondly, it manages security keys which are essential for the encryption and decryption processes, ensuring secure data transmission. The concentrator is responsible for authenticating remote users and granting access to the network after verifying their credentials. It also handles the heavy lifting of encryption and decryption, maintaining the integrity and confidentiality of data traffic.

NEW QUESTION: 155
Which of the following layers performs routing of IP datagrams?
A. Internet layer
B. Application layer
C. Link layer
D. Transport layer
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Hacktivists are threat actors, who can be described as _____ .
A. People motivated by monetary gains
B. People motivated by religious beliefs
C. People having political or social agenda
D. Disgruntled/terminated employees
Answer: C (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: 157

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. Continuity of Operations Plan

D. Business continuity plan

Answer: (SHOW ANSWER)

NEW QUESTION: 158

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

NEW QUESTION: 159

If an organization has decided to consume PaaS Cloud service model, then identify the organization's responsibility that they need to look after based on shared responsibility model.

A. Data, interfaces, application, etc.

B. Data, interfaces, application, middleware, OS, VM, virtual network, etc.

C. Data, interfaces, application, middleware, OS, VM, virtual network, hypervisors, processing and memory, data storage, network interfaces, facilities and data centers, etc.

D. Data, interfaces, etc.

Answer: A (LEAVE A REPLY)

In the PaaS (Platform as a Service) cloud service model, the cloud provider manages the infrastructure, including network, servers, operating systems, and storage. The organization's responsibility is primarily at the application level, which includes the data, interfaces, and the applications themselves. This means the organization must ensure the security and compliance of their data, manage the applications they develop or deploy, and handle the interfaces that connect their applications to other services or users.

NEW QUESTION: 160

The agency Jacob works for stores and transmits vast amounts of sensitive government data that cannot be compromised. Jacob has implemented Encapsulating Security Payload (ESP) to encrypt IP traffic. Jacob wants to encrypt the IP traffic by inserting the ESP header in the IP datagram before the transport layer protocol header. What mode of ESP does Jacob need to use to encrypt the IP traffic?

A. He should use ESP in transport mode.

B. Jacob should utilize ESP in tunnel mode.

C. Jacob should use ESP in pass-through mode.

D. He should use ESP in gateway mode

Answer: (SHOW ANSWER)
Jacob needs to use ESP in tunnel mode to encrypt the IP traffic. In tunnel mode, the entire original IP packet, including both the payload and the IP header, is encrypted and then encapsulated within a new IP packet with a new IP header. This mode is particularly useful for encrypting traffic between different networks, such as in a site-to-site VPN, where the data and security endpoints may differ from the original source and destination IP addresses. Transport mode, on the other hand, would only encrypt the payload of the IP packet, leaving the original IP header unencrypted. Since Jacob's goal is to encrypt the entire IP datagram before the transport layer protocol header, tunnel mode is the appropriate choice.

NEW QUESTION: 161
What is the range for well known ports?
A. 1024 through 49151
B. 49152 through 65535
C. Above 65535
D. 0 through 1023
Answer: D (LEAVE A REPLY)

NEW QUESTION: 162
Which of the following UTP cables uses four pairs of twisted cable and provides transmission speeds of up to 16 Mbps?
A. Category 5e
B. Category 5
C. Category 6
D. Category 3
Answer: D (LEAVE A REPLY)

NEW QUESTION: 163
Which of the following is a computer network protocol used by the hosts to apply for the tasks the IP address and other configuration information?
A. DHCP
B. SNMP
C. None
D. Telnet
E. ARP
Answer: (SHOW ANSWER)

NEW QUESTION: 164
Which of the following types of RAID is also known as disk striping?
A. RAID 0
B. RAID 2

C. RAID 1
D. RAID 3
Answer: A (LEAVE A REPLY)

NEW QUESTION: 165
A company wants to implement a data backup method that allows them to encrypt the data ensuring its security as well as access it at any time and from any location. What is the appropriate backup method that should be implemented?
A. Cloud backup
B. Offsite backup
C. Hot site backup
D. Onsite backup
Answer: A (LEAVE A REPLY)
The appropriate backup method for a company that wants to ensure data encryption and accessibility from any location at any time is Cloud backup. Cloud backup solutions provide data encryption which secures the data during transmission and storage. Moreover, cloud services are designed to be accessible over the internet, allowing for remote access to the data from any location. This aligns with the company's requirements for a secure and readily accessible backup method.

NEW QUESTION: 166
Which of the following protocols is used to share information between routers to transport IP Multicast packets among networks?
A. RPC
B. DVMRP
C. RSVP
D. LWAPP
Answer: B (LEAVE A REPLY)

NEW QUESTION: 167
Which of the following is a type of VPN that involves a single VPN gateway?
A. Remote-access VPN

B. Extranet-based VPN
C. PPTP VPN
D. Intranet-based VPN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 168
Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company's security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company's security policy. What will he do to accomplish this? Each correct answer represents a part of the solution. Choose three.
A. Configure the authentication type for the wireless LAN to Open system.
B. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
C. Install a firewall software on each wireless access point.
D. On each client computer, add the SSID for the wireless LAN as the preferred network.
E. Configure the authentication type for the wireless LAN to Shared Key.
F. Broadcast SSID to connect to the access point (AP).
Answer: (SHOW ANSWER)

NEW QUESTION: 169
Which authorization lets users access a requested resource on behalf of others?
A. Explicit Authorization
B. Decentralized Authorization
C. Implicit Authorization
D. Centralized Authorization
Answer: (SHOW ANSWER)
Implicit Authorization is a type of authorization that allows users to access resources on behalf of others without the need for explicit permission from the resource owner each time. This is commonly implemented through OAuth, where a user grants a third-party application access to their information on another service without sharing their credentials. The application receives an access token that permits it to act on behalf of the user, accessing only what the user is authorized to access.

NEW QUESTION: 170
How is the chip-level security of an IoT device achieved?
A. Closing insecure network services
B. Changing the password of the router

C. Encrypting JTAG interface
D. Keeping the device on a flat network
Answer: C (LEAVE A REPLY)
Chip-level security for an IoT device is achieved by implementing measures that protect the device's hardware, particularly against physical attacks and unauthorized access to debugging ports. Encrypting the JTAG (Joint Test Action Group) interface is a critical step in securing an IoT device at the chip level. The JTAG interface is a standard for testing PCBs (Printed Circuit Boards) and widely used for debugging embedded systems. If left unsecured, it can be exploited to reverse engineer the device firmware or to inject malicious code. Encryption of the JTAG interface ensures that even if attackers gain physical access to the JTAG port, they cannot use it to compromise the device without the encryption key.

NEW QUESTION: 171
Which of the following connects the SDN application layer and SDN controller and allows communication between the network services and business applications?
A. Eastbound API
B. Westbound API
C. Northbound API
D. Southbound API
Answer: C (LEAVE A REPLY)
In the context of Software-Defined Networking (SDN), the Northbound API is the interface that connects the SDN application layer to the SDN controller. It facilitates communication between the network services and business applications. The Northbound API allows applications to communicate their network requirements to the controller, which then translates these requirements into the network configurations necessary to provide the requested services.

NEW QUESTION: 172
Which of the following cables is made of glass or plastic and transmits signals in the form of light?
A. Fiber optic cable
B. Twisted pair cable
C. Plenum cable
D. Coaxial cable
Answer: A (LEAVE A REPLY)

NEW QUESTION: 173
Which of the following protocols is used to exchange encrypted EDI messages via email?
A. S/MIME
B. HTTP
C. HTTPS
D. MIME
Answer: A (LEAVE A REPLY)

NEW QUESTION: 174
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. Both 1 and 2
B. 1 only
C. 2 only
D. None
Answer: B (LEAVE A REPLY)
The Zero-trust network model is designed to ensure strict identity verification for every user or device attempting to access network resources, regardless of whether they are inside or outside the network perimeter. This model operates on the principle of "never trust, always verify," which means that no one is trusted by default, and verification is required from everyone trying to gain access to resources on the network. On the other hand, the Castle-and-Moat model operates on the principle that once inside the network, users or devices are generally trusted. This model does not enforce strict identity verification for every user or device within the network, which is a fundamental difference from the Zero-trust model.

NEW QUESTION: 175
The IP addresses reserved for multicasting belong to which of the following classes?
A. Class E
B. Class D
C. Class B
D. Class C
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
Which of the Windows security component is responsible for controlling access of a user to Windows resources?
A. Network Logon Service (Netlogon)
B. Security Accounts Manager (SAM)
C. Security Reference Monitor (SRM)
D. Local Security Authority Subsystem (LSASS)
Answer: (SHOW ANSWER)
The Security Reference Monitor (SRM) is the core component in Windows operating systems responsible for controlling access to resources. It enforces security policies and checks whether a user's request to access a resource is allowed by the system's security policy. SRM operates in the kernel mode and ensures that access rights and permissions are properly enforced, making it a critical part of the Windows security architecture for resource access control.

NEW QUESTION: 177
Which of the following is a standard protocol for interfacing external application software with an information server, commonly a Web server?
A. IP
B. TCP
C. DHCP
D. CGI
Answer: D (LEAVE A REPLY)

NEW QUESTION: 178
John wants to implement a firewall service that works at the session layer of the OSI model. The firewall must also have the ability to hide the private network information. Which type of firewall service is John thinking of implementing?
A. Application level gateway
B. Stateful Multilayer Inspection
C. Circuit level gateway
D. Packet Filtering
Answer: C (LEAVE A REPLY)
A circuit level gateway is a type of firewall that operates at the session layer of the OSI model, which is Layer 5. This kind of firewall is designed to provide security by validating and managing sessions without inspecting the actual contents of each packet. It is particularly adept at hiding the private network information because it only allows traffic through that is part of an established session, effectively masking the details of the network's internal structure from the outside. This makes it an ideal choice for John's requirements.

NEW QUESTION: 179
John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.
Original cookie values:
ItemID1=2
ItemPrice1=900
ItemID2=1
ItemPrice2=200
Modified cookie values:
ItemID1=2
ItemPrice1=1
ItemID2=1
ItemPrice2=1
Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.
Which of the following hacking techniques is John performing?

A. Cross site scripting
B. Computer-based social engineering
C. Man-in-the-middle attack
D. Cookie poisoning
Answer: D (LEAVE A REPLY)

NEW QUESTION: 180
Patrick wants to change the file permission of a file with permission value 755 to 744. He used a Linux command chmod [permission Value] [File Name] to make these changes. What will be the change in the file access?
A. He changed the file permission from rwxr-xr-x to rwx-r--r--
B. He changes the file permission from rwxr-xr-x to rw-rw-rw-
C. He changed the file permission from rw------- to rw-r--r--
D. He changed the file permission from rwxrwxrwx to rwx------
Answer: A (LEAVE A REPLY)
In Linux file permissions, the numerical value 755 represents the permissions rwxr-xr-x, where `r' stands for read, `w' for write, and `x' for execute. The first digit `7' corresponds to the file owner's permissions, allowing read, write, and execute. The second and third digits `5' and `5' correspond to the group and others' permissions, allowing read and execute. Changing the permission to 744 changes the group and others' permissions to read only (r-), removing the execute permission.

NEW QUESTION: 181
Which of the following IEEE standards defines the demand priority access method?
A. 802.12
B. 802.15
C. 802.3
D. 802.11
Answer: (SHOW ANSWER)

NEW QUESTION: 182
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: (SHOW ANSWER)
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: 183
Identify the spread spectrum technique that multiplies the original data signal with a pseudo random noise spreading code.
A. FHSS
B. DSSS
C. OFDM
D. ISM
Answer: (SHOW ANSWER)
The spread spectrum technique that involves multiplying the original data signal with a pseudo-random noise spreading code is known as Direct Sequence Spread Spectrum (DSSS). In DSSS, the data signal is combined with a higher data-rate bit sequence, also known as a chipping code, which divides the data according to a spreading ratio. The chipping code is a pseudo-random code sequence that spreads the signal across a wider bandwidth. This process allows the signal to be more resistant to interference and eavesdropping.

NEW QUESTION: 184
Peter, a malicious hacker obtains e-mail addresses by collecting them messages, blogs, DNS lists and Web pages. Then he will send a large number of unsolicited commercial e-mail (UCE) messages to these addresses. What Peter at the following e-mail committing crimes?
A. E-Mail bombing
B. None
C. E-Mail scam
D. spam
E. E-Mail storm
Answer: D (LEAVE A REPLY)

NEW QUESTION: 185
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. LogLevel
C. LogFormat
D. ErrorLog
Answer: B (LEAVE A REPLY)

NEW QUESTION: 186
During a security awareness program, management was explaining the various reasons which create threats to network security. Which could be a possible threat to network security?
A. Configuring automatic OS updates
B. Having a web server in the internal network
C. Implementing VPN
D. Patch management
Answer: B (LEAVE A REPLY)
Having a web server within the internal network can pose a threat to network security because it increases the attack surface that an adversary can exploit. If not properly secured, internal web servers can be vulnerable to various attacks, such as SQL injection, cross-site scripting, and others. These vulnerabilities can lead to unauthorized access, data breaches, and other security incidents. Therefore, it is crucial to ensure that web servers are securely configured and isolated from the internal network to minimize the risk.

NEW QUESTION: 187
Which of the following protocols are used to exchange routing information between the two gateways network of autonomous systems?
A. IGMP
B. EGP
C. ICMP
D. None
E. OSPF
Answer: B (LEAVE A REPLY)

NEW QUESTION: 188
----------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: 189
Which of the following is not part of the recommended first response steps for network defenders?
A. Restrict yourself from doing the investigation
B. Extract relevant data from the suspected devices as early as possible
C. Disable virus protection
D. Do not change the state of the suspected device
Answer: C (LEAVE A REPLY)
The recommended first response steps for network defenders typically include preserving the state of the suspected devices and extracting relevant data as early as possible. Disabling virus protection is not part of the recommended first response steps because it could compromise the system's security further and potentially destroy evidence. The primary goal in the initial response is to maintain the integrity of the system and the evidence it contains.

NEW QUESTION: 190
Fargo, head of network defense at Globadyne Tech, has discovered an undesirable process in several Linux systems, which causes machines to hang every 1 hour. Fargo would like to eliminate it; what command should he execute?
A. # update-rc.d -f [service name] remove
B. # service [service name] stop
C. # ps ax | grep [Target Process]
D. # kill -9 [PID]
Answer: D (LEAVE A REPLY)
To eliminate an undesirable process that is causing Linux systems to hang, Fargo should use the command # kill -9 [PID]. This command sends the SIGKILL signal to the process with the specified PID (Process ID), which forcefully stops the process immediately. The kill -9 command is used when a process cannot be terminated using normal shutdown commands. It is important to note that this command should be used with caution, as it does not allow the process to perform any cleanup operations before shutting down.

NEW QUESTION: 191
Which type of risk treatment process includes not allowing the use of laptops in an organization to ensure its security?
A. Eliminate the risk
B. Risk avoidance
C. Reduce the risk
D. Mitigate the risk
Answer: B (LEAVE A REPLY)
The risk treatment process that includes not allowing the use of laptops in an organization to ensure its security is known as risk avoidance. Risk avoidance is a strategy that involves identifying a potential risk and making the decision to not engage in the activity that presents the risk. In the context of information security, this could mean choosing not to use certain technologies or systems that could pose a security threat. By not using laptops, an organization can avoid the risks associated with loss, theft, or unauthorized access that laptops, being portable, are particularly susceptible to.

NEW QUESTION: 192
If Myron, head of network defense at Cyberdyne, wants to change the default password policy settings on the company's Linux systems, which directory should he access?
A. /etc/logrotate.conf
B. /etc/hosts.allow
C. /etc/crontab
D. /etc/login.defs
Answer: (SHOW ANSWER)
The /etc/login.defs file in Linux systems contains the configuration for user login settings, which includes the default password policy settings. This file is used to control several aspects of user management, including password requirements such as password aging, password length, and password complexity. When the head of network defense, like Myron, wants to change these settings, he would access and modify the /etc/login.defs file to implement the new password policies across the company's Linux systems.

NEW QUESTION: 193
Which of the following can be performed with software or hardware devices in order to record everything a person types using his keyboard?
A. Keystroke logging
B. War dialing
C. IRC bot
D. Warchalking
Answer: (SHOW ANSWER)

NEW QUESTION: 194

Individuals in the organization using system resources against acceptable usage policies indicates which of the following security incident:

A. Malicious Code

B. Denial-of-Service (DoS)

C. Improper Usage

D. Unauthorized Access

Answer: C (LEAVE A REPLY)

The term `Improper Usage' refers to instances where individuals use system resources in a manner that is not compliant with the organization's acceptable usage policies. This could involve a range of activities, from excessive personal use of the internet during work hours to the installation of unauthorized software. It is differentiated from `Unauthorized Access,' which implies gaining access to resources one is not permitted to use, and `Malicious Code,' which relates to software designed to harm or exploit systems. `Denial-of-Service' refers to attacks intended to disrupt service availability.

NEW QUESTION: 195

An insider in Hexagon, a leading IT company in USA, was testing a packet crafting tool. This tool generated a lot of malformed TCP/IP packets which crashed the main server's operating system leading to restricting the employees' accesses. Which attack did the insider use in the above situation?

A. DoS attack

B. Session Hijacking

C. Man-in-the-Middle

D. Cross-Site-Scripting

Answer: A (LEAVE A REPLY)

The situation described involves an insider using a packet crafting tool that generated malformed TCP/IP packets, resulting in the crash of the main server's operating system and restricting employee access. This scenario is indicative of a Denial of Service (DoS) attack. A DoS attack aims to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Malformed packets can cause systems to crash, thereby denying service to legitimate users.

NEW QUESTION: 196

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. IP, application, and network interface

B. Network interface, TCP, and IP

C. Application, TCP, and IP

D. Application, IP, and network interface

Answer: C (LEAVE A REPLY)

Multilayer inspection firewalls, also known as Next-Generation Firewalls (NGFWs), are designed to provide comprehensive security by inspecting traffic across multiple layers of the TCP/IP model.
These firewalls offer protection at the:
Application Layer: They can analyze and filter traffic based on application-level protocols and payloads, such as HTTP, FTP, and DNS, providing protection against application-specific attacks.
Transport Layer (TCP): They inspect the transport layer to monitor and control TCP/UDP traffic, preventing threats such as port scans and DoS attacks.
Internet Layer (IP): They filter and monitor IP packets, enforcing security policies based on IP addresses and ensuring protection against IP-level attacks like IP spoofing. By operating at these layers, multilayer inspection firewalls provide a robust defense mechanism against a wide range of network threats.

NEW QUESTION: 197
The network admin decides to assign a class B IP address to a host in the network. Identify which of the following addresses fall within a class B IP address range.
A. 255.255.255.0
B. 18.12.4.1
C. 172.168.12.4
D. 169.254.254.254
Answer: B (LEAVE A REPLY)
Class B IP addresses range from 128.0.0.0 to 191.255.255.255. The first two bits of the first octet in a Class B address are always set to `10', and the default subnet mask is 255.255.0.0. Option B, 18.12.4.1, falls within this range, with the first octet being 18, which is between 128 and 191.

NEW QUESTION: 198
John has implemented_____in the network to restrict the limit 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)
Network Address Translation (NAT) is a network function that translates private IP addresses into a public IP address. This technique restricts the number of public IP addresses required by an organization, as multiple devices on a private network can share a single public IP address. NAT also enhances firewall filtering techniques by hiding the internal IP addresses from the external network, which adds a layer of security by making it more difficult for attackers to target specific devices within the organization's network. It is a common practice in network security to use NAT in conjunction with firewalls to manage the traffic entering and leaving the network, ensuring that only authorized access is permitted.

NEW QUESTION: 199
Who is responsible for conveying company details after an incident?
A. IR officer
B. IR manager
C. PR specialist
D. IR custodians
Answer: C (LEAVE A REPLY)
In the context of incident response (IR), the PR specialist is typically responsible for conveying company details after an incident. Their role involves managing communications with the media, stakeholders, and the public to maintain the organization's reputation. While IR officers, managers, and custodians play crucial roles in handling and responding to the incident itself, the PR specialist is the one who communicates with external parties about the incident.

NEW QUESTION: 200
Which of the following IEEE standards is also called Fast Basic Service Set Transition?
A. 802.11e
B. 802.11b
C. 802.11a
D. 802.11r
Answer: D (LEAVE A REPLY)

NEW QUESTION: 201
Which of the following routing metrics refers to the time required to transfer the package to the source via the Internet?
A. routing delay
B. charge
C. length of the trail
D. bandwidth
E. None
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
Which authentication technique involves mathematical pattern-recognition of the colored part of the eye behind the cornea?
A. Iris Scanning
B. Retinal Scanning
C. Facial Recognition
D. Vein Scanning
Answer: A (LEAVE A REPLY)
Iris scanning is an authentication technique that involves mathematical pattern-recognition of the colored part of the eye, known as the iris. This method uses the unique patterns in the iris to identify and verify an individual's identity. The iris is a muscle within the eye that controls the size of the pupil and is visible from the exterior. It has a complex structure and contains many microscopic features that are unique to each individual, making it a reliable biometric for authentication purposes.

NEW QUESTION: 203
Which BC/DR activity works on the assumption that the most critical processes are brought back from a remote location first, followed by the less critical functions?
A. Restoration
B. Response
C. Resumption
D. Recovery
Answer: (SHOW ANSWER)

NEW QUESTION: 204
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 hosted. Which vulnerability assessment tool should you consider to use?
A. dnsbrute
B. hping
C. OpenVAS
D. wireshark
Answer: C (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: 205

Which of the following is a database encryption feature that secures sensitive data by encrypting it in client applications without revealing the encrypted keys to the data engine in MS SQL Server?

A. Always Encrypted

B. IsEncrypted Enabled

C. Allow Encrypted

D. NeverEncrypted disabled

Answer: A (LEAVE A REPLY)

The 'Always Encrypted' feature in MS SQL Server is designed to protect sensitive data by performing encryption within client applications. It ensures that the encryption keys are never revealed to the Database Engine. This separation between data owners and data managers provides a secure environment where on-premises database administrators or cloud database operators do not have access to the encryption keys. Always Encrypted allows for a secure storage of sensitive data in the cloud and reduces the risk of data theft by malicious insiders.

NEW QUESTION: 206

Which of the following is a communication protocol that multicasts messages and information among all member devices in an IP multicast group?

A. ICMP

B. IGMP

C. BGP

D. EGP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 207

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: 208

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

A. None

B. RG-62

C. RG-59

D. RG-8

E. RG-58

Answer: (SHOW ANSWER)

NEW QUESTION: 209

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: 210

Which of the following is a compatible network device that converts various communication protocols and are used to connect different network technologies?

A. port

B. none

C. bridge

D. router

E. change

Answer: A (LEAVE A REPLY)

NEW QUESTION: 211

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: 212

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: D (LEAVE A REPLY)
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: 213
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: (SHOW ANSWER)
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: 214
Which of the following are the responsibilities of the disaster recovery team?Each correct answer represents a complete solution. Choose all that apply.
A. To notify management, affected personnel, and third parties about the disaster
B. To initiate the execution of the disaster recovery procedures
C. To monitor the execution of the disaster recovery plan and assess the results
D. To modify and update the disaster recovery plan according to the lessons learned from previous disaster recovery efforts
Answer: A,B,C,D (LEAVE A REPLY)

NEW QUESTION: 215

Which of the following is a management process that provides a framework to stimulate a rapid recovery, and the ability to react effectively to protect the interests of its brand, reputation and stakeholders?

A. response systems

B. None

C. Business Continuity Management

D. patch management

E. log analysis

Answer: C (LEAVE A REPLY)

NEW QUESTION: 216

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. Recovery

B. Containment

C. Eradication

D. Preparation

Answer: D (LEAVE A REPLY)

NEW QUESTION: 217

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: (SHOW ANSWER)

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: 218

Which technique is used in RAID level 0 where the data is split into blocks and written evenly across multiple disks?

A. Disk mirroring

B. Disk stripping

C. Data splitting
D. Disk partition
Answer: B (LEAVE A REPLY)
RAID level 0 employs a technique known as disk stripping, which involves splitting data into blocks and distributing them evenly across multiple disks. This method enhances performance by allowing simultaneous read and write operations on multiple drives. However, it does not provide redundancy, meaning if one drive fails, all data on the array could be lost. The primary advantage of disk stripping is the improved I/O performance due to the parallel processing of data across the drives.

NEW QUESTION: 219
USB ports enabled on a laptop is an example of____
A. System Attack Surface
B. Network Attack Surface
C. Physical Attack Surface
D. Software attack Surface
Answer: C (LEAVE A REPLY)
The term "attack surface" refers to the sum of all possible points where an unauthorized user can try to enter data to or extract data from an environment. The enabled USB ports on a laptop are considered a part of the physical attack surface because they allow for physical interaction with the device. This includes the potential for unauthorized devices to be connected, which could be used to compromise security, such as through the introduction of malware or the unauthorized copying of sensitive data.

NEW QUESTION: 220
Fill in the blank with the appropriate term. _____is the complete network configuration and information toolkit that uses multi-threaded and multi-connection technologies in order to be very fast and efficient.
Answer:
NetRanger
Explanation:
NetRanger is the complete network configuration and information toolkit that includes the following tools: a Ping tool, Trace Route tool, Host Lookup tool, Internet time synchronizer, Whois tool, Finger Unix hosts tool, Host and port scanning tool, check multiple POP3 mail accounts tool, manage dialup connections tool, Quote of the day tool, and monitor Network Settings tool. These tools are integrated in order to use an application interface with full online help. NetRanger is designed for both new and experienced users. This tool is used to help diagnose network problems and to get information about users, hosts, and networks on the Internet or on a user computer network. NetRanger uses multi-threaded and multi-connection technologies in order to be very fast and efficient.

NEW QUESTION: 221
Which of the following is the main international standards organization for the World Wide Web?
A. W3C
B. ANSI
C. CCITT
D. WASC
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
Frank is a network technician working for a medium-sized law firm in Memphis. Frank and two other IT employees take care of all the technical needs for the firm. The firm's partners have asked that a secure wireless network be implemented in the office so employees can move about freely without being tied to a network cable. While Frank and his colleagues are familiar with wired Ethernet technologies, 802.3, they are not familiar with how to setup wireless in a business environment. What IEEE standard should Frank and the other IT employees follow to become familiar with wireless?
A. The IEEE standard covering wireless is 802.9 and they should follow this.
B. 802.7 covers wireless standards and should be followed
C. They should follow the 802.11 standard
D. Frank and the other IT employees should follow the 802.1 standard.
Answer: C (LEAVE A REPLY)
The correct IEEE standard for wireless networking in a business environment is 802.11. This series of standards defines the protocols for implementing wireless local area network (WLAN) communications in various frequencies, including 2.4, 5, and 60 GHz bands. The 802.11 standards are widely used worldwide and form the basis of wireless network products that are marketed under the Wi-Fi brand. Frank and his colleagues should familiarize themselves with the 802.11 standards to set up a secure wireless network for their firm.

NEW QUESTION: 223
Which of the following representatives of the incident response team takes the forensic backups of systems that are essential event?
A. None
B. technical representative
C. lead investigator
D. the legal representative
E. Information Security representative
Answer: B (LEAVE A REPLY)

NEW QUESTION: 224
What cryptography technique can encrypt small amounts of data and applies it to digital signatures?

A. Hashing
B. Asymmetric encryption
C. Symmetric encryption
D. Digital certificates
Answer: B (LEAVE A REPLY)
Asymmetric encryption, also known as public-key cryptography, uses a pair of keys--a public key and a private key--to encrypt and decrypt data. This method is widely used for securing small amounts of data, such as digital signatures. In asymmetric encryption:
The public key is used to encrypt the data.
The private key is used to decrypt the data.
Digital signatures utilize asymmetric encryption to ensure the integrity and authenticity of a message. When a sender signs a document with their private key, the recipient can verify the signature using the sender's public key, confirming that the document was indeed signed by the sender and has not been altered.

NEW QUESTION: 225
You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:

What is the IP address of the sender of this email?
A. 141.1.1.1
B. 216.168.54.25
C. 209.191.91.180
D. 172.16.10.90
Answer: B (LEAVE A REPLY)

NEW QUESTION: 226

Which form of access control is trust centric?
A. Application sandboxing
B. Application patch management
C. Application blacklisting
D. Application whitelisting
Answer: (SHOW ANSWER)

NEW QUESTION: 227
Ryan works as a network security engineer at an organization the recently suffered an attack. As a countermeasure, Ryan would like to obtain more information about the attacker and chooses to deploy a honeypot into the organizations production environment called Kojoney. Using this honeypot, he would like to emulate the network vulnerability that was attacked previously. Which type of honeypot is he trying to implement?
A. High interaction honeypots
B. Research honeypot
C. Low interaction honeypots
D. Pure honeypots
Answer: C (LEAVE A REPLY)
A low-interaction honeypot, like Kojoney, is designed to emulate specific network vulnerabilities and gather information about attackers without providing a full-fledged operating environment. These honeypots are typically easier to deploy and maintain compared to high-interaction honeypots. They simulate certain services and responses to attract attackers, allowing the network security team to gather data on attack patterns, tools, and methodologies used by the attackers. This information is crucial for understanding the attack and improving defenses. High-interaction honeypots: Provide a complete environment that can fully engage with attackers, offering more detailed insights but also posing higher risks. Pure honeypots: Essentially full-scale, unmodified systems that an attacker interacts with. Research honeypots: Used primarily for gathering information for research purposes, often involving high-interaction setups.

NEW QUESTION: 228
Which of the following ranges of addresses can be used in the first octet of a Class C network address?

A. 128-191
B. 0-127
C. 192-223
D. 224-255
Answer: C (LEAVE A REPLY)

NEW QUESTION: 229
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. Star
B. Point-to-Point
C. Full Mesh
D. Hub-and-Spoke
Answer: D (LEAVE A REPLY)

NEW QUESTION: 230
Which BC/DR activity includes action taken toward resuming all services that are dependent on business-critical applications?
A. Response
B. Recovery
C. Resumption
D. Restoration
Answer: C (LEAVE A REPLY)
In the context of Business Continuity/Disaster Recovery (BC/DR), the activity that includes actions taken toward resuming all services that are dependent on business-critical applications is referred to as Resumption. This phase focuses on the steps necessary to bring critical functions back into operation after a disruption. Recovery, on the other hand, is more about the actions taken to return the business to normal operating conditions post-disaster, which may include repairs, restorations, and return to normalcy. Response is the immediate reaction to an incident, and Restoration is the process of rebuilding or restoring IT systems and operations.

NEW QUESTION: 231
Which VPN QoS model guarantees the traffic from one customer edge (CE) to another?
A. Pipe Model
B. AAA model
C. Hub-and-Spoke VPN model
D. Hose mode
Answer: (SHOW ANSWER)
The Pipe Model in VPN QoS is designed to guarantee bandwidth between one customer edge (CE) device to another. This model ensures a fixed amount of bandwidth is reserved for the traffic between these two points, providing a consistent and predictable service level. It is particularly

useful in scenarios where a steady and reliable flow of data is critical. The Pipe Model contrasts with the Hose Model, which offers flexible bandwidth allocation based on the total amount of traffic entering and leaving the network, without guaranteeing individual flows between specific CEs.

NEW QUESTION: 232
This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:
It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.
It is commonly used for the following purposes:
a.War driving
b.Detecting unauthorized access points
c.Detecting causes of interference on a WLAN
d.WEP ICV error tracking
e.Making Graphs and Alarms on 802.11 Data, including Signal Strength
This tool is known as _____.
A. NetStumbler
B. THC-Scan
C. Kismet
D. Absinthe
Answer: (SHOW ANSWER)

NEW QUESTION: 233
Stephanie is currently setting up email security so all company data is secured when passed through email. Stephanie first sets up encryption to make sure that a specific user's email is protected. Next, she needs to ensure that the incoming and the outgoing mail has not been modified or altered using digital signatures. What is Stephanie working on?
A. Usability
B. Data Integrity
C. Availability
D. Confidentiality
Answer: B (LEAVE A REPLY)
Stephanie is working on ensuring Data Integrity, which is a critical aspect of information security. It involves maintaining and assuring the accuracy and consistency of data over its entire lifecycle. By setting up digital signatures, Stephanie ensures that the data, in this case, the email content, has not been altered or tampered with during transit. This process provides a means to verify the origin of the message and confirms that the message received is the same as the message sent, thereby safeguarding the integrity of the data.

NEW QUESTION: 234
Which of the following is the best way of protecting important data against virus attack?

A. Implementing a firewall.
B. Using strong passwords to log on to the network.
C. Taking daily backup of data.
D. Updating the anti-virus software regularly.
Answer: (SHOW ANSWER)

NEW QUESTION: 235
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. PING sweep attempt
B. TCP full connect scan attempt
C. TCP null scan attempt
D. ARP scan 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: 236
Which of the following is the standard protocol that provides VPN security at the highest level?
A. PPP
B. None
C. IPSec
D. L2TP
E. P.M
Answer: C (LEAVE A REPLY)

NEW QUESTION: 237
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==0x000
B. Tcp.flags==0000x
C. Tcp.flags==000x0
D. Tcp.flags==x0000

Answer: A (LEAVE A REPLY)
In Wireshark, the filter tcp.flags==0x000 is used to detect TCP packets with no flags set. TCP flags are used to indicate the state of a TCP connection or provide additional information to the receiving party. Common flags include SYN, ACK, RST, FIN, among others. A packet with no flags set (represented as 0x000) could be indicative of a network anomaly or a specific type of attack, such as a reconnaissance or scanning attack. It's important for network administrators like Sam to monitor such packets as they could signify malicious activity on the network.

NEW QUESTION: 238
Which NIST Incident category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service or any combination for later exploit?
A. Malicious code
B. Scans/ Probes/ Attempted Access
C. Denial-of-Service
D. Improper usage
Answer: B (LEAVE A REPLY)
According to NIST guidelines, the incident category that includes activities seeking to access or identify a federal agency computer, open ports, protocols, services, or any combination thereof for later exploitation is categorized as `Scans/Probes/Attempted Access'. This category encompasses any unauthorized attempts to access systems, networks, or data, which may include scanning for vulnerabilities or probing to discover open ports and services.

NEW QUESTION: 239
Which of the following is a credit card-sized device used to securely store personal information and used in conjunction with a PIN number to authenticate users?
A. SD card
B. Java card
C. Proximity card
D. Smart card
Answer: (SHOW ANSWER)

NEW QUESTION: 240
Which of the following protocols is used in wireless networks?
A. CSMA
B. CSMA/CD
C. CSMA/CA
D. ALOHA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 241
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: (SHOW ANSWER)
In Ubuntu, to terminate a specific process, you would use the kill command followed by the signal you want to send and the Process ID (PID) of the target process. The -9 signal is the SIGKILL signal, which forcefully terminates the process. The correct syntax is kill -9 [PID], where [PID] is replaced with the actual numerical ID of the process you wish to terminate.

NEW QUESTION: 242
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 following Wireshark filter(s) will he use to locate the TCP OS fingerprinting attempt? (Choose all that apply.)
A. tcp.options.mss_val<1460
B. tcp.flags=0x00
C. tcp.flags==0x2b
D. tcp.options.wscale_val==20
Answer: (SHOW ANSWER)

NEW QUESTION: 243
Which of the following sets of incident response practices is recommended by the CERT/CC?
A. Prepare, notify, and follow up
B. Prepare, handle, and follow up
C. Notify, handle, and follow up
D. Prepare, handle, and notify
Answer: B (LEAVE A REPLY)

NEW QUESTION: 244
Kelly is taking backups of the organization's data. Currently, she is taking backups of only those files that are created or modified after the last backup. What type of backup is Kelly using?

A. Differential backup
B. Normal backup
C. Full backup
D. Incremental backup
Answer: (SHOW ANSWER)

NEW QUESTION: 245
In which of the following transmission modes is communication bi-directional?
A. Simplex mode
B. Half-duplex mode
C. Root mode
D. Full-duplex mode
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?
A. Automated Field Correlation
B. Field-Based Approach
C. Rule-Based Approach
D. Graph-Based Approach
Answer: B (LEAVE A REPLY)
The Field-Based Approach in event correlation involves systematically checking and comparing all fields for both positive and negative correlations to determine the relationships across one or multiple fields. This approach is methodical and intentional, examining the data within each field and across fields to identify patterns and connections that may indicate security events or incidents.

NEW QUESTION: 247
Which of the following is a free security-auditing tool for Linux?
A. HPing
B. SATAN
C. Nessus
D. SAINT
Answer: (SHOW ANSWER)

NEW QUESTION: 248
Which of the following indicators are discovered through an attacker's intent, their end goal or purpose, and a series of actions that they must take before being able to successfully launch an attack?

A. Indicators of compromise
B. Key risk indicators
C. Indicators of exposure
D. Indicators of attack
Answer: D (LEAVE A REPLY)
Indicators of attack (IoA) provide information about the attacker's intent, end goals, and the actions they take to execute an attack. IoAs help identify the methods and behaviors an attacker uses during the attack lifecycle. Unlike Indicators of Compromise (IoCs), which are used to detect evidence of a breach, IoAs are proactive and help in identifying and preventing potential attacks before they occur by analyzing the patterns and tactics used by attackers. Key risk indicators: Metrics used to signal increased risk exposure. Indicators of compromise: Artifacts observed on a network or in an operating system that with high confidence indicate a computer intrusion.

NEW QUESTION: 249
Which of the following tools is a free laptop tracker that helps in tracking a user's laptop in case it gets stolen?
A. Nessus
B. Snort
C. SAINT
D. Adeona
Answer: (SHOW ANSWER)

NEW QUESTION: 250
Which of the following devices allows wireless communication devices to connect to a wireless network using Wi-Fi, Bluetooth, or related standards?
A. Express card
B. WAP
C. Wireless repeater
D. WNIC
Answer: B (LEAVE A REPLY)

NEW QUESTION: 251
Albert works as a Windows system administrator at an MNC. He uses PowerShell logging to identify any suspicious scripting activity across the network. He wants to record pipeline execution details as PowerShell executes, including variable initialization and command invocations. Which PowerShell logging component records pipeline execution details as PowerShell executes?
A. Module logging
B. Script block logging
C. Event logging
D. Transcript logging
Answer: B (LEAVE A REPLY)

Script block logging is the PowerShell logging component that records the details of pipeline execution as PowerShell executes, including variable initialization and command invocations. This feature is particularly useful for identifying and recording suspicious scripting activity, as it captures the full content of script blocks as they are executed, providing a detailed audit trail. This level of logging is essential for security forensics and understanding the context of commands executed within the PowerShell environment.

NEW QUESTION: 252
Which of the following helps prevent executing untrusted or untested programs or code from untrusted or unverified third-parties?
A. Application sandboxing
B. Deployment of WAFS
C. Application whitelisting
D. Application blacklisting
Answer: A (LEAVE A REPLY)
Application sandboxing is a security mechanism that helps prevent the execution of untrusted or untested programs or code from untrusted or unverified third-parties. It does this by running such programs in a restricted environment, known as a sandbox, where they have limited access to files and system resources. This containment ensures that any malicious code or behavior is isolated from the host system, thereby protecting it from potential harm. Sandboxing is a proactive security measure that can significantly reduce the attack surface and mitigate the risk of security breaches.

NEW QUESTION: 253
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. Extranet-based VPN
B. Intranet-based VPN
C. Remote access VPN
D. PPTP VPN
Answer: A (LEAVE A REPLY)

NEW QUESTION: 254
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. NIDS
C. HIDS
D. DMZ
Answer: (SHOW ANSWER)

NEW QUESTION: 255
If a network is at risk resulting from misconfiguration performed by unskilled and/or unqualified individuals, what type of threat is this?
A. Structured Threats
B. Internal Threats
C. External Threats
D. Unstructured Threats
Answer: D (LEAVE A REPLY)

NEW QUESTION: 256
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. Dictionary Attack
B. Brute Forcing Attack
C. Hybrid Attack
D. Birthday Attack
Answer: D (LEAVE A REPLY)
The Birthday Attack is a type of cryptographic attack that exploits the mathematics behind the birthday problem in probability theory. This attack is relevant to the question as it involves attacking cryptographic hash functions based on the probability of collisions. In the context of hash functions, a collision occurs when two different inputs produce the same hash output. The Birthday Attack leverages the fact that in a set of randomly chosen keys, it is probable that two keys will have the same hash value. This is analogous to the birthday paradox, where in a group of people, there's a high probability that two individuals will share the same birthday. The attack does not rely on the strength or weakness of the hash function itself, but on the statistical likelihood of these collisions occurring, which is surprisingly high even for large sets of possible hash values.

NEW QUESTION: 257
Identify the correct order for a successful black hat operation.

A. Reconnaissance, Gaining Access, Scanning, Maintaining Access, and Covering Tracks
B. Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Covering Tracks
C. Reconnaissance, Scanning, Gaining Access, Covering Tracks, and Maintaining Access
D. Scanning, Reconnaissance, Gaining Access, Maintaining Access, and Covering Tracks
Answer: (SHOW ANSWER)
The correct sequence for a black hat operation follows a structured approach that begins with Reconnaissance, where the attacker gathers preliminary data or intelligence on the target. Next is Scanning, where the attacker uses technical tools to understand the network and system vulnerabilities. Gaining Access is the phase where the vulnerabilities are exploited to enter the system or network. Maintaining Access involves establishing a persistent presence within the system, often for data exfiltration or additional exploitation. Finally, Covering Tracks is the phase where the attacker erases evidence of the intrusion to avoid detection.

NEW QUESTION: 258
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: B (LEAVE A REPLY)
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: 259
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: (SHOW ANSWER)
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: 260
What defines the maximum time period an organization is willing to lose data during a major IT outage event?
A. RPO
B. BC
C. RTO
D. DR
Answer: A (LEAVE A REPLY)
The term that defines the maximum time period an organization is willing to lose data during a major IT outage event is known as the Recovery Point Objective (RPO). RPO is a critical concept in business continuity and disaster recovery planning. It represents the maximum age of the files that an organization must recover from backup storage for normal operations to resume after a disaster. In other words, it's the maximum amount of data loss an organization can tolerate. For instance, if an RPO is set to one hour, the system must be backed up at least every hour so that in case of a system failure, no more than one hour's worth of data is lost.

NEW QUESTION: 261
Which of the following attack signature analysis techniques are implemented to examine the header information and conclude that a packet has been altered?
A. Context-based signature analysis
B. Content-based signature analysis
C. Atomic signature-based analysis
D. Composite signature-based analysis
Answer: D (LEAVE A REPLY)
Composite signature-based analysis is a technique used in intrusion detection systems to examine multiple attributes or behaviors over time to identify potential threats. This method can analyze packet headers to detect anomalies that may indicate a packet has been altered. It looks at a series of packets or fragments to determine if they are part of a legitimate session or if they have been manipulated as part of an attack, such as overlapping fragments which cannot be reassembled properly. This approach is more comprehensive than atomic signature-based analysis, which examines single events or packets in isolation, and provides a more contextual understanding compared to context-based or content-based analyses.

NEW QUESTION: 262
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. Statistical anomaly detection
B. Signature/Pattern matching
C. None of these

D. Stateful protocol analysis

Answer: (SHOW ANSWER)

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: 263

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. Hot site backup

C. Offsite backup

D. Cloud backup

Answer: D (LEAVE A REPLY)

The most appropriate backup method for a company that wants to ensure data encryption and accessibility from any location at any time is cloud backup. Cloud backup solutions provide remote, offsite storage that can be accessed over the internet, which is ideal for ensuring data availability and security. These solutions often include robust encryption protocols to secure data during transfer and while at rest on the cloud servers. This aligns with the need for a backup method that not only encrypts data but also allows for easy access regardless of the user's location.

NEW QUESTION: 264

George was conducting a recovery drill test as a part of his network operation. Recovery drill tests are conducted on the_____.

A. Archived data

B. Deleted data

C. Data in transit

D. Backup data

Answer: D (LEAVE A REPLY)

Recovery drill tests are an essential part of disaster recovery planning. They are conducted on backup data to ensure that the data can be successfully restored in the event of a disaster. During these drills, the backup systems are tested to verify that they function correctly and that the data is intact and recoverable. This process helps organizations prepare for actual disaster scenarios and ensures that their backup solutions are effective and reliable.

NEW QUESTION: 265

Which command list all ports available on a server?
A. sudo apt nst -tunlp
B. sudo netstat -tunlp
C. sudo apt netstate -ls tunlp
D. sudo ntstat -ls tunlp
Answer: (SHOW ANSWER)
The netstat command is used to display network connections, routing tables, interface statistics, masquerade connections, and multicast memberships. To list all ports available on a server, including both TCP and UDP, along with the listening state and associated program names, the -tunlp options are used:
-t shows TCP ports.
-u shows UDP ports.
-n displays addresses and port numbers in numerical form.
-l shows only listening sockets.
-p shows the PID and name of the program to which each socket belongs. Therefore, the command sudo netstat -tunlp effectively lists all ports available on a server with detailed information.

NEW QUESTION: 266
You are an Administrator for a network at an investment bank. You are concerned about individuals breeching your network and being able to steal data before you can detect their presence and shut down their access. Which of the following is the best way to address this issue?
A. Implement network based anti virus.
B. Implement a strong password policy.
C. Implement a strong firewall.
D. Implement a honey pot.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 267
Which of the following is a presentation layer protocol?
A. BGP
B. RPC
C. LWAPP
D. TCP
Answer: C (LEAVE A REPLY)

NEW QUESTION: 268
Which of the following is a service discovery protocol that allows computers and other devices to find services in a local area network without prior configuration?
A. SLP

B. NTP
C. DCAP
D. NNTP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 269
What is the range for private ports?
A. 1024 through 49151
B. Above 65535
C. 49152 through 65535
D. 0 through 1023
Answer: (SHOW ANSWER)

NEW QUESTION: 270
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. Voice recognition voiceprint
B. Facial recognition device
C. Iris camera
D. Fingerprint reader
Answer: (SHOW ANSWER)

NEW QUESTION: 271
What is Azure Key Vault?
A. It is secure storage for the keys used to encrypt data at rest in Azure services
B. It is secure storage for the keys used to encrypt data in motion in Azure services
C. It is secure storage for the keys used to encrypt data in use in Azure services
D. It is secure storage for the keys used to configure IAM in Azure services
Answer: A (LEAVE A REPLY)
Azure Key Vault is a cloud service provided by Microsoft Azure that allows users to securely store and manage sensitive information such as encryption keys, secrets, and certificates. It is designed to safeguard cryptographic keys and other secrets used by cloud applications and services. Azure Key Vault helps ensure that data at rest is protected by providing secure storage for encryption keys, which can be used to encrypt data stored in Azure services. It also supports key management tasks such as creating, importing, rotating, and controlling access to keys, making it an essential tool for managing data security in the cloud.

NEW QUESTION: 272
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)

NEW QUESTION: 273
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. Source Port Address
B. Sequence Number
C. Acknowledgment Number
D. Header Length
Answer: (SHOW ANSWER)

NEW QUESTION: 274
An organization's web server was recently compromised triggering its admin team into action to defend the network. The admin team wants to place the web server in such a way that, even if it is attacked, the other network resources will be unavailable to the attacker. Moreover, the network monitoring will easily detect the future attacks. How can the admin team implement this plan?
A. They can place the web server outside of the organization in a remote place
B. They can remove the web server from their organization
C. They can place it in a separate DMZ area behind the firewall
D. They can place it beside the firewall
Answer: C (LEAVE A REPLY)
Placing the web server in a separate Demilitarized Zone (DMZ) behind the firewall is a security best practice that allows an organization to isolate its public-facing services from the internal network. This setup ensures that if the web server is compromised, the attacker would not have direct access to the internal network resources. Additionally, the DMZ provides a controlled environment where network traffic to and from the web server can be monitored effectively, facilitating the detection of any future attacks. The firewall serves as a barrier, with specific rules

that only allow necessary communication to and from the DMZ, thereby enhancing the overall security posture of the organization.

NEW QUESTION: 275
An IDS or IDPS can be deployed in two modes. Which deployment mode allows the IDS to both detect and stop malicious traffic?
A. passive mode
B. inline mode
C. promiscuous mode
D. firewall mode
Answer: B (LEAVE A REPLY)
The deployment mode that allows an Intrusion Detection System (IDS) or Intrusion Detection and Prevention System (IDPS) to both detect and stop malicious traffic is known as inline mode. In this mode, the IDS/IDPS is placed directly in the network's traffic flow. All traffic must pass through the system, allowing it to inspect packets in real-time and take immediate action to block potential threats before they reach their destination. This contrasts with promiscuous or passive modes, where the system only monitors and alerts on traffic without the ability to intervene directly.

NEW QUESTION: 276
Which of the following is an electronic device that helps in forwarding data packets along networks?
A. Router
B. Hub
C. Repeater
D. Gateway
Answer: A (LEAVE A REPLY)

NEW QUESTION: 277
Which of the following things need to be identified during attack surface visualization?
A. Attacker's tools, techniques, and procedures
B. Authentication, authorization, and auditing in networks
C. Regulatory frameworks, standards and, procedures for organizations
D. Assets, topologies, and policies of the organization
Answer: (SHOW ANSWER)
During attack surface visualization, it is crucial to identify the assets, topologies, and policies of the organization. This involves mapping out all the devices, paths, networks, and understanding the security posture of each asset. By identifying these elements, organizations can determine where vulnerabilities may exist and how an attacker could potentially exploit them. This process helps in prioritizing security efforts and mitigating risks effectively.

NEW QUESTION: 278
Riya bought some clothes and a watch from an online shopping site a few days back. Since then, whenever she accesses any other application (games, browser, etc.) on her mobile, she is spammed with advertisements for clothes and watches similar to the ones she bought. What can be the underlying reason for Riya's situation?
A. Ria's system was infected by Adware
B. Ria's system was infected by Spyware
C. Ria's system was infected by Backdoor
D. Ria's system was infected by Rootkit
Answer: A (LEAVE A REPLY)
Adware is a type of software designed to throw advertisements up on your screen, most often within a web browser. This typically happens when a user installs a free application or software that includes adware in its installation package. In Riya's case, the sudden influx of advertisements for clothes and watches similar to her recent purchases suggests that adware might have been installed on her device. This adware is likely tracking her browsing habits and displaying targeted ads based on her online shopping activity.

NEW QUESTION: 279
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: 280
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: 281
Which of the following standards have been proposed for the improvement of 802.11a and 802.11b wireless local area network (WLAN) specifications, which provides a quality of service (QoS) features, such as the prioritization of data, voice and video transmissions?
A. 802.15
B. 802.11h
C. 802.11n
D. 802.11e
E. None
Answer: (SHOW ANSWER)

NEW QUESTION: 282
In Public Key Infrastructure (PKI), which authority is responsible for issuing and verifying the certificates?
A. Registration authority
B. Certificate authority
C. Digital Certificate authority
D. Digital signature authority
Answer: B (LEAVE A REPLY)
In Public Key Infrastructure (PKI), the Certificate Authority (CA) is responsible for issuing digital certificates. The CA validates entities and binds their public keys with their respective identities through a process of registration and issuance of certificates. This process can be automated or carried out under human supervision. The Registration Authority (RA) often assists the CA by handling the vetting of certificate requests and authenticating the entity making the request, but it does not issue certificates. The CA maintains the integrity of the binding by ensuring that the certificates are issued according to industry norms and best practices, and it also manages the revocation of certificates when necessary.

NEW QUESTION: 283
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: 284
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)

NEW QUESTION: 285
Which among the following options represents professional hackers with an aim of attacking systems for profit?
A. Script kiddies
B. Hacktivists
C. Cyber terrorists
D. Organized hackers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 286
Alex is administrating 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 -o
B. Netstat -a
C. Netstat -ao
D. Netstat -an
Answer: (SHOW ANSWER)
The netstat -an command is used to display all active connections and listening ports with addresses and port numbers in numerical form. This is particularly useful for administrators who need to quickly identify connections without resolving the hostnames, which can save time and resources, especially when dealing with a large number of connections.

NEW QUESTION: 287
Which of the following interfaces uses hot plugging technique to replace computer components without the need to shut down the system?
A. SATA
B. SCSI
C. IDE
D. SDRAM
Answer: A (LEAVE A REPLY)
The hot plugging technique allows for the replacement of computer components without the need to shut down the system. SATA (Serial Advanced Technology Attachment) is known for supporting hot plugging, which is particularly useful for hard drives and solid-state drives. This feature enables users to connect or disconnect the device while the system is running without risking data loss or damage. SCSI (Small Computer System Interface) also supports hot plugging for some devices, but SATA is more commonly associated with this capability for consumer-level computer components.

NEW QUESTION: 288
Which of the following encryption techniques do digital signatures use?
A. IDEA
B. MD5
C. RSA
D. Blowfish
Answer: B (LEAVE A REPLY)

NEW QUESTION: 289
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: 290
Which phase of vulnerability management deals with the actions taken for correcting the discovered vulnerability?
A. Mitigation
B. Assessment
C. Remediation
D. Verification
Answer: (SHOW ANSWER)
The phase of vulnerability management that deals with the actions taken for correcting the discovered vulnerability is known as Remediation. This phase involves the actual fixing or patching of the vulnerabilities to reduce the risk of exploitation. Remediation can include applying patches, making configuration changes, or implementing compensating controls. It is a critical step in the vulnerability management lifecycle, which ensures that the identified vulnerabilities are addressed to protect the network from potential attacks.

NEW QUESTION: 291
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 planning
C. Incident management
D. Incident handling
Answer: A (LEAVE A REPLY)

NEW QUESTION: 292
In _____ mechanism, the system or application sends log records either on the local disk or over the network.
A. Network-based
B. Pull-based
C. Push-based
D. Host-based
Answer: C (LEAVE A REPLY)

In a push-based mechanism, the system or application actively sends log records to a designated storage location, which can be on the local disk or over the network. This is in contrast to a pull-based mechanism, where the log records are retrieved by a separate process. The push-based approach ensures that log records are sent immediately and consistently, which is crucial for real-time monitoring and analysis.

NEW QUESTION: 293
Which of the following represents a network that connects two or more LANs in the same geographic area?
A. WAN
B. MAN
C. PAN
D. SAN
Answer: B (LEAVE A REPLY)

NEW QUESTION: 294
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 network.

NEW QUESTION: 295
Fill in the blank with the appropriate term. The _____is an application layer protocol that is used between workstations and routers for transporting SNA/NetBIOS traffic over TCP sessions.
Answer:
DCAP

NEW QUESTION: 296
Which of the following is a distributed multi-access network that helps in supporting integrated communications using a dual bus and distributed queuing?
A. Logical Link Control
B. Token Ring network
C. Distributed-queue dual-bus
D. CSMA/CA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 297
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: 298
A network is setup using an IP address range of 0.0.0.0 to 127.255.255.255. The network has a default subnet mask of 255.0.0.0. What IP address class is the network range a part of?
A. Class C
B. Class A
C. Class B
D. Class D
Answer: (SHOW ANSWER)
The IP address range from 0.0.0.0 to 127.255.255.255 falls under Class A. In the Class A type of network, the first octet (the first 8 bits of the IP address) is used for the network part, and the remaining 24 bits are used for host addresses. The default subnet mask for Class A is 255.0.0.0, which aligns with the given network's default subnet mask. Class A networks are designed to support a very large number of hosts. The first bit of a Class A address is always set to 0, which means the first octet can range from 1 to 127, thus including the given IP address range.

NEW QUESTION: 299

Individuals in the organization using system resources in a way that violates acceptable usage policies indicates which of the following security incident(s):
A. Unauthorized Access
B. Denial-of-Service (DoS)
C. Malicious Code
D. Improper Usage
Answer: D (LEAVE A REPLY)

NEW QUESTION: 300
John works as an Ethical Hacker for www.company.com Inc. He wants to find out the ports that are open in www.company.com's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?
A. Xmas tree
B. TCP SYN/ACK
C. TCP SYN
D. TCP FIN
Answer: C (LEAVE A REPLY)

NEW QUESTION: 301
Which of the following applications is used for the statistical analysis and reporting of the log files?
A. Sniffer
B. Sawmill
C. Snort
D. jplag
Answer: B (LEAVE A REPLY)

NEW QUESTION: 302
Which of the following is the primary international body for fostering cooperative standards for telecommunications equipment and systems?
A. NIST

B. IEEE
C. ICANN
D. CCITT
Answer: (SHOW ANSWER)

NEW QUESTION: 303
Adam works as a Professional Penetration Tester. A project has been assigned to him to test the vulnerabilities of the CISCO Router of Umbrella Inc. Adam finds out that HTTP Configuration Arbitrary Administrative Access Vulnerability exists in the router. By applying different password cracking tools, Adam gains access to the router. He analyzes the router config file and notices the following lines:
logging buffered errors
logging history critical
logging trap warnings
logging 10.0.1.103
By analyzing the above lines, Adam concludes that this router is logging at log level 4 to the syslog server 10.0.1.103. He decides to change the log level from 4 to 0.
Which of the following is the most likely reason of changing the log level?
A. Changing the log level from 4 to 0 will result in the termination of logging.
This way the modification in the router is not sent to the syslog server.
B. Changing the log level grants access to the router as an Administrator.
C. Changing the log level from 4 to 0 will result in the logging of only emergencies.
This way the modification in the router is not sent to the syslog server.
D. By changing the log level, Adam can easily perform a SQL injection attack.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 304
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 congestion.

NEW QUESTION: 305
How can organizations obtain information about threats through human intelligence?
A. By extracting information from security blogs and forums
B. By discovering vulnerabilities through exploration, understanding malware behavior through malware processing, etc.
C. From the data of past incidents and network monitoring
D. From attackers through the dark web and honeypots
Answer: (SHOW ANSWER)
Human intelligence (HUMINT) in the context of network defense involves the collection of information from human sources. This can include extracting insights from security blogs, forums, and other platforms where cybersecurity professionals and enthusiasts discuss vulnerabilities, threats, and incidents. By monitoring these discussions, organizations can gain valuable information about emerging threats, techniques used by attackers, and potential security weaknesses that need to be addressed.

NEW QUESTION: 306
Which encryption algorithm does S/MIME protocol implement for digital signatures in emails?
A. Rivest-Shamir-Adleman encryption
B. Digital Encryption Standard
C. Triple Data Encryption Standard
D. Advanced Encryption Standard
Answer: A (LEAVE A REPLY)
S/MIME (Secure/Multipurpose Internet Mail Extensions) protocol implements the Rivest-Shamir-Adleman (RSA) encryption algorithm for digital signatures in emails. Digital signatures are a key component of S/MIME, providing authentication, message integrity, and non-repudiation. RSA is a widely used public-key cryptosystem that facilitates secure data transmission and is known for its role in digital signatures. It works on the principle of asymmetric cryptography, where a pair of keys is used: a public key, which is shared openly, and a private key, which is kept secret by the owner. In the context of S/MIME, the sender's email client uses the sender's private key to create a digital signature, and the recipient's email client uses the sender's public key to verify the signature.

NEW QUESTION: 307
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. XSS
B. DDoS
C. XCRF
D. Sniffing
Answer: (SHOW ANSWER)

The type of attack that is used to hack an IoT device and direct large amounts of network traffic toward a web server, causing it to overload with connections and preventing any new connections, is known as a Distributed Denial of Service (DDoS) attack. In a DDoS attack, multiple compromised computer systems, which can include IoT devices, are used to target a single system causing a Denial of Service (DoS) attack. These attacks can overwhelm the target with a flood of internet traffic, which can lead to the server being unable to process legitimate requests, effectively taking it offline.

NEW QUESTION: 308
Which wireless networking topology setup requires same channel name and SSID?
A. Ad-Hoc standalone network architecture
B. Infrastructure network topology
C. Hybrid topology
D. Mesh topology
Answer: B (LEAVE A REPLY)
In an infrastructure network topology, all wireless devices communicate through an access point/base station. The access point serves as the central transmitter and receiver of wireless radio signals. Mainstream wireless APs support the configuration of the same channel name (frequency) and SSID (Service Set Identifier) to facilitate seamless communication between devices. This setup is essential for devices to identify and connect to the correct network, especially in environments where multiple networks may overlap.

NEW QUESTION: 309
Maximus Tech is a multinational company that uses Cisco ASA Firewalls for their systems. Jason is the one of the members of the team that checks the logs at Maximus Tech. As a part of his job, he is going through the logs and he came across a firewall log that looks like this:
May 06 2018 21:27:27 asa 1: % ASA -5 - 11008: User 'enable_15' executed the 'configure term' command Based on the security level mentioned in the log, what did Jason understand about the description of this message?
A. Warning condition message
B. Critical condition message
C. Normal but significant message
D. Informational message
Answer: D (LEAVE A REPLY)
The log entry %ASA-6-11008 indicates that the message is of a severity level 6, which corresponds to an informational message. In the context of Cisco ASA Firewall logs, severity levels range from 0 (emergency) to 7 (debugging), with lower numbers indicating higher severity. A severity level of 6 is used for messages that provide information about normal but significant events. In this case, the log indicates that a user named `enable_16' executed the `configure term' command, which is a noteworthy event but does not indicate an error or critical condition.

NEW QUESTION: 310
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. Centrally assign Windows PC group policies
B. Dedicate a partition on HDD and format the disk using NTFS
C. Download and install latest patches and enable Windows Automatic Updates
D. Install antivirus software and turn off unnecessary services
Answer: (SHOW ANSWER)
To ensure that Windows PCs are up-to-date and have fewer internal security flaws, Byron should focus on regularly applying the latest security patches and updates. This can be achieved by: Downloading and installing the latest patches: Ensures that any vulnerabilities identified in the operating system and applications are fixed promptly.
Enabling Windows Automatic Updates: Automates the process of checking for and installing updates, ensuring that PCs are always protected with the most current security measures. Regularly updating the system helps in closing security loopholes that could be exploited by attackers. Antivirus software and turning off unnecessary services (Option A) are also important, but they do not address the critical need for regular patching. Centrally assigning group policies (Option B) is useful for managing security settings but does not directly address updating and patching. Dedicating a partition and formatting with NTFS (Option D) is unrelated to keeping systems up-to- date.

NEW QUESTION: 311
Which of the following is a software tool used in passive attacks for capturing network traffic?
A. Warchalking
B. Intrusion detection system
C. Sniffer
D. Intrusion prevention system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 312
You are monitoring your network traffic with the Wireshark utility and noticed that your network is experiencing a large amount of traffic from a certain region. You suspect a DoS incident on the network. What will be your first reaction as a first responder?
A. Avoid Fear, Uncertainty and Doubt
B. Communicate the incident
C. Make an initial assessment
D. Disable Virus Protection
Answer: C (LEAVE A REPLY)
As a first responder to a suspected DoS incident, the initial reaction should be to make an initial assessment. This involves quickly evaluating the situation to understand the scope and impact of the incident. An initial assessment helps in determining whether the unusual traffic is indeed a

DoS attack or a false positive. It also aids in deciding the next steps, such as whether to escalate the incident, what resources are required, and how to communicate the issue to relevant stakeholders.

NEW QUESTION: 313
In which of the following transmission modes is communication uni-directional?
A. Root mode
B. Full-duplex mode
C. Simplex mode
D. Half-duplex mode
Answer: C (LEAVE A REPLY)

NEW QUESTION: 314
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. Eavesdropping
B. False message
C. Message replay
D. Message digest
E. Message repudiation
F. Message modification
G. Identity theft
Answer: A,B,C,E,F,G (LEAVE A REPLY)

NEW QUESTION: 315
Which protocol could choose the network administrator for the wireless network design, if he need to satisfied the minimum requirement of 2.4 GHz, 22 MHz of bandwidth, 2 Mbits/s stream for data rate and use DSSS for modulation.
A. 802.11g
B. 802.11b
C. 802.11n
D. 802.11a
Answer: B (LEAVE A REPLY)

NEW QUESTION: 316
An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?
A. Install a CCTV with cameras pointing to the entrance doors and the street
B. Use fences in the entrance doors
C. Use lights in all the entrance doors and along the company's perimeter

D. Use an IDS in the entrance doors and install some of them near the corners

Answer: A (LEAVE A REPLY)

The best option for 24-hour monitoring of the physical perimeter and entrance doors is to install a CCTV system. CCTV cameras serve as both a deterrent to unauthorized entry and a means of surveillance to monitor activities. They can be positioned to cover the entrance doors and the street, providing a broad view of the area that needs to be secured. This aligns with the principles of intrusion detection and prevention, which include deterrence through visible security measures like cameras, and detection through continuous monitoring.

NEW QUESTION: 317

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: (SHOW ANSWER)

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: 318

Which of the following protocols sends a jam signal when a collision is detected?

A. CSMA

B. ALOHA

C. CSMA/CA

D. CSMA/CD

Answer: D (LEAVE A REPLY)

NEW QUESTION: 319
Fill in the blank with the appropriate term.
The_____ model is a description framework for computer network protocols and is sometimes called the Internet Model or the DoD Model.
Answer:
TCP/IP

NEW QUESTION: 320
Which of the following standards defines Logical Link Control (LLC)?
A. 802.5
B. 802.4
C. 802.3
D. 802.2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 321
Identify the attack where an attacker manipulates or tricks people into revealing their confidential details like bank account information, credit card details, etc.?
A. Social Engineering Attacks
B. Port Scanning
C. DNS Footprinting
D. ICMP Scanning
Answer: (SHOW ANSWER)
The attack described in the question is a Social Engineering Attack. This type of attack involves manipulating or deceiving people into divulging confidential information such as bank account details, credit card numbers, and other sensitive data. Social engineering attacks exploit human psychology rather than technical hacking techniques to gain access to systems, networks, or physical locations, or for financial gain. Attackers may use various tactics such as phishing, pretexting, baiting, or tailgating to trick individuals into providing the information they seek1.

NEW QUESTION: 322
What is the range for registered ports?
A. Above 65535
B. 49152 through 65535
C. 0 through 1023
D. 1024 through 49151
Answer: (SHOW ANSWER)

NEW QUESTION: 323
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: 324
Which of the following is a passive attack?
A. Replay attack
B. Traffic analysis
C. Session hijacking
D. Unauthorized access
Answer: B (LEAVE A REPLY)

NEW QUESTION: 325
Which firewall technology provides the best of both packet filtering and application-based filtering and is used in Cisco Adaptive Security Appliances?
A. Stateful multilayer inspection
B. Application-level gateway
C. VPN
D. Network address translation
Answer: A (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: 326

Which of the following is a network interconnectivity device that translates different communication protocols and is used to connect dissimilar network technologies?

A. Switch

B. Router

C. Bridge

D. Gateway

Answer: D (LEAVE A REPLY)

NEW QUESTION: 327

Rosa is working as a network defender at Linda Systems. Recently, the company migrated from Windows to MacOS. Rosa wants to view the security related logs of her system, where can she find these logs?

A. /Library/Logs/Sync

B. /private/var/log

C. /var/log/cups/access_log

D. ~/Library/Logs

Answer: B (LEAVE A REPLY)

In MacOS, security-related logs are typically stored in the /private/var/log directory. This location is used to store various system logs, including authentication attempts and other security events. The secure.log file within this directory is particularly relevant for tracking security incidents, as it records authentication attempts and other security-related events. It's important for network defenders like Rosa to be familiar with these log locations to monitor and respond to potential security issues on the systems they manage.