CompTIA.SY0-601.v2023-10-18.q228

Exam Code:	SY0-601
Exam Name:	CompTIA Security+ Exam
Certification Provider:	CompTIA
Free Question Number:	228
Version:	v2023-10-18
# of views:	1367
# of Questions views:	2280
https://www.freepdfdumps.com/CompTIA.SY0-601.v2023-10-18.q228.html	

NEW QUESTION: 1
An organization recently released a zero-trust policy that will enforce who is able to remotely access certain dat a. Authenticated users who access the data must have a need to know, depending on their level of permissions.
Which of the following is the first step the organization should take when implementing the policy?
A. Determine a quality CASB solution.
B. Configure the DLP policies by user groups.
C. Implement agentless NAC on boundary devices.
D. Classify all data on the file servers.
Answer: (SHOW ANSWER)
zero trust is a security strategy that assumes breach and verifies each request as though it originates from an untrusted network12. A zero trust policy is a set of "allow rules" that specify conditions for accessing certain resources3.
According to one source4, the first step in implementing a zero trust policy is to identify and classify all data and assets in the organization. This helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.
Classifying all data on the file servers is the first step in implementing a zero trust policy because it helps to determine the level of sensitivity and risk associated with each resource and apply appropriate access controls.

NEW QUESTION: 2
Which of the following is the correct order of evidence from most to least volatile in forensic analysis?
A. Memory, disk, temporary filesystems, CPU cache
B. CPU cache, memory, disk, temporary filesystems
C. CPU cache, memory, temporary filesystems, disk
D. CPU cache, temporary filesystems, memory, disk
Answer: C (LEAVE A REPLY)
The correct order of evidence from most to least volatile in forensic analysis is based on how quickly the evidence can be lost or altered if not collected or preserved properly. CPU cache is the most volatile type of evidence because it is stored in a small amount of memory on the processor and can be overwritten or erased very quickly. Memory is the next most volatile type of

evidence because it is stored in RAM and can be lost when the system is powered off or rebooted. Temporary filesystems are less volatile than memory because they are stored on disk, but they can still be deleted or overwritten by other processes or users. Disk is the least volatile type of evidence because it is stored on permanent storage devices and can be recovered even after deletion or formatting, unless overwritten by new data. Reference: https://www.comptia.org/blog/what-is-volatility-in-digital-forensics

NEW QUESTION: 3
A company's help desk has received calls about the wireless network being down and users being unable to connect to it The network administrator says all access points are up and running One of the help desk technicians notices the affected users are working in a building near the parking lot. Which of the following is the most likely reason for the outage?
A. Someone near the building is jamming the signal
B. A user has set up a rogue access point near the building
C. Someone set up an evil twin access point in the affected area.
D. The APs in the affected area have been unplugged from the network
Answer: A (LEAVE A REPLY)
Jamming is a type of denial-of-service attack that involves interfering with or blocking the wireless signal using a device that emits radio waves at the same frequency as the wireless network. It can cause the wireless network to be down and users to be unable to connect to it, especially if they are working in a building near the parking lot where someone could easily place a jamming device.

NEW QUESTION: 4
A security analyst has received several reports of an issue on an internal web application. Users state they are having to provide their credentials twice to log in. The analyst checks with the application team and notes this is not an expected behavior. After looking at several logs, the analyst decides to run some commands on the gateway and obtains the following output:
Which of the following BEST describes the attack the company is experiencing?
A. MAC flooding
B. URL redirection
C. ARP poisoning
D. DNS hijacking
Answer: (SHOW ANSWER)
The output of the "netstat -ano" command shows that there are two connections to the same IP address and port number. This indicates that there are two active sessions between the client and server.
The issue of users having to provide their credentials twice to log in is known as a double login prompt issue. This issue can occur due to various reasons such as incorrect configuration of authentication settings, incorrect configuration of web server settings, or issues with the client's browser.
Based on the output of the "netstat -ano" command, it is difficult to determine the exact cause of the issue. However, it is possible that an attacker is intercepting traffic between the client and server and stealing user credentials. This type of attack is known as C. ARP poisoning.
ARP poisoning is a type of attack where an attacker sends fake ARP messages to associate their MAC address with the IP address of another device on the network. This allows them to intercept traffic between the two devices and steal sensitive information such as user credentials.

NEW QUESTION: 5
A security analyst is reviewing computer logs because a host was compromised by malware After the computer was infected it displayed an error screen and shut down. Which of the following should the analyst review first to determine more information?
A. Dump file
B. System log
C. Web application log
D. Security too
Answer: A (LEAVE A REPLY)
A dump file is the first thing that a security analyst should review to determine more information about a compromised device that displayed an error screen and shut down. A dump file is a file that contains a snapshot of the memory contents of a device at the time of a system crash or error. A dump file can help a security analyst analyze the cause and source of the crash or error, as well as identify any malicious code or activity that may have triggered it.

NEW QUESTION: 6
A cybersecurity analyst needs to adopt controls to properly track and log user actions to an individual. Which of the following should the analyst implement?
A. Non-repudiation
B. Baseline configurations
C. MFA
D. DLP
Answer: (SHOW ANSWER)
Non-repudiation is the process of ensuring that a party involved in a transaction or communication cannot deny their involvement. By implementing non-repudiation controls, a cybersecurity analyst can properly track and log user actions, attributing them to a specific individual. This can be achieved through methods such as digital signatures, timestamps, and secure logging mechanisms.
Reference:
1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/CompTIA%20Security%2B%20SY0-601%20Exam%20Objectives.pdf
2. Stewart, J. M., Chapple, M., & Gibson, D. (2021). CompTIA Security+ Study Guide: Exam SY0-601. John Wiley & Sons.

NEW QUESTION: 7
A company wants to enable BYOD for checking email and reviewing documents. Many of the documents contain sensitive organizational information. Which of the following should be deployed first before allowing the use of personal devices to access company data?
A. MDM
B. RFID
C. DLR
D. SIEM
Answer: (SHOW ANSWER)

MDM stands for Mobile Device Management, which is a solution that can be used to manage and secure personal devices that access company data. MDM can enforce policies and rules, such as password protection, encryption, remote wipe, device lock, application control, and more. MDM can help a company enable BYOD (Bring Your Own Device) while protecting sensitive organizational information.

NEW QUESTION: 8
Which of the following terms should be included in a contract to help a company monitor the ongo-ing security maturity Of a new vendor?
A. A right-to-audit clause allowing for annual security audits
B. Requirements for event logs to kept for a minimum of 30 days
C. Integration of threat intelligence in the companys AV
D. A data-breach clause requiring disclosure of significant data loss
Answer: A (LEAVE A REPLY)
A right-to-audit clause is a contractual provision that allows one party to audit the records and activities of another party to ensure compliance with security policies and standards. It can help a company monitor the ongoing security maturity of a new vendor by conducting annual security audits and identifying any gaps or issues that need to be addressed.

NEW QUESTION: 9
Which of the following can reduce vulnerabilities by avoiding code reuse?
A. Memory management
B. Stored procedures
C. Normalization
D. Code obfuscation
Answer: A (LEAVE A REPLY)
Memory management is a technique that can allocate and deallocate memory for applications and processes. Memory management can reduce vulnerabilities by avoiding code reuse, which is a technique that exploits a memory corruption vulnerability to execute malicious code that already exists in memory. Memory management can prevent code reuse by implementing features such as address space layout randomization (ASLR), data execution prevention (DEP), or stack canaries.

NEW QUESTION: 10
A user attempts to load a web-based application, but the expected login screen does not appear A help desk analyst troubleshoots the issue by running the following command and reviewing the output on the user's PC
The help desk analyst then runs the same command on the local PC
Which of the following BEST describes the attack that is being detected?
A. Domain hijacking
B. DNS poisoning
C. MAC flooding
D. Evil twin
Answer: (SHOW ANSWER)
DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect

result record, such as an IP address. This results in traffic being diverted to the attacker's computer (or any other malicious destination).
DNS poisoning can be performed by various methods, such as:
Intercepting and forging DNS responses from legitimate servers
Compromising DNS servers and altering their records
Exploiting vulnerabilities in DNS protocols or implementations
Sending malicious emails or links that trigger DNS queries with poisoned responses According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:
"DNS poisoning, also known as DNS spoofing or DNS cache poisoning, is a form of computer security hacking in which corrupt Domain Name System (DNS) data is introduced into the DNS resolver's cache, causing the name server to return an incorrect result record."

NEW QUESTION: 11
Multiple beaconing activities to a malicious domain have been observed. The malicious domain is hosting malware from various endpoints on the network. Which of the following technologies would be best to correlate the activities between the different endpoints?
A. Firewall
B. SIEM
C. IPS
D. Protocol analyzer
Answer: (SHOW ANSWER)
SIEM stands for Security Information and Event Management, which is a technology that collects, analyzes, and correlates data from multiple sources, such as firewall logs, IDS/IPS alerts, network devices, applications, and endpoints. SIEM provides real-time monitoring and alerting of security events, as well as historical analysis and reporting for compliance and forensic purposes. A SIEM technology would be best to correlate the activities between the different endpoints that are beaconing to a malicious domain. A SIEM can detect the malicious domain by comparing it with threat intelligence feeds or known indicators of compromise (IOCs). A SIEM can also identify the endpoints that are communicating with the malicious domain by analyzing the firewall logs and other network traffic data. A SIEM can alert the security team of the potential compromise and provide them with relevant information for investigation and remediation.

NEW QUESTION: 12
Which of the following best describes the situation where a successfully onboarded employee who is using a fingerprint reader is denied access at the company's mam gate?
A. Crossover error rate
B. False match raw
C. False rejection
D. False positive
Answer: C (LEAVE A REPLY)
False rejection Short A false rejection occurs when a biometric system fails to recognize an authorized user and denies access. This can happen due to poor quality of the biometric sample, environmental factors, or system errors. Reference: https://www.comptia.org/blog/what-is-biometrics

NEW QUESTION: 13
A manager for the development team is concerned about reports showing a common set of vulnerabilities. The set of vulnerabilities is present on almost all of the applications developed by the team. Which of the following approaches would be most effective for the manager to use to address this issue?
A. Tune the accuracy of fuzz testing.
B. Invest in secure coding training and application security guidelines.
C. Increase the frequency of dynamic code scans 1o detect issues faster.
D. Implement code signing to make code immutable.
Answer: (SHOW ANSWER)
Invest in secure coding training and application security guidelines is the most effective approach for the manager to use to address the issue of common vulnerabilities in the applications developed by the team. Secure coding training can help the developers learn how to write code that follows security best practices and avoids common mistakes or flaws that can introduce vulnerabilities. Application security guidelines can provide a set of standards and rules for developing secure applications that meet the company's security requirements and policies. By investing in secure coding training and application security guidelines, the manager can improve the security awareness and skills of the development team and reduce the number of vulnerabilities in their applications. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, Objective 2.3: Summarize secure application development, deployment, and automation concepts 2 CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 3 https://www.comptia.org/blog/what-is-secure-coding

NEW QUESTION: 14
The technology department at a large global company is expanding its Wi-Fi network infrastructure at the headquarters building Which of the following should be closely coordinated between the technology, cybersecurity, and physical security departments?
A. Authentication protocol
B. Encryption type
C. WAP placement
D. VPN configuration
Answer: C (LEAVE A REPLY)
WAP stands for wireless access point, which is a device that allows wireless devices to connect to a wired network using Wi-Fi or Bluetooth. WAP placement refers to where and how WAPs are installed in a building or area.
WAP placement should be closely coordinated between the technology, cybersecurity, and physical security departments because it affects several aspects of network performance and security, such as:
Coverage: WAP placement determines how well wireless devices can access the network throughout the building or area. WAPs should be placed in locations that provide optimal signal strength and avoid interference from other sources.
Capacity: WAP placement determines how many wireless devices can connect to the network simultaneously without affecting network speed or quality. WAPs should be placed in locations that balance network load and avoid congestion or bottlenecks.
Security: WAP placement determines how vulnerable wireless devices are to eavesdropping or hacking attacks from outside or inside sources. WAPs should be placed in locations that minimize exposure to unauthorized access and maximize encryption and authentication methods.

NEW QUESTION: 15
Which of the following describes a maintenance metric that measures the average time required to troubleshoot and restore failed equipment?
A. RTO
B. MTBF
C. MTTR
D. RPO
Answer: C (LEAVE A REPLY)
Mean Time To Repair (MTTR) is a maintenance metric that measures the average time required to troubleshoot and restore failed equipment. Reference: CompTIA Security+ Certification Exam Objectives - 4.6 Explain the importance of secure coding practices. Study Guide: Chapter 7, page 323.

NEW QUESTION: 16
A security analyst is responding to an alert from the SIEM. The alert states that malware was discovered on a host and was not automatically deleted. Which of the following would be BEST for the analyst to perform?
A. Add a deny-all rule to that host in the network ACL
B. Implement a network-wide scan for other instances of the malware.
C. Quarantine the host from other parts of the network
D. Revoke the client's network access certificates
Answer: (SHOW ANSWER)
When malware is discovered on a host, the best course of action is to quarantine the host from other parts of the network. This prevents the malware from spreading and potentially infecting other hosts. Adding a deny-all rule to the host in the network ACL may prevent legitimate traffic from being processed, implementing a network-wide scan is time-consuming and may not be necessary, and revoking the client's network access certificates is an extreme measure that may not be warranted. Reference: CompTIA Security+ Study Guide, pages 113-114

NEW QUESTION: 17
A security investigation revealed mat malicious software was installed on a server using a server administrator credentials. During the investigation the server administrator explained that Telnet was regularly used to log in. Which of the blowing most likely occurred?
A. A spraying attack was used to determine which credentials to use
B. A packet capture tool was used to steal the password
C. A remote-access Trojan was used to install the malware

D. A directory attack was used to log in as the server administrator

Answer: (SHOW ANSWER)

Telnet is an insecure protocol that transmits data in cleartext over the network. This means that anyone who can intercept the network traffic can read the data, including the username and password of the server administrator. A packet capture tool is a software or hardware device that can capture and analyze network packets. An attacker can use a packet capture tool to steal the password and use it to install malicious software on the server. Reference: https://www.comptia.org/content/guides/what-is-network-security

NEW QUESTION: 18

A company has discovered unauthorized devices are using its WiFi network, and it wants to harden the access point to improve security. Which f the following configuration should an analysis enable To improve security? (Select TWO.)

A. RADIUS

B. PEAP

C. WPS

D. WEP-EKIP

E. SSL

F. WPA2-PSK

Answer: (SHOW ANSWER)

To improve the security of the WiFi network and prevent unauthorized devices from accessing the network, the configuration options of RADIUS and WPA2-PSK should be enabled. RADIUS (Remote Authentication Dial-In User Service) is an authentication protocol that can be used to control access to the WiFi network. It can provide stronger authentication and authorization than WEP and WPA. WPA2-PSK (WiFi Protected Access 2 with Pre-Shared Key) is a security protocol that uses stronger encryption than WEP and WPA. It requires a pre-shared key (PSK) to be entered on each device that wants to access the network. This helps prevent unauthorized devices from accessing the network.

NEW QUESTION: 19

If a current private key is compromised, which of the following would ensure it cannot be used to decrypt ail historical data?

A. Perfect forward secrecy

B. Elliptic-curve cryptography

C. Key stretching

D. Homomorphic encryption

Answer: A (LEAVE A REPLY)

Perfect forward secrecy would ensure that it cannot be used to decrypt all historical data. Perfect forward secrecy (PFS) is a security protocol that generates a unique session key for each session between two parties. This ensures that even if one session key is compromised, it cannot be used to decrypt other sessions.

NEW QUESTION: 20

A global company is experiencing unauthorized logging due to credential theft and account lockouts caused by brute-force attacks. The company is considering implementing a third-party identity provider to help mitigate these attacks. Which of the following would be the BEST control for the company to require from prospective vendors?

A. IP restrictions

B. Multifactor authentication
C. A banned password list
D. A complex password policy
Answer: B (LEAVE A REPLY)
Multifactor authentication (MFA) would be the best control to require from a third-party identity provider to help mitigate attacks such as credential theft and brute-force attacks. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 2

NEW QUESTION: 21
Which of the following BEST describes the method a security analyst would use to confirm a file that is downloaded from a trusted security website is not altered in transit or corrupted using a verified checksum?
A. Hashing
B. Salting
C. Integrity
D. Digital signature
Answer: A (LEAVE A REPLY)
Hashing is a cryptographic function that produces a unique fixed-size output (i.e., hash value) from an input (i.e., data). The hash value is a digital fingerprint of the data, which means that if the data changes, so too does the hash value. By comparing the hash value of the downloaded file with the hash value provided by the security website, the security analyst can verify that the file has not been altered in transit or corrupted.

NEW QUESTION: 22
A company is adopting a BYOD policy and is looking for a comprehensive solution to protect company information on user devices. Which of the following solutions would best support the policy?
A. Mobile device management
B. Full device encryption
C. Remote wipe
D. Biometrics
Answer: (SHOW ANSWER)
Mobile device management (MDM) is a solution that allows an organization to manage, monitor, and secure mobile devices that are used by employees for work purposes. It can protect company information on user devices by enforcing policies and controls such as encryption, password, remote wipe, etc., and detecting and preventing unauthorized access or data leakage.

NEW QUESTION: 23
Which of the following environments typically hosts the current version configurations and code, compares user-story responses and workflow, and uses a modified version of actual data for testing?
A. Development
B. Staging
C. Production
D. Test
Answer: B (LEAVE A REPLY)

Staging is an environment in the software development lifecycle that is used to test a modified version of the actual data, current version configurations, and code. This environment compares user-story responses and workflow before the software is released to the production environment. Reference: CompTIA Security+ Study Guide, Sixth Edition, Sybex, pg. 496

NEW QUESTION: 24
An organization would like to remediate the risk associated with its cloud service provider not meeting its advertised 99.999% availability metrics. Which of the following should the organization consult for the exact requirements for the cloud provider?
A. SLA
B. BPA
C. NDA
D. MOU
Answer: A (LEAVE A REPLY)
The Service Level Agreement (SLA) is a contract between the cloud service provider and the organization that stipulates the exact requirements for the cloud provider. It outlines the level of service that the provider must deliver, including the minimum uptime percentage, support response times, and the remedies and penalties for failing to meet the agreed-upon service levels.

NEW QUESTION: 25
A company's help desk received several AV alerts indicating Mimikatz attempted to run on the remote systems Several users also reported that the new company flash drives they picked up in the break room only have 512KB of storage Which of the following is most likely the cause?
A. The GPO prevents the use of flash drives, which triggers a false positive AV indication and restricts the drives to only 512KB of storage
B. The new flash drives need a driver that is being blocked by the AV software because the flash drives are not on the application's allow list, temporarily restricting the drives to 512KB of storage.
C. The new flash drives are incorrectly partitioned, and the systems are automatically trying to use an unapproved application to repartition the drives.
D. The GPO blocking the flash drives is being bypassed by a malicious flash drive that is attempting to harvest plaintext credentials from memory.
Answer: D (LEAVE A REPLY)
Mimikatz is a tool that can extract plaintext credentials from memory on Windows systems. A malicious flash drive can bypass the GPO blocking the flash drives by using techniques such as autorun.inf or HID spoofing to execute Mimikatz on the target system without user interaction or consent. This can cause AV alerts indicating Mimikatz attempted to run on the remote systems and also reduce the storage capacity of the flash drives to only 512KB by creating hidden partitions or files on them.

NEW QUESTION: 26
A police department is using the cloud to share information city officials Which of the cloud models describes this scenario?
A. Hybrid
B. private
C. pubic
D. Community
Answer: D (LEAVE A REPLY)

A community cloud model describes a scenario where a cloud service is shared among multiple organizations that have common goals, interests, or requirements. A community cloud can be hosted by one of the organizations, a third-party provider, or a combination of both. A community cloud can offer benefits such as cost savings, security, compliance, and collaboration. A police department using the cloud to share information with city officials is an example of a community cloud model.

NEW QUESTION: 27
A network administrator needs to determine the sequence of a server farm's logs. Which of the following should the administrator consider? (Select two).
A. Chain of custody
B. Tags
C. Reports
D. Time stamps
E. Hash values
F. Time offset
Answer: D,F (LEAVE A REPLY)
A server farm's logs are records of events that occur on a group of servers that provide the same service or function. Logs can contain information such as date, time, source, destination, message, error code, and severity level. Logs can help administrators monitor the performance, security, and availability of the servers and troubleshoot any issues.
To determine the sequence of a server farm's logs, the administrator should consider the following factors:
Time stamps: Time stamps are indicators of when an event occurred on a server. Time stamps can help administrators sort and correlate events across different servers based on chronological order. However, time stamps alone may not be sufficient to determine the sequence of events if the servers have different time zones or clock settings.
Time offset: Time offset is the difference between the local time of a server and a reference time, such as Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT). Time offset can help administrators adjust and synchronize the time stamps of different servers to a common reference time and eliminate any discrepancies caused by time zones or clock settings.

NEW QUESTION: 28
During a Chief Information Security Officer (CISO) convention to discuss security awareness, the attendees are provided with a network connection to use as a resource. As the convention progresses, one of the attendees starts to notice delays in the connection, and the HIIPS site requests are reverting to HTTP Which of the following BEST describes what is happening?
A. Birthday collision on the certificate key
B. DNS hijacking to reroute traffic
C. Brute force to the access point
D. ASSLILS downgrade
Answer: B (LEAVE A REPLY)
The attendee is experiencing delays in the connection, and the HIIPS site requests are reverting to HTTP, indicating that the DNS resolution is redirecting the connection to another server. DNS hijacking is a technique that involves redirecting a user's requests for a domain name to a different IP address. Attackers use DNS hijacking to redirect users to malicious websites and steal sensitive information, such as login credentials and credit card details.
Reference:
https://www.cloudflare.com/learning/dns/dns-hijacking/

NEW QUESTION: 29
Which of the following BEST describes data streams that are compiled through artificial intelligence that provides insight on current cyberintrusions, phishing, and other malicious cyberactivity?
A. Intelligence fusion
B. Review reports
C. Log reviews
D. Threat feeds
Answer: A (LEAVE A REPLY)
Intelligence fusion is a process that involves aggregating and analyzing data from multiple sources, including artificial intelligence, to provide insight on current cyberintrusions, phishing, and other malicious cyberactivity.

NEW QUESTION: 30
Which of the following social engineering attacks best describes an email that is primarily intended to mislead recipients into forwarding the email to others?
A. Phishing
B. Pharming
C. Hoaxing
D. Watering-hole
Answer: C (LEAVE A REPLY)
Hoaxing is a type of social engineering attack that involves sending false or misleading information via email or other means to trick recipients into believing something that is not true. Hoaxing emails often contain a request or an incentive for the recipients to forward the email to others, such as a warning of a virus, a promise of a reward, or a petition for a cause. The goal of hoaxing is to spread misinformation, cause panic, waste resources, or damage reputations.
A hoaxing email is primarily intended to mislead recipients into forwarding the email to others, which can increase the reach and impact of the hoax.

NEW QUESTION: 31
A security team is engaging a third-party vendor to do a penetration test of a new proprietary application prior to its release.
Which of the following documents would the third-party vendor most likely be required to review and sign?
A. SLA
B. NDA
C. MOU
D. AUP
Answer: B (LEAVE A REPLY)
NDA stands for Non-Disclosure Agreement, which is a legal contract that binds the parties to keep confidential information secret and not to disclose it to unauthorized parties. A third-party vendor who is doing a penetration test of a new proprietary application would most likely be required to review and sign an NDA to protect the intellectual property and trade secrets of the security team.

NEW QUESTION: 32
A cyber security administrator is using iptables as an enterprise firewall. The administrator created some rules, but the network now seems to be unresponsive. All connections are being dropped by the firewall Which of the following would be the best option to remove the rules?
A. # iptables -t mangle -X
B. # iptables -F
C. # iptables -2
D. # iptables -P INPUT -j DROP
Answer: B (LEAVE A REPLY)
iptables is a command-line tool that allows an administrator to configure firewall rules for a Linux system. The -F option flushes or deletes all the existing rules in the selected chain or in all chains if none is given. It can be used to remove the rules that caused the network to be unresponsive and restore the default firewall behavior.

NEW QUESTION: 33
A security researcher has alerted an organization that its sensitive user data was found for sale on a website. Which of the following should the organization use to inform the affected parties?
A. A An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan
Answer: (SHOW ANSWER)
The organization should use a communications plan to inform the affected parties. A communications plan is a document that outlines how an organization will communicate with internal and external stakeholders during a crisis or incident. It should include details such as who will be responsible for communicating with different stakeholders, what channels will be used to communicate, and what messages will be communicated.
An incident response plan is a document that outlines the steps an organization will take to respond to a security incident or data breach. A business continuity plan is a document that outlines how an organization will continue to operate during and after a disruption. A disaster recovery plan is a document that outlines how an organization will recover its IT infrastructure and data after a disaster.

NEW QUESTION: 34
The Chief Information Security Officer directed a risk reduction in shadow IT and created a policy requiring all unsanctioned high-risk SaaS applications to be blocked from user access Which of the following is the BEST security solution to reduce this risk?
A. CASB

B. VPN concentrator
C. MFA
D. VPC endpoint
Answer: (SHOW ANSWER)
A Cloud Access Security Broker (CASB) can be used to monitor and control access to cloud-based applications, including unsanctioned SaaS applications. It can help enforce policies that prevent access to high-risk SaaS applications and provide visibility into the use of such applications by employees. Reference: CompTIA Security+ SY0-601 Exam Objectives: 3.3 Given a scenario, implement secure mobile solutions.

NEW QUESTION: 35
A network engineer receives a call regarding multiple LAN-connected devices that are on the same switch. The devices have suddenly been experiencing speed and latency issues while connecting to network resources. The engineer enters the command show mac address-table and reviews the following output Which of the following best describes the attack that is currently in progress?
A. MAC flooding
B. Evil twin
C. ARP poisoning
D. DHCP spoofing
Answer: C (LEAVE A REPLY)
This is an attempt to redirect traffic to an attacking host by sending an ARP packet that contains the forged address of the next hop router. The attacker tricks the victim into believing that it is the legitimate router by sending a spoofed ARP reply with its own MAC address. This causes the victim to send all its traffic to the attacker instead of the router. The attacker can then intercept, modify, or drop the packets as they please.

NEW QUESTION: 36
A desktop support technician recently installed a new document-scanning software program on a computer. However, when the end user tried to launch the program, it did not respond. Which of the following is MOST likely the cause?
A. A new firewall rule is needed to access the application.
B. The system was quarantined for missing software updates.
C. The software was not added to the application whitelist.
D. The system was isolated from the network due to infected software
Answer: C (LEAVE A REPLY)
The most likely cause of the document-scanning software program not responding when launched by the end user is that the software was not added to the application whitelist. An application whitelist is a list of approved software applications that are allowed to run on a system. If the software is not on the whitelist, it may be blocked from running by the system's security policies. Adding the software to the whitelist should resolve the issue and allow the program to run. Reference: https://www.techopedia.com/definition/31541/application-whitelisting

NEW QUESTION: 37

While performing a threat-hunting exercise, a security analyst sees some unusual behavior occurring in an application when a user changes the display name. The security analyst decides to perform a static code analysis and receives the following pseudocode:
Which of the following attack types best describes the root cause of the unusual behavior?
A. Server-side request forgery
B. Improper error handling
C. Buffer overflow
D. SQL injection
Answer: D (LEAVE A REPLY)
SQL injection is one of the most common web hacking techniques. SQL injection is the placement of malicious code in SQL statements, via web page input12. A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system3.
According to the pseudocode given in the question, the application takes a user input for display name and concatenates it with a SQL query to update the user's profile. This is a vulnerable practice that allows an attacker to inject malicious SQL code into the query and execute it on the database. For example, an attacker could enter something like this as their display name:
John'; DROP TABLE users; --
This would result in the following SQL query being executed:
UPDATE profile SET displayname = 'John'; DROP TABLE users; --' WHERE userid = 1; The semicolon (;) terminates the original update statement and starts a new one that drops the users table. The double dash (-) comments out the rest of the query. This would cause a catastrophic loss of data for the application.

NEW QUESTION: 38
A network manager is concerned that business may be negatively impacted if the firewall in its data center goes offline. The manager would like to implement a high availability pair to:
A. decrease the mean time between failures.
B. remove the single point of failure.
C. cut down the mean time to repair
D. reduce the recovery time objective
Answer: B (LEAVE A REPLY)
A single point of failure is a component or element of a system that, if it fails, will cause the entire system to fail or stop functioning. It can pose a high risk and impact for business continuity and availability. A high availability pair is a configuration that involves two identical devices or systems that operate in parallel and provide redundancy and failover capabilities. It can remove the single point of failure by ensuring that if one device or system fails, the other one can take over its functions without interruption or downtime.

NEW QUESTION: 39
A security analyst is investigating multiple hosts that are communicating to external IP addresses during the hours of 2:00 a.m - 4:00 am. The malware has evaded detection by traditional antivirus software. Which of the following types of malware is MOST likely infecting the hosts?

A. A RAT
B. Ransomware
C. Polymophic
D. A worm
Answer: A (LEAVE A REPLY)
Based on the given information, the most likely type of malware infecting the hosts is a RAT (Remote Access Trojan). RATs are often used for stealthy unauthorized access to a victim's computer, and they can evade traditional antivirus software through various sophisticated techniques. In particular, the fact that the malware is communicating with external IP addresses during specific hours suggests that it may be under the control of an attacker who is issuing commands from a remote location. Ransomware, polymorphic malware, and worms are also possible culprits, but the context of the question suggests that a RAT is the most likely answer.

NEW QUESTION: 40
Which of the following is constantly scanned by internet bots and has the highest risk of attack in the case of the default configurations?
A. Wearable sensors
B. Raspberry Pi
C. Surveillance systems
D. Real-time operating systems
Answer: (SHOW ANSWER)
Surveillance systems are constantly scanned by internet bots and have the highest risk of attack in the case of the default configurations because they are often connected to the internet and use weak or default passwords that can be easily guessed or cracked by malicious bots. Internet bots are software applications that run automated tasks over the internet, usually with the intent to imitate human activity or exploit vulnerabilities. Some bots are used for legitimate purposes, such as web crawling or indexing, but others are used for malicious purposes, such as spamming, phishing, denial-of-service attacks, or credential stuffing. Security misconfigurations are one of the most common gaps that criminal hackers look to exploit. Therefore, it is important to secure the configuration of surveillance systems by changing the default passwords, updating the firmware, disabling unnecessary services, and enabling encryption and authentication.
https://www.cctvcameraworld.com/setup-ip-camera-system-on-network/

NEW QUESTION: 41
A company recently experienced an attack during which its main website was Directed to the attacker's web server, allowing the attacker to harvest credentials from unsuspecting customers, Which of the following should the company implement to prevent this type of attack from occurring In the future?
A. IPsec
B. SSL/TLS
C. ONSSEC
D. SMIME
Answer: (SHOW ANSWER)
To prevent attacks where the main website is directed to the attacker's web server and allowing the attacker to harvest credentials from unsuspecting customers, the company should implement SSL/TLS (Secure Sockets Layer/Transport Layer

Security) to encrypt the communication between the web server and the clients. This will prevent attackers from intercepting and tampering with the communication, and will also help to verify the identity of the web server to the clients.

NEW QUESTION: 42
A company would like to move to the cloud. The company wants to prioritize control and security over cost and ease of management. Which of the following cloud models would best suit this company's priorities?
A. Public
B. Hybrid
C. Community
D. Private
Answer: D (LEAVE A REPLY)
A private cloud model would best suit the company's priorities of control and security over cost and ease of management. In a private cloud, the infrastructure is dedicated to a single organization, providing greater control over the environment and the ability to implement strict security measures. This is in contrast to public, community, or hybrid cloud models, where resources are shared among multiple organizations, potentially compromising control and security. While private clouds can be more expensive and more difficult to manage, they the highest level of control and security for the company.
Reference:
- CompTIA Security+ Certification Exam Objectives (SY0-601), Section 3.2: "Explain the importance of secure staging deployment concepts."
- Cisco: Private Cloud - https://www.cisco.com/c/en/us/solutions/cloud/private-cloud.html

NEW QUESTION: 43
Which of the following is a primary security concern for a company setting up a BYOD program?
A. End of life
B. Buffer overflow
C. VM escape
D. Jailbreaking
Answer: D (LEAVE A REPLY)
Jailbreaking is a process of bypassing or removing the manufacturer-imposed restrictions on a mobile device's operating system, allowing users to install unauthorized applications, modify settings, etc. It is a primary security concern for setting up a BYOD program because it can expose the device and its data to malware, vulnerabilities, unauthorized access, etc.

NEW QUESTION: 44
A systems engineer thinks a business system has been compromised and is being used to exfiltrated data to a competitor The engineer contacts the CSIRT The CSIRT tells the engineer to immediately disconnect the network cable and to not do anything else Which of the following is the most likely reason for this request?
A. The CSIRT thinks an insider threat is attacking the network
B. Outages of business-critical systems cost too much money
C. The CSIRT does not consider the systems engineer to be trustworthy
D. Memory contents including fileles malware are lost when the power is turned off
Answer: D (LEAVE A REPLY)

Memory contents including files and malware are lost when the power is turned off. This is because memory is a volatile storage device that requires constant power to retain data. If a system has been compromised and is being used to exfiltrate data to a competitor, the CSIRT may want to preserve the memory contents for forensic analysis and evidence collection. Therefore, the CSIRT may tell the engineer to immediately disconnect the network cable and not do anything else to prevent further data loss or tampering.

NEW QUESTION: 45
A systems analyst determines the source of a high number of connections to a web server that were initiated by ten different IP addresses that belong to a network block in a specific country. Which of the following techniques will the systems analyst MOST likely implement to address this issue?
A. Content filter
B. SIEM
C. Firewall rules
D. DLP
Answer: (SHOW ANSWER)
A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. The systems analyst can use firewall rules to block connections from the ten IP addresses in question, or from the entire network block in the specific country. This would be a quick and effective way to address the issue of high connections to the web server initiated by these IP addresses.

NEW QUESTION: 46
A company wants to deploy PKI on its internet-facing website The applications that are currently deployed are
* www company.com (mam website)
* contact us company com (for locating a nearby location)
* quotes company.com (for requesting a price quote)
The company wants to purchase one SSL certificate that will work for all the existing applications and any future applications that follow the same naming conventions, such as store company com Which of the following certificate types would best meet the requirements?
A. SAN
B. Wildcard
C. Extended validation
D. Self-signed
Answer: B (LEAVE A REPLY)
A wildcard certificate is a type of SSL certificate that can secure multiple subdomains under one domain name by using an asterisk (*) as a placeholder for any subdomain name. For example, *.company.com can secure www.company.com, contactus.company.com, quotes.company.com, etc. It can work for all the existing applications and any future applications that follow the same naming conventions, such as store.company.com.

NEW QUESTION: 47
An upcoming project focuses on secure communications and trust between external parties. Which of the following security components will need to be considered to ensure a chosen trust provider IS used and the selected option is highly scalable?
A. Self-signed certificate
B. Certificate attributes
C. Public key Infrastructure
D. Domain validation
Answer: C (LEAVE A REPLY)
PKI is a security technology that enables secure communication between two parties by using cryptographic functions. It consists of a set of components that are used to create, manage, distribute, store, and revoke digital certificates. PKI provides a secure way to exchange data between two parties, as well as a trust provider to ensure that the data is not tampered with. It also helps to create a highly scalable solution, as the same certificate can be used for multiple parties.
According to the CompTIA Security+ Study Guide, "PKI is a technology used to secure communications between two external parties. PKI is based on the concept of digital certificates, which are used to authenticate the sender and recipient of a message. PKI provides a trust provider to ensure that the digital certificate is valid and has not been tampered with. It also provides a scalable solution, as multiple parties can use the same certificate."

NEW QUESTION: 48
Which of the following would most likely include language prohibiting end users from accessing personal email from a company device?
A. SLA
B. BPA
C. NDA
D. AUP
Answer: D (LEAVE A REPLY)
AUP or Acceptable Use Policy is a document that defines the rules and guidelines for using a company's IT resources, such as devices, networks, internet, email, etc. It usually includes language prohibiting end users from accessing personal email from a company device, as well as other activities that may compromise security or productivity1.
https://www.thesecuritybuddy.com/governance-risk-and-compliance/what-are-sla-mou-bpa-and-nda/ 3:
https://www.professormesser.com/security-plus/sy0-501/agreement-types/ 1:
https://www.techopedia.com/definition/2471/acceptable-use-policy-aup

NEW QUESTION: 49

An engineer recently deployed a group of 100 web servers in a cloud environment. Per the security policy, all web-server ports except 443 should be disabled. Which of the following can be used to accomplish this task?

A. Application allow list

B. Load balancer

C. Host-based firewall

D. VPN

Answer: C (LEAVE A REPLY)

A host-based firewall is a software application that runs on each individual host and controls the incoming and outgoing network traffic based on a set of rules. A host-based firewall can be used to block or allow specific ports, protocols, IP addresses, or applications.

An engineer can use a host-based firewall to accomplish the task of disabling all web-server ports except 443 on a group of 100 web servers in a cloud environment. The engineer can configure the firewall rules on each web server to allow only HTTPS traffic on port 443 and deny any other traffic. Alternatively, the engineer can use a centralized management tool to deploy and enforce the firewall rules across all web servers.

NEW QUESTION: 50

Which of the following would be best to ensure data is saved to a location on a server, is easily scaled, and is centrally monitored?

A. Edge computing

B. Microservices

C. Containers

D. Thin client

Answer: C (LEAVE A REPLY)

Containers are a method of virtualization that allow you to run multiple isolated applications on a single server. Containers are lightweight, portable, and scalable, which means they can save resources, improve performance, and simplify deployment. Containers also enable centralized monitoring and management of the applications running on them, using tools such as Docker or Kubernetes. Containers are different from edge computing, which is a distributed computing paradigm that brings computation and data storage closer to the location where it is needed. Microservices are a software architecture style that breaks down complex applications into smaller, independent services that communicate with each other. Thin clients are devices that rely on a server to perform most of the processing tasks and only provide a user interface.

NEW QUESTION: 51

Which of the following should a technician consider when selecting an encryption method for data that needs to remain confidential for a specific length of time?

A. The key length of the encryption algorithm

B. The encryption algorithm's longevity

C. A method of introducing entropy into key calculations

D. The computational overhead of calculating the encryption key

Answer: B (LEAVE A REPLY)

When selecting an encryption method for data that needs to remain confidential for a specific length of time, the longevity of the encryption algorithm should be considered to ensure that the data remains secure for the required period. Reference: CompTIA

Security+ Certification Exam Objectives - 3.2 Given a scenario, use appropriate cryptographic methods. Study Guide: Chapter 4, page 131.

NEW QUESTION: 52
Which of the following BEST describes a social-engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested?
A. Whaling
B. Spam
C. Invoice scam
D. Pharming
Answer: (SHOW ANSWER)
A social engineering attack that relies on an executive at a small business visiting a fake banking website where credit card and account details are harvested is known as whaling. Whaling is a type of phishing attack that targets high-profile individuals, such as executives, to steal sensitive information or gain access to their accounts.

NEW QUESTION: 53
Which of the following roles would MOST likely have direct access to the senior management team?
A. Data custodian
B. Data owner
C. Data protection officer
D. Data controller
Answer: (SHOW ANSWER)
A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization. A DPO is responsible for ensuring that the organization follows data protection laws and regulations, such as the General Data Protection Regulation (GDPR), and protects the privacy rights of data subjects. A DPO also acts as a liaison between the organization and data protection authorities, as well as data subjects and other stakeholders.
A DPO would most likely have direct access to the senior management team, as they need to report on data protection issues, risks, and incidents, and advise on data protection policies and practices.
The other options are not correct because:
a) Data custodian is a role that implements and maintains the technical controls and procedures for data security and integrity. A data custodian does not have direct access to the senior management team, as they are more involved in operational tasks than strategic decisions.
b) Data owner is a role that determines the classification and usage of data within an organization. A data owner does not have direct access to the senior management team, as they are more involved in business functions than data protection compliance.
d) Data controller is a role that determines the purposes and means of processing personal data within an organization. A data controller does not have direct access to the senior management team, as they are more involved in data processing activities than data protection oversight.
According to CompTIA Security+ SY0-601 Exam Objectives 2.3 Given a scenario, implement secure protocols:
"A data protection officer (DPO) is a role that oversees the data protection strategy and compliance of an organization."

NEW QUESTION: 54

A user's laptop constantly disconnects from the Wi-Fi network. Once the laptop reconnects, the user can reach the internet but cannot access shared folders or other network resources. Which of the following types of attacks is the user MOST likely experiencing?

A. Bluejacking

B. Jamming

C. Rogue access point

D. Evil twin

Answer: D (LEAVE A REPLY)

An evil twin attack is when an attacker sets up a fake Wi-Fi network that looks like a legitimate network, but is designed to capture user data that is sent over the network. In this case, the user's laptop is constantly disconnecting and reconnecting to the Wi-Fi network, indicating that it is connecting to the fake network instead of the legitimate one. Once the user connects to the fake network, they are unable to access shared folders or other network resources, as those are only available on the legitimate network.

NEW QUESTION: 55

A company is developing a new initiative to reduce insider threats. Which of the following should the company focus on to make the greatest impact?

A. Social media analysis

B. Least privilege

C. Nondisclosure agreements

D. Mandatory vacation

Answer: (SHOW ANSWER)

Least privilege is a security principle that states that users and processes should only have the minimum level of access and permissions required to perform their tasks. This reduces the risk of insider threats by limiting the potential damage that a malicious or compromised user or process can cause to the system or data. Reference: https://www.comptia.org/blog/what-is-least-privilege

NEW QUESTION: 56

A user received an SMS on a mobile phone that asked for bank details. Which of the following social engineering techniques was used in this case?

A. SPIM

B. Vishing

C. Spear phishing

D. Smishing

Answer: (SHOW ANSWER)

Smishing is a type of social engineering technique that involves sending fraudulent or malicious text messages (SMS) to a user's mobile phone. It can trick the user into providing personal or financial information, clicking on malicious links, downloading malware, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity.

NEW QUESTION: 57

A desktop computer was recently stolen from a desk located in the lobby of an office building. Which of the following would be the best way to secure a replacement computer and deter future theft?

A. Installing proximity card readers on all entryway doors

B. Deploying motion sensor cameras in the lobby

C. Encrypting the hard drive on the new desktop

D. Using cable locks on the hardware

Answer: D (LEAVE A REPLY)

Using cable locks on the hardware can be an effective way to secure a desktop computer and deter future theft. Cable locks are physical security devices that attach to the computer case and to a nearby stationary object, such as a desk or wall. This makes it more difficult for a thief to remove the computer without damaging it or attracting attention.

Installing proximity card readers on all entryway doors can enhance physical security by limiting access to authorized individuals. Deploying motion sensor cameras in the lobby can also help deter theft by capturing images of any unauthorized individuals entering the premises or attempting to steal the computer. Encrypting the hard drive on the replacement desktop can also help protect sensitive data in the event of theft, but it does not provide physical security for the device itself.

NEW QUESTION: 58

A company would like to protect credit card information that is stored in a database from being exposed and reused. However, the current POS system does not support encryption. Which of the following would be BEST suited to secure this information?
(Give me related explanation and references from CompTIA Security+ SY0-601 documents for Correct answer option)

A. Masking

B. Tokenization

C. DLP

D. SSL/TLS

Answer: B (LEAVE A REPLY)

Tokenization replaces sensitive data with non-sensitive data, such as a unique identifier. This means that the data is still present in the system, but the sensitive information itself is replaced with the token. Tokenization is more secure than masking, which only obscures the data but does not eliminate it. DLP is not suitable for this task, as it is designed to prevent the loss or leakage of data from the system. SSL/TLS can be used to secure the transmission of data, but it cannot prevent the data itself from being exposed or reused. For more information, please refer to CompTIA Security+ SY0-601 Exam Objectives, Section 3.3: Explain the security purpose of authentication, authorization and accounting (AAA) services, and Section 4.7: Explain the purpose and characteristics of various types of encryption.

NEW QUESTION: 59

A company needs to centralize its logs to create a baseline and have visibility on its security events Which of the following technologies will accomplish this objective?

A. Security information and event management

B. A web application firewall

C. A vulnerability scanner

D. A next-generation firewall

Answer: A (LEAVE A REPLY)

Security information and event management (SIEM) is a solution that collects, analyzes, and correlates logs and events from various sources such as firewalls, servers, applications, etc., within an organization's network. It can centralize logs to create a baseline and have visibility on security events by providing a unified dashboard and reporting system for log management and security monitoring.

NEW QUESTION: 60
A security administrator has discovered that workstations on the LAN are becoming infected with malware. The cause of the infections appears to be users receiving phishing emails that are bypassing the current email-filtering technology. As a result, users are being tricked into clicking on malicious URLs, as no internal controls currently exist in the environment to evaluate their safety. Which of the following would be BEST to implement to address the issue?
A. Forward proxy
B. HIDS
C. Awareness training
D. A jump server
E. IPS
Answer: C (LEAVE A REPLY)
Awareness training should be implemented to educate users on the risks of clicking on malicious URLs. Reference: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 9

NEW QUESTION: 61
A backup operator wants to perform a backup to enhance the RTO and RPO in a highly time- and storage-efficient way that has no impact on production systems. Which of the following backup types should the operator use?
A. Tape
B. Full
C. Image
D. Snapshot
Answer: (SHOW ANSWER)
A snapshot backup is a type of backup that captures the state of a system at a point in time. It is highly time- and storage-efficient because it only records the changes made to the system since the last backup. It also has no impact on production systems because it does not require them to be offline or paused during the backup process. Reference: https://www.comptia.org/blog/what-is-a-snapshot-backup

NEW QUESTION: 62

A security analyst is investigating what appears to be unauthorized access to a corporate web application. The security analyst reviews the web server logs and finds the following entries:
Which of the following password attacks is taking place?
A. Dictionary
B. Brute-force
C. Rainbow table
D. Spraying
Answer: D (LEAVE A REPLY)
Spraying is a password attack that involves trying a few common passwords against a large number of usernames. Spraying is different from brute-force attacks, which try many possible passwords against one username, or dictionary attacks, which try a list of words from a dictionary file against one username. Spraying is often used when the web application has a lockout policy that prevents multiple failed login attempts for the same username. Spraying can be detected by looking for patterns of failed login attempts from the same source IP address with different usernames and the same or similar passwords.

NEW QUESTION: 63
Cloud security engineers are planning to allow and deny access to specific features in order to in-crease data security. Which of the following cloud features is the most appropriate to ensure ac-cess is granted properly?
A. API integrations
B. Auditing
C. Resource policies
D. Virtual networks
Answer: C (LEAVE A REPLY)
Resource policies are cloud features that allow and deny access to specific features in order to increase data security. Resource policies are rules or statements that define what actions can be performed on a particular resource by which entities under what conditions. Resource policies can be attached to cloud resources such as virtual machines, storage accounts, databases, or functions. Resource policies can help enforce security best practices, compliance requirements, and cost management. Resource policies can also help implement the principle of least privilege, which grants users only the minimum level of access they need to perform their tasks.

NEW QUESTION: 64
A company has installed badge readers for building access but is finding unau-thorized individuals roaming the hallways Of the following is the most likely cause?
A. Shoulder surfing
B. Phishing
C. Tailgating
D. Identity fraud
Answer: C (LEAVE A REPLY)
Tailgating is a physical security threat that occurs when an unauthorized person follows an authorized person into a restricted area without proper identification or authorization. It can cause unauthorized individuals to roam the hallways after gaining access through badge readers installed for building access.

NEW QUESTION: 65
After installing a patch On a security appliance. an organization realized a massive data exfiltration occurred. Which Of the following describes the incident?
A. Supply chain attack
B. Ransomware attack
C. Cryptographic attack
D. Password attack
Answer: A (LEAVE A REPLY)
A supply chain attack is a type of attack that involves compromising a trusted third-party provider or vendor and using their products or services to deliver malware or gain access to the target organization. The attacker can exploit the trust and dependency that the organization has on the provider or vendor and bypass their security controls. In this case, the attacker may have tampered with the patch for the security appliance and used it to exfiltrate data from the organization.

NEW QUESTION: 66
The alert indicates an attacker entered thousands of characters into the text box of a web form. The web form was intended for legitimate customers to enter their phone numbers. Which of the attacks has most likely occurred?
A. Privilege escalation
B. Buffer overflow
C. Resource exhaustion
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
A buffer overflow attack occurs when an attacker inputs more data than the buffer can store, causing the excess data to overwrite adjacent memory locations and corrupt or execute code1. In this case, the attacker entered thousands of characters into a text box that was intended for phone numbers, which are much shorter. This could result in a buffer overflow attack that compromises the web application or server. The other options are not related to this scenario. Privilege escalation is when an attacker gains unauthorized access to higher-level privileges or resources2. Resource exhaustion is when an attacker consumes all the available resources of a system, such as CPU, memory, disk space, etc., to cause a denial of service3. Cross-site scripting is when an attacker injects malicious code into a web page that is executed by the browser of a victim who visits the page.

NEW QUESTION: 67
Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)
* Hostname: ws01
* Domain: comptia.org
* IPv4: 10.1.9.50
* IPV4: 10.2.10.50
* Root: home.aspx
* DNS CNAME:homesite.
Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.
Answer:

NEW QUESTION: 68
A software developer used open-source libraries to streamline development. Which of the following is the greatest risk when using this approach?
A. Unsecure root accounts
B. Default settings
C. Password complexity
D. Lack of vendor support
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69
Which Of the following supplies non-repudiation during a forensics investiga-tion?
A. Dumping volatile memory contents first
B. Duplicating a drive With dd
C. a SHA 2 signature of a drive image
D. Logging everyone in contact with evidence
E. Encrypting sensitive data
Answer: (SHOW ANSWER)
A SHA 2 signature is a cryptographic hash function that produces a unique and fixed-length output for any given input. It can provide non-repudiation during a forensics investigation by verifying the integrity and authenticity of a drive image and proving that it has not been altered or tampered with since it was created

NEW QUESTION: 70
Physical access to the organization's servers in the data center requires entry and exit through multiple access points: a lobby, an access control vestibule, three doors leading to the server floor itself and eventually to a caged area solely for the organization's hardware. Which of the following controls is described in this scenario?
A. Compensating
B. Deterrent
C. Preventive
D. Detective
Answer: C (LEAVE A REPLY)
The scenario describes preventive controls, which are designed to stop malicious actors from gaining access to the organization's servers. This includes using multiple access points, such as a lobby, an access control vestibule, and multiple doors leading to the server floor, as well as caging the organization's hardware. According to the CompTIA Security+ SY0-601 document, preventive controls are "designed to stop malicious actors from performing a malicious activity or gaining access to an asset." These controls can include technical solutions, such as authentication and access control systems, physical security solutions, such as locks and barriers, and administrative solutions such as policy enforcement.

NEW QUESTION: 71

Hackers recently attacked a company's network and obtained several unfavorable pictures from the Chief Executive Officer's workstation. The hackers are threatening to send the images to the press if a ransom is not paid. Which of the following is impacted the MOST?

A. Identify theft

B. Data loss

C. Data exfiltration

D. Reputation

Answer: D (LEAVE A REPLY)

The best option that describes what is impacted the most by the hackers' attack and threat would be D. Reputation. Reputation is the perception or opinion that others have about a person or an organization. Reputation can affect the trust, credibility, and success of a person or an organization. In this scenario, if the hackers send the unfavorable pictures to the press, it can damage the reputation of the Chief Executive Officer and the company, and cause negative consequences such as loss of customers, partners, investors, or employees.

NEW QUESTION: 72

A cybersecurity administrator needs to implement a Layer 7 security control on a network and block potential attacks. Which of the following can block an attack at Layer 7? (Select TWO).

A. HIDS

B. NIPS

C. HSM

D. WAF

E. NAC

F. NIDS

G. Stateless firewall

Answer: D,F (LEAVE A REPLY)

A WAF (Web Application Firewall) and NIDS (Network Intrusion Detection System) are both examples of Layer 7 security controls. A WAF can block attacks at the application layer (Layer 7) of the OSI model by filtering traffic to and from a web server. NIDS can also detect attacks at Layer 7 by monitoring network traffic for suspicious patterns and behaviors. Reference: CompTIA Security+ Study Guide, pages 94-95, 116-118

NEW QUESTION: 73

Which of the following identifies the point in time when an organization will recover data in the event of an outage?

A. SLA

B. RPO

C. MTBF

D. ARO

Answer: B (LEAVE A REPLY)

Detailed Recovery Point Objective (RPO) is the maximum duration of time that an organization can tolerate data loss in the event of an outage. It identifies the point in time when data recovery must begin, and any data loss beyond that point is considered unacceptable.

NEW QUESTION: 74
An organization recently completed a security control assessment The organization determined some controls did not meet the existing security measures. Additional mitigations are needed to lessen the risk of the non-complaint controls. Which of the following best describes these mitigations?
A. Corrective
B. Compensating
C. Deterrent
D. Technical
Answer: B (LEAVE A REPLY)
Compensating controls are additional security measures that are implemented to reduce the risk of non-compliant controls. They do not fix the underlying issue, but they provide an alternative way of achieving the same security objective. For example, if a system does not have encryption, a compensating control could be to restrict access to the system or use a secure network connection.

NEW QUESTION: 75
During an incident a company CIRT determine it is necessary to observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the risk of lateral spread and the risk that the adversary would notice any changes?
A. Physical move the PC to a separate internet pint of presence
B. Create and apply micro segmentation rules.
C. Emulate the malware in a heavily monitored DM Z segment.
D. Apply network blacklisting rules for the adversary domain
Answer: C (LEAVE A REPLY)
To observe the continued network-based transaction between a callback domain and the malware running on an enterprise PC while reducing the risk of lateral spread and the risk that the adversary would notice any changes, the best technique to use is to emulate the malware in a heavily monitored DMZ segment. This is a secure environment that is isolated from the rest of the network and can be heavily monitored to detect any suspicious activity. By emulating the malware in this environment, the activity can be observed without the risk of lateral spread or detection by the adversary. Reference: https://www.sans.org/blog/incident-response-fundamentals-why-is-the-dmz-so-important/

NEW QUESTION: 76
Which of the following is a cryptographic concept that operates on a fixed length of bits?
A. Block cipher
B. Hashing
C. Key stretching
D. Salting
Answer: A (LEAVE A REPLY)
Single-key or symmetric-key encryption algorithms create a fixed length of bits known as a block cipher with a secret key that the creator/sender uses to encipher data (encryption) and the receiver uses to decipher it.

NEW QUESTION: 77
A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:
Which ol the following types of attacks is being attempted and how can it be mitigated?
A. XSS. mplement a SIEM
B. CSRF. implement an IPS
C. Directory traversal implement a WAF
D. SQL infection, mplement an IDS
Answer: (SHOW ANSWER)
Detailed The attack being attempted is directory traversal, which is a web application attack that allows an attacker to access files and directories outside of the web root directory. A WAF can help mitigate this attack by detecting and blocking attempts to access files outside of the web root directory.

NEW QUESTION: 78
An enterprise has hired an outside security firm to facilitate penetration testing on its network and applications. The firm has agreed to pay for each vulnerability that ts discovered. Which of the following BEST represents the type of testing that is being used?
A. White-box
B. Red-leam
C. Bug bounty
D. Gray-box
E. Black-box
Answer: C (LEAVE A REPLY)
Bug bounty is a type of testing in which an organization offers a reward or compensation to anyone who can identify vulnerabilities or security flaws in their network or applications. The outside security firm has agreed to pay for each vulnerability found, which is an example of a bug bounty program.

NEW QUESTION: 79
A systems administrator is required to enforce MFA for corporate email account access, relying on the possession factor. Which of the following authentication methods should the systems administrator choose? (Select two).
A. passphrase
B. Time-based one-time password
C. Facial recognition
D. Retina scan
E. Hardware token

F. Fingerprints

Answer: B,E (LEAVE A REPLY)

Time-based one-time password (TOTP) and hardware token are authentication methods that rely on the possession factor, which means that the user must have a specific device or object in their possession to authenticate. A TOTP is a password that is valid for a short period of time and is generated by an app or a device that the user has. A hardware token is a physical device that displays a code or a password that the user can enter to authenticate. A passphrase (Option A) is a knowledge factor, while facial recognition (Option C), retina scan (Option D), and fingerprints (Option F) are all inherence factors.

https://ptgmedia.pearsoncmg.com/imprint_downloads/pearsonitcertification/bookreg/9780136798675/9780136798675_tearcard.pdf

https://www.youtube.com/watch?v=yCJyPPvM-xg

NEW QUESTION: 80

A company completed a vulnerability scan. The scan found malware on several systems that were running older versions of Windows. Which of the following is MOST likely the cause of the malware infection?

A. Open permissions

B. Improper or weak patch management

C. Unsecure root accounts

D. Default settings

Answer: B (LEAVE A REPLY)

The reason for this is that older versions of Windows may have known vulnerabilities that have been patched in more recent versions. If a company is not regularly patching their systems, they are leaving those vulnerabilities open to exploit, which can allow malware to infect the systems.

It is important to regularly update and patch systems to address known vulnerabilities and protect against potential malware infections. This is an important aspect of proper security management.

Here is a reference to the CompTIA Security+ certification guide which states that "Properly configuring and maintaining software, including patch management, is critical to protecting systems and data."

NEW QUESTION: 81

The Chief information Security Officer has directed the security and networking team to retire the use of shared passwords on routers and switches. Which of the following choices BEST meets the requirements?

A. SAML

B. TACACS+

C. Password vaults

D. OAuth

Answer: (SHOW ANSWER)

TACACS+ is a protocol used for remote authentication, authorization, and accounting (AAA) that can be used to replace shared passwords on routers and switches. It provides a more secure method of authentication that allows for centralized management of access control policies. Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

NEW QUESTION: 82

An attacker is using a method to hide data inside of benign files in order to exfiltrate confidential dat a. Which of the following is the attacker most likely using?

A. Base64 encoding
B. Steganography
C. Data encryption
D. Perfect forward secrecy
Answer: B (LEAVE A REPLY)
Steganography is a technique for hiding data inside of benign files such as images, audio, or video. This can be used to exfiltrate confidential data without raising suspicion or detection.

NEW QUESTION: 83
A security engineer is reviewing the logs from a SAML application that is configured to use MFA, during this review the engineer notices a high volume of successful logins that did not require MFA from users who were traveling internationally. The application, which can be accessed without a VPB, has a policy that allows time-based tokens to be generated. Users who changed locations should be required to reauthenticate but have been Which of the following statements BEST explains the issue?
A. An incorrect browser has been detected by the SAML application
B. OpenID is mandatory to make the MFA requirements work
C. The user's IP address is changing between logins, bur the application is not invalidating the token
D. The access device has a trusted certificate installed that is overwriting the session token
Answer: C (LEAVE A REPLY)

NEW QUESTION: 84
A user is trying unsuccessfully to send images via SMS. The user downloaded the images from a corporate email account on a work phone. Which of the following policies is preventing the user from completing this action?
A. Application management
B. Content management
C. Containerization
D. Full disk encryption
Answer: (SHOW ANSWER)
Content management is a policy that controls what types of data can be accessed, modified, shared, or transferred by users or applications. Content management can prevent data leakage or exfiltration by blocking or restricting certain actions, such as copying, printing, emailing, or sending data via SMS. If the user downloaded the images from a corporate email account on a work phone, the content management policy may prevent the user from sending the images via SMS to protect the confidentiality and integrity of the data. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 10, Domain 2.0: Architecture and Design, Objective 2.4: Explain the importance of embedded and specialized systems security 2 CompTIA Security+ Certification Exam Objectives, page 12, Domain 3.0: Implementation, Objective 3.1: Implement secure network architecture concepts 3 https://www.comptia.org/blog/what-is-data-loss-prevention

NEW QUESTION: 85
A company that provides an online streaming service made its customers' personal data including names and email addresses publicly available in a cloud storage service. As a result, the company experienced an increase m the number of requests to delete user accounts. Which of the following best describes the consequence of tins data disclosure?
A. Regulatory tines

B. Reputation damage
C. Increased insurance costs
D. Financial loss
Answer: B (LEAVE A REPLY)
Reputation damage Short Reputation damage is the loss of trust or credibility that a company suffers when its customers' personal data is exposed or breached. This can lead to customer dissatisfaction, loss of loyalty, and requests to delete user accounts. Reference: https://www.comptia.org/content/guides/what-is-cybersecurity

NEW QUESTION: 86
A security analyst received the following requirements for the deployment of a security camera solution:
* The cameras must be viewable by the on-site security guards.
+ The cameras must be able to communicate with the video storage server.
* The cameras must have the time synchronized automatically.
* The cameras must not be reachable directly via the internet.
* The servers for the cameras and video storage must be available for remote maintenance via the company VPN.
Which of the following should the security analyst recommend to securely meet the remote connectivity requirements?
A. Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on
B. Deploying a jump server that is accessible via the internal network that can communicate with the servers
C. Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering
D. Implementing a WAF to allow traffic from the local NTP server to the camera server
Answer: B (LEAVE A REPLY)
A jump server is a system that is used to manage and access systems in a separate security zone. It acts as a bridge between two different security zones and provides a controlled and secure way of accessing systems between them12. A jump server can also be used for auditing traffic and user activity for real-time surveillance3. By deploying a jump server that is accessible via the internal network, the security analyst can securely meet the remote connectivity requirements for the servers and cameras without exposing them directly to the internet or allowing outgoing traffic from their subnet. The other options are not suitable because:
a) Creating firewall rules that prevent outgoing traffic from the subnet the servers and cameras reside on would not allow remote maintenance via the company VPN.
c) Disabling all unused ports on the switch that the cameras are plugged into and enabling MAC filtering would not prevent direct internet access to the cameras or servers.
d) Implementing a WAF to allow traffic from the local NTP server to the camera server would not address the remote connectivity requirements or protect the servers from internet access.
Reference:
1: https://www.thesecuritybuddy.com/network-security/what-is-a-jump-server/ 3: https://www.ssh.com/academy/iam/jump-server
2: https://en.wikipedia.org/wiki/Jump_server

NEW QUESTION: 87
A company acquired several other small companies The company thai acquired the others is transitioning network services to the cloud The company wants to make sure that performance and security remain intact Which of the following BEST meets both requirements?
A. High availability

B. Application security
C. Segmentation
D. Integration and auditing
Answer: (SHOW ANSWER)
High availability refers to the ability of a system or service to remain operational and available to users with minimal downtime. By ensuring high availability, the company can maintain good performance and ensure that users have access to the network services they need. High availability can also improve security, as it helps to prevent disruptions that could potentially be caused by security incidents or other issues.

NEW QUESTION: 88
A security administrator performs weekly vulnerability scans on all cloud assets and provides a detailed report. Which of the following describes the administrator's activities?
A. Continuous deployment
B. Continuous integration
C. Continuous validation
D. Continuous monitoring
Answer: C (LEAVE A REPLY)
Continuous validation is a process that involves performing regular and automated tests to verify the security and functionality of a system or an application. Continuous validation can help identify and remediate vulnerabilities, bugs, or misconfigurations before they cause any damage or disruption. The security administrator's activities of performing weekly vulnerability scans on all cloud assets and providing a detailed report are examples of continuous validation.

NEW QUESTION: 89
A data cento has experienced an increase in under-voltage events Mowing electrical grid maintenance outside the facility These events are leading to occasional losses of system availability Which of the following would be the most cost-effective solution for the data center 10 implement"
A. Uninterruptible power supplies with battery backup
B. Managed power distribution units lo track these events
C. A generator to ensure consistent, normalized power delivery
D. Dual power supplies to distribute the load more evenly
Answer: A (LEAVE A REPLY)
Uninterruptible power supplies with battery backup would be the most cost-effective solution for the data center to implement to prevent under-voltage events following electrical grid maintenance outside the facility. An uninterruptible power supply (UPS) is a device that provides emergency power to a load when the main power source fails or drops below an acceptable level. A UPS with battery backup can help prevent under-voltage events by switching to battery power when it detects a voltage drop or outage in the main power source. A UPS with battery backup can also protect the data center equipment from power surges or spikes.

NEW QUESTION: 90
Which of the following would be the best resource for a software developer who is looking to improve secure coding practices for web applications?
A. OWASP

B. Vulnerability scan results
C. NIST CSF
D. Third-party libraries
Answer: A (LEAVE A REPLY)
OWASP (Open Web Application Security Project) is a non-profit organization that provides resources and guidance for improving the security of web applications. It can be the best resource for a software developer who is looking to improve secure coding practices for web applications by offering various tools, frameworks, standards, cheat sheets, testing guides, etc., that cover various aspects of web application security development and testing

NEW QUESTION: 91
A client sent several inquiries to a project manager about the delinquent delivery status of some critical reports. The project manager claimed the reports were previously sent via email, but then quickly generated and backdated the reports before submitting them as plain text within the body of a new email message thread. Which of the following actions MOST likely supports an investigation for fraudulent submission?
A. Establish chain of custody.
B. Inspect the file metadata.
C. Reference the data retention policy.
D. Review the email event logs
Answer: D (LEAVE A REPLY)
Reviewing the email event logs can support an investigation for fraudulent submission, as these logs can provide details about the history of emails, including the message content, timestamps, and sender/receiver information. Reference: CompTIA Security + Certification Exam Objectives, Exam SY0-601, 3.2 Given a scenario, implement appropriate data security and privacy controls.

NEW QUESTION: 92
Which of the following BEST describes a technique that compensates researchers for finding vulnerabilities?
A. Penetration testing
B. Code review
C. Wardriving
D. Bug bounty
Answer: D (LEAVE A REPLY)
A bug bounty is a technique that compensates researchers for finding vulnerabilities in software or systems. A bug bounty program is an initiative that offers rewards, usually monetary, to ethical hackers who report security flaws to the owners or developers of the software or system. Bug bounty programs are often used by companies such as Meta (formerly Facebook),

Google, Microsoft, and others to improve the security of their products and services Bug bounty programs compensate researchers, often financially, for finding vulnerabilities in software, websites, or other technology. These programs provide an additional layer of security testing and incentivize researchers to report vulnerabilities instead of exploiting them.

NEW QUESTION: 93
Which of the following conditions impacts data sovereignty?
A. Rights management
B. Criminal investigations
C. Healthcare data
D. International operations
Answer: D (LEAVE A REPLY)
Data sovereignty refers to the legal concept that data is subject to the laws and regulations of the country in which it is located. International operations can impact data sovereignty as companies operating in multiple countries may need to comply with different laws and regulations. Reference:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 5

NEW QUESTION: 94
A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the companVs mobile application. After reviewing the back-end server logs, the security analyst finds the following entries Which of the following is the most likely cause of the security control bypass?
A. IP address allow list
B. user-agent spoofing
C. WAF bypass
D. Referrer manipulation
Answer: B (LEAVE A REPLY)
User-agent spoofing is a technique that allows an attacker to modify the user-agent header of an HTTP request to impersonate another browser or device12. User-agent spoofing can be used to bypass security controls that rely on user-agent filtering or validation12. In this case, the attacker spoofed the user-agent header to match the company's mobile application, which was allowed to access the back-end server's API2.

NEW QUESTION: 95
A financial institution recently joined a bug bounty program to identify security issues in the institution's new public platform. Which of the following best describes who the institution is working with to identify security issues?
A. Script kiddie
B. Insider threats
C. Malicious actor
D. Authorized hacker
Answer: D (LEAVE A REPLY)

An authorized hacker, also known as an ethical hacker or a white hat hacker, is someone who uses their skills and knowledge to find and report security issues in a system or application with the permission of the owner. An authorized hacker follows the rules and guidelines of the bug bounty program and does not cause any harm or damage to the system or its users.

NEW QUESTION: 96
A network security manager wants to implement periodic events that will test the security team's preparedness for incidents in a controlled and scripted manner, Which of the following concepts describes this scenario?
A. Red-team exercise
B. Business continuity plan testing
C. Tabletop exercise
D. Functional exercise
Answer: (SHOW ANSWER)
A tabletop exercise is a type of security exercise that involves a simulated scenario of a security incident and a discussion of how the security team would respond to it1. A tabletop exercise is a low-impact and cost-effective way to test the security team's preparedness, identify gaps and areas for improvement, and enhance communication and coordination among team members2. A tabletop exercise is different from a red-team exercise, which is a simulated attack by an authorized group of ethical hackers to test the security defenses and response capabilities of an organization3. A business continuity plan testing is a process of verifying that an organization can continue its essential functions and operations in the event of a disaster or disruption4. A functional exercise is a type of security exercise that involves a realistic simulation of a security incident and requires the security team to perform their roles and responsibilities as if it were a real event.

NEW QUESTION: 97
A store receives reports that shoppers' credit card information is being stolen. Upon further analysis, those same shoppers also withdrew money from an ATM in that store.
The attackers are using the targeted shoppers' credit card information to make online purchases. Which of the following attacks is the MOST probable cause?
A. Identity theft
B. RFID cloning
C. Shoulder surfing
D. Card skimming
Answer: D (LEAVE A REPLY)
The attackers are using card skimming to steal shoppers' credit card information, which they use to make online purchases.
Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 5

NEW QUESTION: 98
A company would like to provide flexibility for employees on device preference. However, the company is concerned about supporting too many different types of hardware. Which of the following deployment models will provide the needed flexibility with the GREATEST amount of control and security over company data and infrastructure?
A. BYOD
B. VDI

C. COPE
D. CYOD
Answer: D (LEAVE A REPLY)
Choose Your Own Device (CYOD) is a deployment model that allows employees to select from a predefined list of devices. It provides employees with flexibility in device preference while allowing the company to maintain control and security over company data and infrastructure. CYOD deployment model provides a compromise between the strict control provided by Corporate-Owned, Personally Enabled (COPE) deployment model and the flexibility provided by Bring Your Own Device (BYOD) deployment model. Reference: CompTIA Security+ Study Guide, Chapter 6: Securing Application, Data, and Host Security, 6.5 Implement Mobile Device Management, pp. 334-335

NEW QUESTION: 99
An organization wants to quickly assess how effectively the IT team hardened new laptops Which of the following would be the best solution to perform this assessment?
A. Install a SIEM tool and properly configure it to read the OS configuration files.
B. Load current baselines into the existing vulnerability scanner.
C. Maintain a risk register with each security control marked as compliant or non-compliant.
D. Manually review the secure configuration guide checklists.
Answer: (SHOW ANSWER)
A vulnerability scanner is a tool that can scan devices and systems for known vulnerabilities, misconfigurations, and compliance issues. By loading the current baselines into the scanner, the organization can compare the actual state of the new laptops with the desired state and identify any deviations or weaknesses. This is a quick and automated way to assess the hardening of the new laptops.

NEW QUESTION: 100
A security administrator is managing administrative access to sensitive systems with the following requirements:
* Common login accounts must not be used for administrative duties.
* Administrative accounts must be temporal in nature.
* Each administrative account must be assigned to one specific user.
* Accounts must have complex passwords.
" Audit trails and logging must be enabled on all systems.
Which of the following solutions should the administrator deploy to meet these requirements? (Give Explanation and Reference from CompTIA Security+ SY0-601 Official Text Book and Resources)
A. ABAC
B. SAML
C. PAM
D. CASB
Answer: C (LEAVE A REPLY)
PAM is a solution that enables organizations to securely manage users' accounts and access to sensitive systems. It allows administrators to create unique and complex passwords for each user, as well as assign each account to a single user for administrative duties. PAM also provides audit trails and logging capabilities, allowing administrators to monitor user activity and

ensure that all systems are secure. According to the CompTIA Security+ SY0-601 Course Book, "PAM is the most comprehensive way to control and monitor privileged accounts".

NEW QUESTION: 101
An employee received multiple messages on a mobile device. The messages instructing the employee to pair the device to an unknown device. Which of the following BEST describes What a malicious person might be doing to cause this issue to occur?
A. Jamming
B. Bluesnarfing
C. Evil twin
D. Rogue access point
Answer: B (LEAVE A REPLY)
Bluesnarfing is a hacking technique that exploits Bluetooth connections to snatch data from a wireless device. An attacker can perform bluesnarfing when the Bluetooth function is on and your device is discoverable by other devices within range. In some cases, attackers can even make calls from their victim's phone1.

NEW QUESTION: 102
A security analyst is investigating a report from a penetration test. During the penetration test, consultants were able to download sensitive data from a back-end server. The back-end server was exposing an API that should have only been available from the company's mobile application. After reviewing the back-end server logs, the security analyst finds the following entries:
Which of the following is the most likely cause of the security control bypass?
A. IP address allow list
B. User-agent spoofing
C. WAF bypass
D. Referrer manipulation
Answer: B (LEAVE A REPLY)
User-agent spoofing is a technique that involves changing the user-agent string of a web browser or other client to impersonate another browser or device. The user-agent string is a piece of information that identifies the client to the web server and can contain details such as the browser name, version, operating system, and device type. User-agent spoofing can be used to bypass security controls that rely on the user-agent string to determine the legitimacy of a request. In this scenario, the consultants were able to spoof the user-agent string of the company's mobile application and access the API that should have been restricted to it.

NEW QUESTION: 103
During a forensic investigation, a security analyst discovered that the following command was run on a compromised host:
Which of the following attacks occurred?
A. Buffer overflow
B. Pass the hash
C. SQL injection
D. Replay attack
Answer: (SHOW ANSWER)

Pass the hash is an attack technique that allows an attacker to authenticate to a remote server or service by using the hashed version of a user's password, rather than requiring the plaintext password

NEW QUESTION: 104
A Chief Information Security Officer (CISO) wants to implement a new solution that can protect against certain categories of websites, whether the employee is in the offer or away. Which of the following solutions should the CISO implement?
A. VAF
B. SWG
C. VPN
D. WDS
Answer: B (LEAVE A REPLY)
A secure web gateway (SWG) is a solution that can filter and block malicious or inappropriate web traffic based on predefined policies. It can protect users from web-based threats, such as malware, phishing, or ransomware, whether they are in the office or away. An SWG can be deployed as a hardware appliance, a software application, or a cloud service. Reference: https://www.comptia.org/content/guides/what-is-a-secure-web-gateway

NEW QUESTION: 105
The security team received a report of copyright infringement from the IP space of the corporate network. The report provided a precise time stamp for the incident as well as the name of the copyrighted files. The analyst has been tasked with determining the infringing source machine and instructed to implement measures to prevent such incidents from occurring again. Which of the following is MOST capable of accomplishing both tasks?
A. HIDS
B. Allow list
C. TPM
D. NGFW
Answer: (SHOW ANSWER)
Next-Generation Firewalls (NGFWs) are designed to provide advanced threat protection by combining traditional firewall capabilities with intrusion prevention, application control, and other security features. NGFWs can detect and block unauthorized access attempts, malware infections, and other suspicious activity. They can also be used to monitor file access and detect unauthorized copying or distribution of copyrighted material.
A next-generation firewall (NGFW) can be used to detect and prevent copyright infringement by analyzing network traffic and blocking unauthorized transfers of copyrighted material. Additionally, NGFWs can be configured to enforce access control policies that prevent unauthorized access to sensitive resources. Reference:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 6

NEW QUESTION: 106
An organization is concerned about hackers potentially entering a facility and plugging in a remotely accessible Kali Linux box. Which of the following should be the first lines of defense against such an attack? (Select TWO).
A. MAC filtering
B. Zero trust segmentation
C. Network access control

D. Access control vestibules
E. Guards
F. Bollards.
Answer: (SHOW ANSWER)
MAC filtering is a method of allowing or denying access to a network based on the MAC address of the device attempting to connect. By creating a list of approved MAC addresses, the organization can prevent unauthorized devices from connecting to the network.
Network Access Control (NAC) is a security solution that allows organizations to restrict access to their networks based on the device's identity, configuration, and security posture. This can be used to ensure that only legitimate devices are allowed to connect to the network, and any unauthorized devices are blocked.

NEW QUESTION: 107
A security analyst is taking part in an evaluation process that analyzes and categorizes threat actors Of real-world events in order to improve the incident response team's process. Which Of the following is the analyst most likely participating in?
A. MITRE ATT&CK
B. Walk-through
C. Red team
D. Purple team-I
E. TAXI
Answer: A (LEAVE A REPLY)
MITRE ATT&CK is a knowledge base and framework that analyzes and categorizes threat actors and real-world events based on their tactics, techniques and procedures. It can help improve the incident response team's process by providing a common language and reference for identifying, understanding and mitigating threats

NEW QUESTION: 108
A security team suspects that the cause of recent power consumption overloads is the unauthorized use of empty power outlets in the network rack Which of the following options will mitigate this issue without compromising the number of outlets available?
A. Adding a new UPS dedicated to the rack
B. Installing a managed PDU
C. Using only a dual power supplies unit
D. Increasing power generator capacity
Answer: B (LEAVE A REPLY)

A managed Power Distribution Unit (PDU) allows you to monitor and control power outlets on the rack. This will allow the security team to identify which devices are drawing power and from which outlets, which can help to identify any unauthorized devices. Moreover, with a managed PDU, you can also control the power to outlets, turn off outlets that are not in use, and set up alerts if an outlet is overloaded. This will help to mitigate the issue of power consumption overloads without compromising the number of outlets available.

NEW QUESTION: 109
Which ol the following is required in order (or an IDS and a WAF to be effective on HTTPS traffic?
A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking
Answer: C (LEAVE A REPLY)
TLS (Transport Layer Security) is a protocol that is used to encrypt data sent over HTTPS (Hypertext Transfer Protocol Secure). In order for an intrusion detection system (IDS) and a web application firewall (WAF) to be effective on HTTPS traffic, they must be able to inspect the encrypted traffic. TLS inspection allows the IDS and WAF to decrypt and inspect the traffic, allowing them to detect any malicious activity. Reference: [1] CompTIA Security+ Study Guide Exam SY0-601 [1], Sixth Edition, Chapter 11, "Network Security Monitoring" [2] CompTIA Security+ Get Certified Get Ahead: SY0-501 Study Guide, Chapter 7, "Intrusion Detection and Prevention"

NEW QUESTION: 110
A company recently decided to allow its employees to use their personally owned devices for tasks like checking email and messaging via mobile applications. The company would like to use MDM, but employees are concerned about the loss of personal dat a. Which of the following should the IT department implement to BEST protect the company against company data loss while still addressing the employees' concerns?
A. Enable the remote-wiping option in the MDM software in case the phone is stolen.
B. Configure the MDM software to enforce the use of PINs to access the phone.
C. Configure MDM for FDE without enabling the lock screen.
D. Perform a factory reset on the phone before installing the company's applications.
Answer: C (LEAVE A REPLY)
MDM software is a type of remote asset-management software that runs from a central server. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets. It can monitor and regulate both corporate-owned and personally owned devices to the organization's policies.
FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage. FDE can protect data from unauthorized access in case the device is lost or stolen.
If a company decides to allow its employees to use their personally owned devices for work tasks, it should configure MDM software to enforce FDE on those devices. This way, the company can protect its data from being exposed if the device falls into the wrong hands.
However, employees may be concerned about the loss of personal data if the company also enables the remote-wiping option in the MDM software. Remote wiping is a feature that allows the company to erase all data on a device remotely in case of theft or loss. Remote wiping can also affect personal data on the device, which may not be acceptable to employees.

Therefore, a possible compromise is to configure MDM for FDE without enabling the lock screen. This means that the device will be encrypted, but it will not require a password or PIN to unlock it. This way, employees can access their personal data easily, while the company can still protect its data with encryption.
The other options are not correct because:
a) Enable the remote-wiping option in the MDM software in case the phone is stolen. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. Remote wiping can erase both work and personal data on the device, which may not be desirable for employees.
b) Configure the MDM software to enforce the use of PINs to access the phone. This option may enhance the security of the device, but it may not address the company's concern about data loss. PINs can be guessed or bypassed by attackers, and they do not protect data if the device is physically accessed.
d) Perform a factory reset on the phone before installing the company's applications. This option may address the company's concern about data loss, but it may not address the employees' concern about personal data loss. A factory reset will erase all data on the device, including personal data, which may not be acceptable to employees.
According to CompTIA Security+ SY0-601 Exam Objectives 2.4 Given a scenario, implement secure systems design:
"MDM software is a type of remote asset-management software that runs from a central server1. It is used by businesses to optimize the functionality and security of their mobile devices, including smartphones and tablets2."
"FDE stands for full disk encryption, which is a method of encrypting all data on a device's storage3."

NEW QUESTION: 111
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?
A. Dictionary
B. Rainbow table
C. Spraying
D. Brute-force
Answer: C (LEAVE A REPLY)
Detailed Password spraying is an attack where an attacker tries a small number of commonly used passwords against a large number of usernames. The goal of password spraying is to avoid detection by avoiding too many failed login attempts for any one user account. The fact that different usernames are being attacked from the same IP address is a strong indication that a password spraying attack is underway.

NEW QUESTION: 112
After multiple on-premises security solutions were migrated to the cloud, the incident response time increased The analysts are spending a long time trying to trace information on different cloud consoles and correlating data in different formats. Which of the following can be used to optimize the incident response time?
A. CASB
B. VPC
C. SWG
D. CMS
Answer: D (LEAVE A REPLY)

CMS (Cloud Management System) is a software or platform that allows an organization to manage and monitor multiple cloud services and resources from a single interface or console. It can optimize the incident response time by providing a centralized view and control of the cloud infrastructure and applications, and enabling faster detection, analysis, and remediation of security incidents across different cloud environments.

NEW QUESTION: 113
During an incident, a company's CIRT determines it is necessary to observe the continued network-based transactions between a callback domain and the malware running on an enterprise PC. Which of the following techniques would be BEST to enable this activity while reducing the nsk of lateral spread and the risk that the adversary would notice any changes?
A. Physically move the PC to a separate Internet point of presence.
B. Create and apply microsegmentation rules,
C. Emulate the malware in a heavily monitored DMZ segment
D. Apply network blacklisting rules for the adversary domain
Answer: C (LEAVE A REPLY)
Emulating the malware in a heavily monitored DMZ segment is the best option for observing network-based transactions between a callback domain and the malware running on an enterprise PC. This approach provides an isolated environment for the malware to run, reducing the risk of lateral spread and detection by the adversary. Additionally, the DMZ can be monitored closely to gather intelligence on the adversary's tactics and techniques. Reference: CompTIA Security+ Study Guide, page 129

NEW QUESTION: 114
The help desk has received calls from users in multiple locations who are unable to access core network services The network team has identified and turned off the network switches using remote commands. Which of the following actions should the network team take NEXT?
A. Disconnect all external network connections from the firewall
B. Send response teams to the network switch locations to perform updates
C. Turn on all the network switches by using the centralized management software
D. Initiate the organization's incident response plan.
Answer: (SHOW ANSWER)
An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned.
If the help desk has received calls from users in multiple locations who are unable to access core network services, it could indicate that a network outage or a denial-of-service attack has occurred. The network team has identified and turned off the network switches using remote commands, which could be a containment measure to isolate the affected devices and prevent further damage.
The next action that the network team should take is to initiate the organization's incident response plan, which would involve notifying the appropriate stakeholders, such as management, security team, legal team, etc., and following the predefined steps to investigate, analyze, document, and resolve the incident.
The other options are not correct because:

a) Disconnect all external network connections from the firewall. This could be another containment measure to prevent external attackers from accessing the network, but it would also disrupt legitimate network traffic and services. This action should be taken only if it is part of the incident response plan and after notifying the relevant parties.
b) Send response teams to the network switch locations to perform updates. This could be a recovery measure to restore normal network operations and apply patches or updates to prevent future incidents, but it should be done only after the incident has been properly identified, contained, and eradicated.
c) Turn on all the network switches by using the centralized management software. This could be a recovery measure to restore normal network operations, but it should be done only after the incident has been properly identified, contained, and eradicated.
According to CompTIA Security+ SY0-601 Exam Objectives 1.5 Given a scenario, analyze indicators of compromise and determine the type of malware:
"An incident response plan is a set of procedures and guidelines that defines how an organization should respond to a security incident. An incident response plan typically includes the following phases: preparation, identification, containment, eradication, recovery, and lessons learned."

NEW QUESTION: 115
Which of the following BEST describes the team that acts as a referee during a penetration-testing exercise?
A. White team
B. Purple team
C. Green team
D. Blue team
E. Red team
Answer: A (LEAVE A REPLY)
During a penetration testing exercise, the white team is responsible for acting as a referee and providing oversight and support to ensure that the testing is conducted safely and effectively. They may also be responsible for determining the rules and guidelines of the exercise, monitoring the progress of the teams, and providing feedback and insights on the strengths and weaknesses of the organization's security measures.

NEW QUESTION: 116
A security analyst is looking for a solution to help communicate to the leadership team the seventy levels of the organization's vulnerabilities. Which of the following would best meet this need?
A. CVE
B. SIEM
C. SOAR
D. CVSS
Answer: (SHOW ANSWER)
CVSS (Common Vulnerability Scoring System) is a framework and a metric that provides a standardized and consistent way of assessing and communicating the severity levels of vulnerabilities. It assigns a numerical score and a vector string to each vulnerability based on various factors, such as exploitability, impact, scope, etc. It can help communicate to the leadership team the severity levels of the organization's vulnerabilities by providing a quantitative and qualitative measure of the risks and the potential impacts.

NEW QUESTION: 117
A corporate security team needs to secure the wireless perimeter of its physical facilities to ensure only authorized users can access corporate resources. Which of the following should the security team do? (Refer the answer from CompTIA SY0-601 Security+ documents or guide at comptia.org)
A. Identify rogue access points.
B. Check for channel overlaps.
C. Create heat maps.
D. Implement domain hijacking.
Answer: A (LEAVE A REPLY)
Based on CompTIA SY0-601 Security+ guide, the answer to the question is A. Identify rogue access points.
To secure the wireless perimeter of its physical facilities, the corporate security team should focus on identifying rogue access points, which are unauthorized access points that have been set up by employees or outsiders to bypass security controls. By identifying and removing these rogue access points, the team can ensure that only authorized users can access corporate resources through the wireless network.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION: 118
A new security engineer has started hardening systems. One of the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability to use SCP to transfer files to the NAS, even through the data is still viewable from the user's PCs. Which of the following is the most likely cause of this issue?
A. TFTP was disabled on the local hosts
B. SSH was turned off instead of modifying the configuration file
C. Remote login was disabled in the networkd.config instead of using the sshd.conf
D. Network services are no longer running on the NAS
Answer: (SHOW ANSWER)
SSH stands for Secure Shell Protocol, which is a cryptographic network protocol that allows secure remote login and command execution on a network device12. SSH can encrypt both the authentication information and the data being exchanged between the client and the server2. SSH can be used to access and manage a NAS device remotely3.

NEW QUESTION: 119
A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?
A. A reverse proxy
B. A decryption certificate
C. A split-tunnel VPN
D. Load-balanced servers
Answer: B (LEAVE A REPLY)
A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.

To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

NEW QUESTION: 120
Which of the following biometric authentication methods is the MOST accurate?
A. Gait
B. Retina
C. Signature
D. Voice
Answer: B (LEAVE A REPLY)
Retina authentication is the most accurate biometric authentication method. Retina authentication is based on recognizing the unique pattern of blood vessels and other features in the retina. This makes it virtually impossible to duplicate or bypass, making it the most secure form of biometric authentication currently available.

NEW QUESTION: 121
Which of the following are common VoIP-associated vulnerabilities? (Select two).
A. SPIM
B. Vishing
C. VLAN hopping
D. Phishing
E. DHCP snooping
F. Tailgating
Answer: A,B (LEAVE A REPLY)
SPIM (Spam over Internet Messaging) is a type of VoIP-associated vulnerability that involves sending unsolicited or fraudulent messages over an internet messaging service, such as Skype or WhatsApp. It can trick users into clicking on malicious links, downloading malware, providing personal or financial information, etc., by impersonating a legitimate entity or creating a sense of urgency or curiosity. Vishing (Voice Phishing) is a type of VoIP-associated vulnerability that involves making unsolicited or fraudulent phone calls over an internet telephony service, such as Google Voice or Vonage. It can trick users into disclosing personal or financial information, following malicious instructions, transferring money, etc., by using voice spoofing, caller ID spoofing, or interactive voice response systems.

NEW QUESTION: 122

A network engineer and a security engineer are discussing ways to monitor network operations. Which of the following is the BEST method?

A. Disable Telnet and force SSH.

B. Establish a continuous ping.

C. Utilize an agentless monitor

D. Enable SNMPv3 With passwords.

Answer: (SHOW ANSWER)

An agentless monitor is the best method to monitor network operations because it does not require any software or agents to be installed on the devices being monitored, making it less intrusive and less likely to disrupt network operations. This method can monitor various aspects of network operations, such as traffic, performance, and security.

CompTIA Security+ Study Guide, Sixth Edition (SY0-601), Chapter 4: Attacks, Threats, and Vulnerabilities, Monitoring and Detection Techniques, pg. 167-170.

NEW QUESTION: 123

Audit logs indicate an administrative account that belongs to a security engineer has been locked out multiple times during the day. The security engineer has been on vacation (or a few days. Which of the following attacks can the account lockout be attributed to?

A. Backdoor

B. Brute-force

C. Rootkit

D. Trojan

Answer: (SHOW ANSWER)

The account lockout can be attributed to a brute-force attack. A brute-force attack is a type of attack where an attacker attempts to guess a user's password by continually trying different combinations of characters. In this case, it is likely that the security engineer's account was locked out due to an attacker attempting to guess their password. Backdoor, rootkit, and Trojan attacks are not relevant in this scenario.

NEW QUESTION: 124

Which of the following is most likely to contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented?

A. An RTO report

B. A risk register

C. A business impact analysis

D. An asset value register

E. A disaster recovery plan

Answer: B (LEAVE A REPLY)

A risk register is a document or a tool that records and tracks information about the identified risks and their analysis, such as likelihood, impact, priority, mitigation strategies, residual risks, etc. It can contain ranked and ordered information on the likelihood and potential impact of catastrophic events that may affect business processes and systems, while also highlighting the residual risks that need to be managed after mitigating controls have been implemented.

NEW QUESTION: 125
After gaining access to a dual-homed (i.e.. wired and wireless) multifunction device by exploiting a vulnerability in the device's firmware, a penetration tester then gains shell access on another networked asset This technique is an example of:
A. privilege escalation
B. footprinting
C. persistence
D. pivoting.
Answer: D (LEAVE A REPLY)
The technique of gaining access to a dual-homed multifunction device and then gaining shell access on another networked asset is an example of pivoting. Reference: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Enumeration and Penetration Testing

NEW QUESTION: 126
While researching a data exfiltration event, the security team discovers that a large amount of data was transferred to a file storage site on the internet. Which of the following controls would work best to reduce the risk of further exfiltration using this method?
A. Data loss prevention
B. Blocking IP traffic at the firewall
C. Containerization
D. File integrity monitoring
Answer: A (LEAVE A REPLY)
Data loss prevention (DLP) is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help reduce the risk of further exfiltration using file storage sites on the internet by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, upload, or download sensitive data to or from file storage sites based on predefined policies and rules.

NEW QUESTION: 127
Which of the following would satisfy three-factor authentication requirements?
A. Password, PIN, and physical token
B. PIN, fingerprint scan, and ins scan
C. Password, fingerprint scan, and physical token
D. PIN, physical token, and ID card
Answer: C (LEAVE A REPLY)
Three-factor authentication combines three types of authentication methods: something you know (password), something you have (physical token), and something you are (fingerprint scan). Option C satisfies these requirements, as it uses a password (something you know), a physical token (something you have), and a fingerprint scan (something you are) for authentication.
Reference:
Note: There could be other options as well that could satisfy the three-factor authentication requirements as per the organization's security policies.

NEW QUESTION: 128
Which of Ihe following control types is patch management classified under?
A. Deterrent
B. Physical
C. Corrective
D. Detective
Answer: C (LEAVE A REPLY)
Patch management is classified as a corrective control because it is used to correct vulnerabilities or weaknesses in systems and applications after they have been identified. It is a reactive approach that aims to fix problems that have already occurred rather than prevent them from happening in the first place.

NEW QUESTION: 129
Which of the following automation use cases would best enhance the security posture Of an organi-zation by rapidly updating permissions when employees leave a company Or change job roles inter-nally?
A. Provisioning resources
B. Disabling access
C. APIs
D. Escalating permission requests
Answer: B (LEAVE A REPLY)
Disabling access is an automation use case that can enhance the security posture of an organization by rapidly updating permissions when employees leave a company or change job roles internally. It can prevent unauthorized access and data leakage by revoking or modifying the access rights of employees based on their current status and role.

NEW QUESTION: 130
Which of the following disaster recovery tests is the LEAST time consuming for the disaster recovery team?
A. Tabletop
B. Parallel
C. Full interruption
D. Simulation
Answer: A (LEAVE A REPLY)
A tabletop exercise is a type of disaster recovery test that simulates a disaster scenario in a discussion-based format, without actually disrupting operations or requiring physical testing of recovery procedures. It is the least time-consuming type of test for the disaster recovery team.

NEW QUESTION: 131
An account was disabled atter several failed and successful login connections were made from various parts of the Word at various times. A security analysts investigating the issue. Which of the following account policies most likely triggered the action to disable the
A. Time based logins
B. Password history
C. Geofencing

D. Impossible travel time

Answer: D (LEAVE A REPLY)

Impossible travel time is a policy that detects and blocks login attempts from locations that are geographically impossible to reach from the previous login location within a certain time frame. For example, if a user logs in from New York and then tries to log in from Tokyo within an hour, the policy would flag this as impossible travel time and disable the account. This policy helps prevent unauthorized access from compromised credentials or attackers using proxy servers. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 6, Domain 1.0: Attacks, Threats, and Vulnerabilities, Objective 1.2: Compare and contrast different types of social engineering techniques 2 CompTIA Security+ Certification Exam Objectives, page 14, Domain 3.0: Implementation, Objective 3.4: Implement identity and account management controls 3 https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy#impossible-travel

NEW QUESTION: 132

Which Of the following is the best method for ensuring non-repudiation?

A. SSO

B. Digital certificate

C. Token

D. SSH key

Answer: B (LEAVE A REPLY)

A digital certificate is an electronic document that contains the public key and identity information of an entity, such as a person, organization, website, etc. It is issued and signed by a trusted authority called a certificate authority (CA). It can provide non-repudiation by proving the identity and authenticity of the sender and verifying the integrity of the message or data.

NEW QUESTION: 133

Which of the following types of controls is a turnstile?

A. Physical

B. Detective

C. Corrective

D. Technical

Answer: A (LEAVE A REPLY)

A turnstile is a physical security control that regulates the entry and exit of people into a facility or an area. It can prevent unauthorized access, tailgating, etc., by requiring valid credentials or tokens to pass through

NEW QUESTION: 134

A company was compromised, and a security analyst discovered the attacker was able to get access to a service account. The following logs were discovered during the investigation:

Which of the following MOST likely would have prevented the attacker from learning the service account name?

A. Race condition testing

B. Proper error handling

C. Forward web server logs to a SIEM

D. Input sanitization

Answer: D (LEAVE A REPLY)

Input sanitization can help prevent attackers from learning the service account name by removing potentially harmful characters from user input, reducing the likelihood of successful injection attacks. Reference:
CompTIA Security+ Certification Exam Objectives 2.2: Given a scenario, implement secure coding techniques.
CompTIA Security+ Study Guide, Sixth Edition, pages 72-73

NEW QUESTION: 135
A company wants the ability to restrict web access and monitor the websites that employees visit, Which Of the following would best meet these requirements?
A. Internet Proxy
B. VPN
C. WAF
D. Firewall
Answer: A (LEAVE A REPLY)
An internet proxy is a server that acts as an intermediary between a client and a destination server on the internet. It can restrict web access and monitor the websites that employees visit by filtering the requests and responses based on predefined rules and policies, and logging the traffic and activities for auditing purposes

NEW QUESTION: 136
A security administrator needs to block a TCP connection using the corporate firewall, Because this connection is potentially a threat. the administrator not want to back an RST Which of the following actions in rule would work best?
A. Drop
B. Reject
C. Log alert
D. Permit
Answer: A (LEAVE A REPLY)
the difference between drop and reject in firewall is that the drop target sends nothing to the source, while the reject target sends a reject response to the source. This can affect how the source handles the connection attempt and how fast the port scanning is. In this context, a human might say that the best action to block a TCP connection using the corporate firewall is A. Drop, because it does not send back an RST packet and it may slow down the port scanning and protect against DoS attacks.

NEW QUESTION: 137
A financial institution would like to store its customer data in a cloud but still allow the data to be accessed and manipulated while encrypted. Doing so would prevent the cloud service provider from being able to decipher the data due to its sensitivity. The

financial institution is not concerned about computational overheads and slow speeds. Which of the following cryptographic techniques would BEST meet the requirement?

A. Asymmetric

B. Symmetric

C. Homomorphic

D. Ephemeral

Answer: B (LEAVE A REPLY)

Symmetric encryption allows data to be encrypted and decrypted using the same key. This is useful when the data needs to be accessed and manipulated while still encrypted. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 6

NEW QUESTION: 138

Which of the following isa risk that is specifically associated with hesting applications iin the public cloud?

A. Unsecured root accounts

B. Zero day

C. Shared tenancy

D. Insider threat

Answer: C (LEAVE A REPLY)

When hosting applications in the public cloud, there is a risk of shared tenancy, meaning that multiple organizations are sharing the same infrastructure. This can potentially allow one tenant to access another tenant's data, creating a security risk. Reference: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION: 139

A company recently enhanced mobile device configuration by implementing a set of security controls: biometrics, context-aware authentication, and full device encryption. Even with these settings in place, an unattended phone was used by a malicious actor to access corporate data.

Which of the following additional controls should be put in place first?

A. GPS tagging

B. Remote wipe

C. Screen lock timer

D. SEAndroid

Answer: C (LEAVE A REPLY)

According to NIST Special Publication 1800-4B1, some of the security controls that can be used to protect mobile devices include:

Root and jailbreak detection: ensures that the security architecture for a mobile device has not been compromised.

Encryption: protects the data stored on the device and in transit from unauthorized access.

Authentication: verifies the identity of the user and the device before granting access to enterprise resources.

Remote wipe: allows the organization to erase the data on the device in case of loss or theft.

Screen lock timer: sets a time limit for the device to lock itself after a period of inactivity.

NEW QUESTION: 140

A company recently upgraded its authentication infrastructure and now has more computing power. Which of the following should the company consider using to ensure user credentials are being transmitted and stored more securely?

A. Blockchain

B. Salting

C. Quantum

D. Digital signature

Answer: B (LEAVE A REPLY)

Salting is a technique that adds random data to user credentials before hashing them. This makes the hashed credentials more secure and resistant to brute-force attacks or rainbow table attacks. Salting also ensures that two users with the same password will have different hashed credentials.

A company that has more computing power can consider using salting to ensure user credentials are being transmitted and stored more securely. Salting can increase the complexity and entropy of the hashed credentials, making them harder to crack or reverse.

NEW QUESTION: 141

A security engineer is hardening existing solutions to reduce application vulnerabilities. Which of the following solutions should the engineer implement FIRST? (Select TWO)

A. Auto-update

B. HTTP headers

C. Secure cookies

D. Third-party updates

E. Full disk encryption

F. Sandboxing

G. Hardware encryption

Answer: A,F (LEAVE A REPLY)

Auto-update can help keep the app up-to-date with the latest security fixes and enhancements, and reduce the risk of exploitation by attackers who target outdated or vulnerable versions of the app.

Sandboxing can help isolate the app from other processes and resources on the system, and limit its access and permissions to only what is necessary. Sandboxing can help prevent the app from being affected by or affecting other applications or system components, and contain any potential damage in case of a breach.

NEW QUESTION: 142

A candidate attempts to go to but accidentally visits http://comptiia.org. The malicious website looks exactly like the legitimate website. Which of the following best describes this type of attack?

A. Reconnaissance

B. Impersonation

C. Typosquatting

D. Watering-hole

Answer: (SHOW ANSWER)

Typosquatting is a type of cyberattack that involves registering domains with deliberately misspelled names of well-known websites. The attackers do this to lure unsuspecting visitors to alternative websites, typically for malicious purposes. Visitors may

end up at these alternative websites by inadvertently mistyping the name of popular websites into their web browser or by being lured by a phishing scam. The attackers may emulate the look and feel of the legitimate websites and trick users into entering sensitive information or downloading malware.

NEW QUESTION: 143
A company is required to continue using legacy software to support a critical service. Which of the following BEST explains a risk of this practice?
A. Default system configuration
B. Unsecure protocols
C. Lack of vendor support
D. Weak encryption
Answer: C (LEAVE A REPLY)
Using legacy software to support a critical service poses a risk due to lack of vendor support. Legacy software is often outdated and unsupported, which means that security patches and upgrades are no longer available. This can leave the system vulnerable to exploitation by attackers who may exploit known vulnerabilities in the software to gain unauthorized access to the system.

NEW QUESTION: 144
A network analyst is setting up a wireless access point for a home office in a remote, rural location. The requirement is that users need to connect to the access point securely but do not want to have to remember passwords Which of the following should the network analyst enable to meet the requirement?
A. MAC address filtering
B. 802.1X
C. Captive portal
D. WPS
Answer: D (LEAVE A REPLY)
The network analyst should enable Wi-Fi Protected Setup (WPS) to allow users to connect to the wireless access point securely without having to remember passwords. WPS allows users to connect to a wireless network by pressing a button or entering a PIN instead of entering a password.

NEW QUESTION: 145
Which of the following describes software on network hardware that needs to be updated on a rou-tine basis to help address possible vulnerabilities?
A. Vendor management
B. Application programming interface
C. Vanishing
D. Encryption strength
E. Firmware
Answer: (SHOW ANSWER)
Firmware is software that allows your computer to communicate with hardware devices, such as network routers, switches, or firewalls. Firmware updates can fix bugs, improve performance, and enhance security features. Without firmware updates, the devices you connect to your network might not work properly or might be vulnerable to attacks1. You can have Windows

automatically download recommended drivers and firmware updates for your hardware devices1, or you can use a network monitoring software to keep track of the firmware status of your devices2. You should also follow the best practices for keeping devices and software up to date, such as enforcing automatic updates, monitoring update status, and testing updates before deploying them

NEW QUESTION: 146
Which of the following can be used by an authentication application to validate a user's credentials without the need to store the actual sensitive data?
A. Salt string
B. Private Key
C. Password hash
D. Cipher stream
Answer: C (LEAVE A REPLY)
Password hash is a method of storing a user's credentials without the need to store the actual sensitive data. A password hash is a one-way function that transforms the user's password into a fixed-length string of characters that cannot be reversed. The authentication application can then compare the password hash with the stored hash to validate the user's credentials without revealing the original password. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 15, Domain 3.0: Implementation, Objective 3.5: Implement secure authentication mechanisms 2 CompTIA Security+ Certification Exam Objectives, page 16, Domain 3.0: Implementation, Objective 3.6: Implement identity and account management best practices 3 https://www.comptia.org/blog/what-is-password-hashing

NEW QUESTION: 147
A security analyst receives an alert that indicates a user's device is displaying anomalous behavior The analyst suspects the device might be compromised Which of the following should the analyst to first?
A. Reboot the device
B. Set the host-based firewall to deny an incoming connection
C. Update the antivirus definitions on the device
D. Isolate the device
Answer: D (LEAVE A REPLY)
Isolating the device is the first thing that a security analyst should do if they suspect that a user's device might be compromised. Isolating the device means disconnecting it from the network or placing it in a separate network segment to prevent further communication with potential attackers or malicious hosts. Isolating the device can help contain the incident, limit the damage or data loss, preserve the evidence, and facilitate the investigation and remediation.

NEW QUESTION: 148
A cybersecurity analyst at Company A is working to establish a secure communication channel with a counter part at Company B, which is 3,000 miles (4.828 kilometers) away. Which of the following concepts would help the analyst meet this goal m a secure manner?
A. Digital signatures
B. Key exchange
C. Salting

D. PPTP

Answer: (SHOW ANSWER)

Key exchange Short Key exchange is the process of securely sharing cryptographic keys between two parties over a public network. This allows them to establish a secure communication channel and encrypt their messages. There are different methods of key exchange, such as Diffie-Hellman or RSA. Reference: https://www.comptia.org/content/guides/what-is-encryption

NEW QUESTION: 149

A security analyst is investigating network issues between a workstation and a company server. The workstation and server occasionally experience service disruptions, and employees are forced to reconnect to the server. In addition, some reports indicate sensitive information is being leaked from the server to the public.

The workstation IP address is 192.168.1.103, and the server IP address is 192.168.1.101.

The analyst runs arp -a On a separate workstation and obtains the following results:

Which of the following is most likely occurring?

A. Evil twin attack

B. Domain hijacking attack

C. On-path attack

D. MAC flooding attack

Answer: (SHOW ANSWER)

An on-path attack is a type of attack where an attacker places themselves between two devices (such as a workstation and a server) and intercepts or modifies the communications between them. An on-path attacker can collect sensitive information, impersonate either device, or disrupt the service. In this scenario, the attacker is likely using an on-path attack to capture and alter the network traffic between the workstation and the server, causing service disruptions and data leakage.

NEW QUESTION: 150

An information security officer at a credit card transaction company is conducting a framework-mapping exercise with the internal controls. The company recently established a new office in Europe. To which of the following frameworks should the security officer map the existing controls' (Select two).

A. ISO

B. PCI DSS

C. SOC

D. GDPR

E. CSA

F. NIST

Answer: B,D (LEAVE A REPLY)

PCI DSS (Payment Card Industry Data Security Standard) is a set of security standards and requirements for organizations that store, process, or transmit payment card data. It aims to protect cardholder data and prevent fraud and data breaches. GDPR (General Data Protection Regulation) is a regulation that governs the collection, processing, and transfer of personal data of individuals in the European Union. It aims to protect the privacy and rights of data subjects and impose obligations and penalties on data controllers and processors. These are the frameworks that the security officer should map the existing controls to, as they are relevant for a credit card transaction company that has a new office in Europe

NEW QUESTION: 151
A security analyst is running a vulnerability scan to check for missing patches during a suspected security rodent During which of the following phases of the response process is this activity MOST likely occurring?
A. Containment
B. Identification
C. Recovery
D. Preparation
Answer: B (LEAVE A REPLY)
Vulnerability scanning is a proactive security measure used to identify vulnerabilities in the network and systems. Reference: CompTIA Security+ Study Guide 601, Chapter 4

NEW QUESTION: 152
Which of the following would be BEST for a technician to review to determine the total risk an organization can bear when assessing a "cloud-first" adoption strategy?
A. Risk matrix
B. Risk tolerance
C. Risk register
D. Risk appetite
Answer: B (LEAVE A REPLY)
To determine the total risk an organization can bear, a technician should review the organization's risk tolerance, which is the amount of risk the organization is willing to accept. This information will help determine the organization's "cloud-first" adoption strategy. Reference: CompTIA Security+ Certification Exam Objectives (SY0-601)

NEW QUESTION: 153
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?
A. A DMZ
B. A VPN a
C. A VLAN
D. An ACL
Answer: D (LEAVE A REPLY)

After segmenting the network, a network manager can use an access control list (ACL) to control the traffic between the segments. An ACL is a set of rules that permit or deny traffic based on its characteristics, such as the source and destination IP addresses, protocol type, and port number. Reference: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION: 154
Which of the following involves the inclusion of code in the main codebase as soon as it is written?
A. Continuous monitoring
B. Continuous deployment
C. Continuous Validation
D. Continuous integration
Answer: D (LEAVE A REPLY)
Detailed Continuous Integration (CI) is a practice where developers integrate code into a shared repository frequently, preferably several times a day. Each integration is verified by an automated build and automated tests. CI allows for the detection of errors early in the development cycle, thereby reducing overall development costs.

NEW QUESTION: 155
Which of the following security design features can an development team to analyze the deletion eoting Of data sets the copy?
A. Code reuse
B. Stored procedures
C. Version control
D. Continunus
Answer: (SHOW ANSWER)

NEW QUESTION: 156
Which of the following procedures would be performed after the root cause of a security incident has been identified to help avoid future incidents from occurring?
A. Walk-throughs
B. Lessons learned
C. Attack framework alignment
D. Containment
Answer: B (LEAVE A REPLY)
After the root cause of a security incident has been identified, it is important to take the time to analyze what went wrong and how it could have been prevented. This process is known as "lessons learned" and allows organizations to identify potential improvements to their security processes and protocols. Lessons learned typically involve a review of the incident and the steps taken to address it, a review of the security systems and procedures in place, and an analysis of any potential changes that can be made to prevent similar incidents from occurring in the future.

NEW QUESTION: 157
A security administrator is seeking a solution to prevent unauthorized access to the internal network. Which of the following security solutions should the administrator choose?
A. MAC filtering

B. Anti-malware
C. Translation gateway
D. VPN
Answer: (SHOW ANSWER)
A VPN (virtual private network) is a secure tunnel used to encrypt traffic and prevent unauthorized access to the internal network. It is a secure way to extend a private network across public networks, such as the Internet, and can be used to allow remote users to securely access resources on the internal network. Additionally, a VPN can be used to prevent malicious traffic from entering the internal network.

NEW QUESTION: 158
A Chief Information Officer is concerned about employees using company-issued laptops to steal data when accessing network shares. Which of the following should the company implement?
A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI
Answer: (SHOW ANSWER)
The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data. Reference: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION: 159
The new Chief Information Security Officer at a company has asked the security learn to implement stronger user account policies. The new policies require:
* Users to choose a password unique to their last ten passwords
* Users to not log in from certain high-risk countries
Which of the following should the security team implement? (Select two).
A. Password complexity
B. Password history
C. Geolocation
D. Geospatial
E. Geotagging
F. Password reuse
Answer: (SHOW ANSWER)
Password history is a policy that prevents users from reusing their previous passwords. This can reduce the risk of password cracking or compromise. Geolocation is a policy that restricts users from logging in from certain locations based on their IP address. This can prevent unauthorized access from high-risk countries or regions. Reference: https://www.comptia.org/content/guides/what-is-identity-and-access-management

NEW QUESTION: 160

A network penetration tester has successfully gained access to a target machine. Which of the following should the penetration tester do next?

A. Clear the log files of all evidence

B. Move laterally to another machine.

C. Establish persistence for future use.

D. Exploit a zero-day vulnerability.

Answer: C (LEAVE A REPLY)

Establishing persistence for future use is the next step that a network penetration tester should do after gaining access to a target machine. Persistence means creating a backdoor or a covert channel that allows the penetration tester to maintain access to the target machine even if the initial exploit is patched or the connection is lost. Persistence can be achieved by installing malware, creating hidden user accounts, modifying registry keys, or setting up remote access tools. Establishing persistence can help the penetration tester to perform further reconnaissance, move laterally to other machines, or exfiltrate data from the target network.

NEW QUESTION: 161

After a phishing scam fora user's credentials, the red team was able to craft payload to deploy on a server. The attack allowed the installation of malicious software that initiates a new remote session Which of the following types of attacks has occurred?

A. Privilege escalation

B. Session replay

C. Application programming interface

D. Directory traversal

Answer: A (LEAVE A REPLY)

"Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user." In this scenario, the red team was able to install malicious software, which would require elevated privileges to access and install. Therefore, the type of attack that occurred is privilege escalation. Reference: CompTIA Security+ Study Guide, pages 111-112

NEW QUESTION: 162

Which of the following would produce the closet experience of responding to an actual incident response scenario?

A. Lessons learned

B. Simulation

C. Walk-through

D. Tabletop

Answer: B (LEAVE A REPLY)

A simulation exercise is designed to create an experience that is as close as possible to a real-world incident response scenario. It involves simulating an attack or other security incident and then having security personnel respond to the situation as they would in a real incident. Reference: CompTIA Security+ SY0-601 Exam Objectives: 1.1 Explain the importance of implementing security concepts, methodologies, and practices.

NEW QUESTION: 163

A company policy requires third-party suppliers to self-report data breaches within a specific time frame. Which of the following third-party risk management policies is the company complying with?

A. MOU
B. SLA
C. EOL
D. NDA
Answer: (SHOW ANSWER)
An SLA or service level agreement is a type of third-party risk management policy that defines the expectations and obligations between a service provider and a customer. An SLA typically includes metrics and standards for measuring the quality and performance of the service, as well as penalties or remedies for non-compliance. An SLA can also specify the reporting requirements for data breaches or other incidents that may affect the customer's security or privacy.

NEW QUESTION: 164
An organization has hired a security analyst to perform a penetration test The analyst captures 1Gb worth of inbound network traffic to the server and transfers the pcap back to the machine for analysis. Which of the following tools should the analyst use to further review the pcap?
A. Nmap
B. CURL
C. Neat
D. Wireshark
Answer: (SHOW ANSWER)
Wireshark is a tool that can analyze pcap files, which are files that capture network traffic. Wireshark can display the packets, protocols, and other details of the network traffic in a graphical user interface. Nmap is a tool that can scan networks and hosts for open ports and services. CURL is a tool that can transfer data from or to a server using various protocols. Neat is a tool that can test network performance and quality.

NEW QUESTION: 165
A security analyst reports a company policy violation in a case in which a large amount of sensitive data is being downloaded after hours from various mobile devices to an external site. Upon further investigation, the analyst notices that successful login attempts are being conducted with impossible travel times during the same time periods when the unauthorized downloads are occurring. The analyst also discovers a couple of WAPs are using the same SSID, but they have non-standard DHCP configurations and an overlapping channel. Which of the following attacks is being conducted?
A. Evil twin
B. Jamming
C. DNS poisoning
D. Bluesnarfing
E. DDoS
Answer: (SHOW ANSWER)
The attack being conducted is an Evil twin attack. An Evil twin attack involves creating a rogue wireless access point (WAP) with the same Service Set Identifier (SSID) as a legitimate WAP to trick users into connecting to it. Once connected, the attacker can intercept traffic or steal login credentials. The successful login attempts with impossible travel times suggest that an attacker is using a stolen or compromised credential to access the external site to which the sensitive data is being downloaded. The non-standard DHCP configurations and overlapping channels of the WAPs suggest that the attacker is using a rogue WAP to intercept

traffic. Reference: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.4 Compare and contrast types of attacks, p. 8

NEW QUESTION: 166
The Chief Technology Officer of a local college would like visitors to utilize the school's WiFi but must be able to associate potential malicious activity to a specific person. Which of the following would BEST allow this objective to be met?
A. Requiring all new, on-site visitors to configure their devices to use WPS
B. Implementing a new SSID for every event hosted by the college that has visitors
C. Creating a unique PSK for every visitor when they arrive at the reception area
D. Deploying a captive portal to capture visitors' MAC addresses and names
Answer: D (LEAVE A REPLY)
A captive portal is a web page that requires visitors to authenticate or agree to an acceptable use policy before allowing access to the network. By capturing visitors' MAC addresses and names, potential malicious activity can be traced back to a specific person.

NEW QUESTION: 167
A network analyst is investigating compromised corporate information. The analyst leads to a theory that network traffic was intercepted before being transmitted to the internet. The following output was captured on an internal host:
Based on the IoCS, which of the following was the MOST likely attack used to compromise the network communication?
A. Denial of service
B. ARP poisoning
C. Command injection
D. MAC flooding
Answer: (SHOW ANSWER)
ARP poisoning (also known as ARP spoofing) is a type of attack where an attacker sends falsified ARP messages over a local area network to link the attacker's MAC address with the IP address of another host on the network. Reference: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 6, page 271.

NEW QUESTION: 168
A user reports constant lag and performance issues with the wireless network when working at a local coffee shop A security analyst walks the user through an installation of Wireshark and gets a five-minute pcap to analyze. The analyst observes the following output:

Which of the following attacks does the analyst most likely see in this packet capture?

A. Session replay

B. Evil twin

C. Bluejacking

D. ARP poisoning

Answer: B (LEAVE A REPLY)

An evil twin is a type of wireless network attack that involves setting up a rogue access point that mimics a legitimate one. It can trick users into connecting to the rogue access point instead of the real one, and then intercept or modify their traffic, steal their credentials, launch phishing pages, etc. In this packet capture, the analyst can see that there are two access points with the same SSID (CoffeeShop) but different MAC addresses (00:0c:41:82:9c:4f and 00:0c:41:82:9c:4e). This indicates that one of them is an evil twin that is trying to impersonate the other one.

NEW QUESTION: 169

A junior human resources administrator was gathering data about employees to submit to a new company awards program The employee data included job title business phone number location first initial with last name and race Which of the following best describes this type of information?

A. Sensitive

B. Non-PII

C. Private

D. Confidential

Answer: B (LEAVE A REPLY)

Non-PII stands for non-personally identifiable information, which is any data that does not directly identify a specific individual. Non-PII can include information such as job title, business phone number, location, first initial with last name, and race. Non-PII can be used for various purposes, such as statistical analysis, marketing, or research. However, non-PII may still pose some privacy risks if it is combined or linked with other data that can reveal an individual's identity.

NEW QUESTION: 170

Given the following snippet of Python code:

Which of the following types of malware MOST likely contains this snippet?

A. Logic bomb

B. Keylogger

C. Backdoor

D. Ransomware

Answer: (SHOW ANSWER)

A logic bomb is a type of malware that executes malicious code when certain conditions are met. A logic bomb can be triggered by various events, such as a specific date or time, a user action, a system configuration change, or a command from an attacker. A logic bomb can perform various malicious actions, such as deleting files, encrypting data, displaying messages, or launching other malware.

The snippet of Python code shows a logic bomb that executes a function called delete_all_files() when the current date is December 25th. The code uses the datetime module to get the current date and compare it with a predefined date object. If the condition is true, the code calls the delete_all_files() function, which presumably deletes all files on the system.

NEW QUESTION: 171
During a security assessment, a security finds a file with overly permissive permissions. Which of the following tools will allow the analyst to reduce the permission for the existing users and groups and remove the set-user-ID from the file?
A. 1s
B. chflags
C. chmod
D. lsof
E. setuid
Answer: C (LEAVE A REPLY)
The chmod command is used to change the permissions of a file or directory. The analyst can use chmod to reduce the permissions for existing users and groups and remove the set-user-ID bit from the file. Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION: 172
A company recently experienced a major breach. An investigation concludes that customer credit card data was stolen and exfiltrated through a dedicated business partner connection to a vendor, who is not held to the same security contral standards. Which of the following is the MOST likely source of the breach?
A. Side channel
B. Supply chain
C. Cryptographic downgrade
D. Malware
Answer: (SHOW ANSWER)
A supply chain attack occurs when a third-party supplier or business partner is compromised, leading to an attacker gaining unauthorized access to the targeted organization's network. In this scenario, the dedicated business partner connection to a vendor was used to exfiltrate customer credit card data, indicating that the vendor's network was breached and used as a supply chain attack vector.

NEW QUESTION: 173
A security engineer is concerned the strategy for detection on endpoints is too heavily dependent on previously defined attacks. The engineer wants a tool that can monitor for changes to key files and network traffic for the device. Which of the following tools should the engineer select?
A. HIDS
B. AV
C. NGF-W
D. DLP
Answer: A (LEAVE A REPLY)
The security engineer should select a Host Intrusion Detection System (HIDS) to address the concern. HIDS monitors and analyzes the internals of a computing system, such as key files and network traffic, for any suspicious activity. Unlike antivirus software (AV), which relies on known signatures of malware, HIDS can detect anomalies, policy violations, and previously undefined attacks by monitoring system behavior and the network traffic of the device.

Reference:
1. CompTIA Security+ Certification Exam Objectives (SY0-601): https://www.comptia.jp/pdf/Security%2B%20SY0-601%20Exam%20Objectives.pdf
2. Scarfone, K., & Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-94. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

NEW QUESTION: 174
An organization needs to implement more stringent controls over administrator/root credentials and service accounts.
Requirements for the project include:
* Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?
A. OAuth 2.0
B. Secure Enclave
C. A privileged access management system
D. An OpenID Connect authentication system
Answer: (SHOW ANSWER)
A privileged access management (PAM) system is a solution that helps protect organizations against cyberthreats by monitoring, detecting, and preventing unauthorized privileged access to critical resources12. A PAM system can meet the requirements of the project by providing features such as:
Check-in/checkout of credentials: A PAM system can store and manage privileged credentials in a secure vault, and allow authorized users to check out credentials when needed and check them back in when done. This reduces the risk of credential theft, misuse, or sharing23.
The ability to use but not know the password: A PAM system can enable users to access privileged accounts or resources without revealing the actual password, using methods such as password injection, session proxy, or single sign-on23. This prevents users from copying, changing, or sharing passwords2.
Automated password changes: A PAM system can automatically rotate and update passwords for privileged accounts according to predefined policies, such as frequency, complexity, and uniqueness23. This ensures that passwords are always strong and unpredictable, and reduces the risk of password reuse or compromise2.
Logging of access to credentials: A PAM system can record and audit all activities related to privileged access, such as who accessed what credentials, when, why, and what they did with them23. This provides visibility and accountability for privileged access, and enables detection and investigation of anomalies or incidents2.
A PAM system is different from OAuth 2.0, which is an authorization framework that enables third-party applications to obtain limited access to an HTTP service on behalf of a resource owner4. OAuth 2.0 does not provide the same level of control and security over privileged access as a PAM system does.
A PAM system is also different from a secure enclave, which is a hardware-based security feature that creates an isolated execution environment within a processor to protect sensitive data from unauthorized access or modification5. A secure enclave does not provide the same functionality as a PAM system for managing privileged credentials and access.

A PAM system is also different from an OpenID Connect authentication system, which is an identity layer on top of OAuth 2.0 that enables users to verify their identity across multiple websites using a single login6. OpenID Connect does not provide the same scope and granularity as a PAM system for controlling and monitoring privileged access.

NEW QUESTION: 175
A security administrator installed a new web server. The administrator did this to increase the capacity for an application due to resource exhaustion on another server. Which of the following algorithms should the administrator use to split the number of the connections on each server in half?
A. Weighted response
B. Round-robin
C. Least connection
D. Weighted least connection
Answer: B (LEAVE A REPLY)
Round-robin is a type of load balancing algorithm that distributes traffic to a list of servers in rotation. It is a static algorithm that does not take into account the state of the system for the distribution of tasks. It assumes that all servers have equal capacity and can handle an equal amount of traffic.

NEW QUESTION: 176
A cybersecurity administrator needs to allow mobile BYOD devices to access network resources. As the devices are not enrolled to the domain and do not have policies applied to them, which of the following are best practices for authentication and infrastructure security? (Select TWO).
A. Create a new network for the mobile devices and block the communication to the internal network and servers
B. Use a captive portal for user authentication.
C. Authenticate users using OAuth for more resiliency
D. Implement SSO and allow communication to the internal network
E. Use the existing network and allow communication to the internal network and servers.
F. Use a new and updated RADIUS server to maintain the best solution
Answer: B,C (LEAVE A REPLY)
When allowing mobile BYOD devices to access network resources, using a captive portal for user authentication and authenticating users using OAuth are both best practices for authentication and infrastructure security. A captive portal requires users to authenticate before accessing the network and can be used to enforce policies and restrictions. OAuth allows users to authenticate using third-party providers, reducing the risk of password reuse and credential theft. Reference: CompTIA Security+ Study Guide, pages 217-218, 225-226

NEW QUESTION: 177
During a security incident the security operations team identified sustained network traffic from a malicious IP address: 10.1.4.9 A security analyst is creating an inbound firewall rule to block the IP address from accessing the organization's network. Which of the following fulfills this request?
A. access-list inbound deny ip source 0.0.0.0/0 destination 10.1.4.9/32
B. access-list inbound deny ip source 10.1.4.9/32 destination 0.0.0.0/0
C. access-list inbound permit ip source 10.1.4.9/32 destination 0.0.0.0/0

D. access-list inbound permit ip source 0.0.0.0/0 destination 10.1.4.9/32

Answer: B (LEAVE A REPLY)

This command creates an inbound access list that denies any IP traffic from the source IP address of 10.1.4.9/32 to any destination IP address (0.0.0.0/0). It blocks the originating source of malicious traffic from accessing the organization's network.

NEW QUESTION: 178

A security operations center wants to implement a solution that can execute files to test for malicious activity. The solution should provide a report of the files' activity against known threats.

Which of the following should the security operations center implement?

A. theHarvester

B. Nessus

C. Cuckoo

D. Sn1per

Answer: C (LEAVE A REPLY)

Cuckoo is a sandbox that is specifically written to run programs inside and identify any malware. A sandbox is a virtualized environment that isolates the program from the rest of the system and monitors its behavior. Cuckoo can analyze files of various types, such as executables, documents, URLs, and more. Cuckoo can provide a report of the files' activity against known threats, such as network traffic, file operations, registry changes, API calls, and so on.

A security operations center can implement Cuckoo to execute files to test for malicious activity and generate a report of the analysis. Cuckoo can help the security operations center to detect and prevent malware infections, investigate incidents, and perform threat intelligence.

NEW QUESTION: 179

A company's help desk has received calls about the wireless network being down and users being unable to connect to it. The network administrator says all access pcints are up and running. One of the help desk technicians notices the affected users are working in a near the parking Jot Which Of the following IS the most likely reason for the outage?

A. Someone near the is jamming the signal.

B. A user has set up a rogue access point near building.

C. Someone set up an evil twin access Print in tie affected area.

D. The APS in the affected area have been from the network

Answer: A (LEAVE A REPLY)

Wireless jamming is a way for an attacker to disrupt a wireless network and create a denial of ser-vice situation by decreasing the signal-to-noise ratio at the receiving device. The attacker would need to be relatively close to the wireless network to overwhelm the good signal. The other options are not likely to cause a wireless network outage for users near the parking lot.

NEW QUESTION: 180

A network-connected magnetic resonance imaging (MRI) scanner at a hospital is controlled and operated by an outdated and unsupported specialized Windows OS. Which of the following is most likely preventing the IT manager at the hospital from upgrading the specialized OS?

A. The time needed for the MRI vendor to upgrade the system would negatively impact patients.

B. The MRI vendor does not support newer versions of the OS.

C. Changing the OS breaches a support SLA with the MRI vendor.
D. The IT team does not have the budget required to upgrade the MRI scanner.
Answer: B (LEAVE A REPLY)
This option is the most likely reason for preventing the IT manager at the hospital from upgrading the specialized OS. The MRI scanner is a complex and sensitive device that requires a specific OS to control and operate it. The MRI vendor may not have developed or tested newer versions of the OS for compatibility and functionality with the scanner. Upgrading the OS without the vendor's support may cause the scanner to malfunction or stop working altogether.

NEW QUESTION: 181
Which of the following authentication methods is considered to be the LEAST secure?
A. TOTP
B. SMS
C. HOTP
D. Token key
Answer: B (LEAVE A REPLY)
SMS-based authentication is considered to be the least secure among the given options. This is because SMS messages can be intercepted or redirected by attackers through techniques such as SIM swapping, man-in-the-middle attacks, or exploiting weaknesses in the SS7 protocol used by mobile networks. Additionally, SMS messages can be compromised if a user's phone is lost, stolen, or infected with malware. In contrast, TOTP (Time-based One-Time Password), HOTP (HMAC-based One-Time Password), and token keys are more secure as they rely on cryptographic algorithms or physical devices to generate one-time use codes, which are less susceptible to interception or unauthorized access. Reference: 1. National Institute of Standards and Technology (NIST). (2017). Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf

NEW QUESTION: 182
A Chief Information Officer is concerned about employees using company-issued laptops lo steal data when accessing network shares. Which of the following should the company Implement?
A. DLP
B. CASB
C. HIDS
D. EDR
E. UEFI
Answer: A (LEAVE A REPLY)

The company should implement Data Loss Prevention (DLP) to prevent employees from stealing data when accessing network shares. Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 8

NEW QUESTION: 183
A security analyst is currently addressing an active cyber incident. The analyst has been able to identify affected devices that are running a malicious application with a unique hash. Which of the following is the next step according to the incident response process?
A. Recovery
B. Lessons learned
C. Containment
D. Preparation
Answer: C (LEAVE A REPLY)
Containment is the next step according to the incident response process after identifying affected devices that are running a malicious application with a unique hash. Containment involves isolating the compromised devices or systems from the rest of the network to prevent the spread of the attack and limit its impact. Containment can be done by disconnecting the devices from the network, blocking network traffic to or from them, or applying firewall rules or access control lists. Containment is a critical step in incident response because it helps to preserve evidence for further analysis and remediation, and reduces the risk of data loss or exfiltration
https://www.fortinet.com/resources/cyberglossary/incident-response
https://www.ibm.com/topics/incident-response

NEW QUESTION: 184
A company is implementing a new SIEM to log and send alerts whenever malicious activity is blocked by its antivirus and web content filters. Which of the following is the primary use case for this scenario?
A. Implementation of preventive controls
B. Implementation of detective controls
C. Implementation of deterrent controls
D. Implementation of corrective controls
Answer: B (LEAVE A REPLY)
A Security Information and Event Management (SIEM) system is a tool that collects and analyzes security-related data from various sources to detect and respond to security incidents. Reference: CompTIA Security+ Study Guide 601, Chapter 5

NEW QUESTION: 185
An organization is moving away from the use of client-side and server-side certificates for EAR The company would like for the new EAP solution to have the ability to detect rogue access points. Which of the following would accomplish these requirements?
A. PEAP
B. EAP-FAST
C. EAP-TLS
D. EAP-TTLS
Answer: B (LEAVE A REPLY)

EAP-FAST (Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling) supports mutual authentication and is designed to simplify the deployment of strong, password-based authentication. EAP-FAST includes a mechanism for detecting rogue access points. Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION: 186
A company was recently breached. Part of the company's new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?
A. Log enrichment
B. Log queue
C. Log parser
D. Log collector
Answer: (SHOW ANSWER)
A log collector can collect logs from various sources, such as servers, devices, applications, or network components, and forward them to a central source for analysis and storage23.

NEW QUESTION: 187
A network architect wants a server to have the ability to retain network availability even if one of the network switches it is connected to goes down. Which of the following should the architect implement on the server to achieve this goal?
A. RAID
B. UPS
C. NIC teaming
D. Load balancing
Answer: C (LEAVE A REPLY)
NIC Teaming is a feature that allows a server to be connected to multiple network switches, providing redundancy and increased network availability. If one of the switches goes down, the server will still be able to send and receive data through one of the other switches. To configure NIC Teaming in Windows Server, see Microsoft's documentation: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nic-teaming. For more information on NIC Teaming and other network redundancy features, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION: 188
A security engineer is investigating a penetration test report that states the company website is vulnerable to a web application attack. While checking the web logs from the time of the test, the engineer notices several invalid web form submissions using an unusual address: "SELECT * FROM customername". Which of the following is most likely being attempted?
A. Directory traversal
B. SQL injection
C. Privilege escalation
D. Cross-site scripting
Answer: B (LEAVE A REPLY)
SQL injection is a web application attack that involves inserting malicious SQL statements into an input field, such as a web form, to manipulate or access the database behind the application. SQL injection can be used to perform various actions, such as

reading, modifying, or deleting data, executing commands on the database server, or bypassing authentication. In this scenario, the attacker is trying to use a SQL statement "SELECT * FROM customername" to retrieve all data from the customername table in the database.

NEW QUESTION: 189
A third party asked a user to share a public key for secure communication. Which of the following file formats should the user choose to share the key?
A. .pfx
B. .csr
C. .pvk
D. .cer
Answer: D (LEAVE A REPLY)
A user should choose the .cer file format to share a public key for secure communication. A .cer file is a public key certificate that can be shared with third parties to enable secure communication.
Reference:
A public key is a cryptographic key that can be used to encrypt or verify data. A public key file is a file that contains one or more public keys in a specific format.
There are different formats for public key files, depending on the application and the algorithm used. Some of the common formats are:
.pfx: This is a file format that stores a certificate and its private and public keys. It is also known as PKCS#12 or Personal Information Exchange. It is used by some applications such as Microsoft Internet Explorer and Outlook to import and export certificates and keys.1
.csr: This is a file format that stores a Certificate Signing Request, which is a message sent to a Certificate Authority (CA) to request a digital certificate. It contains the public key and some information about the identity of the requester. It is also known as PKCS#10 or Certification Request Syntax.2
.pvk: This is a file format that stores a private key for Microsoft Authenticode code signing. It is used with a .spc file that contains the certificate and public key.3
.cer: This is a file format that stores a certificate, which is a document that binds a public key to an identity. It is also known as DER or Distinguished Encoding Rules. It is used by some applications such as OpenSSL and Java to read and write certificates.4

NEW QUESTION: 190
A user is trying to upload a tax document, which the corporate finance department requested, but a security program IS prohibiting the upload A security analyst determines the file contains PII, Which of the following steps can the analyst take to correct this issue?
A. Create a URL filter with an exception for the destination website.
B. Add a firewall rule to the outbound proxy to allow file uploads
C. Issue a new device certificate to the user's workstation.
D. Modify the exception list on the DLP to allow the upload
Answer: D (LEAVE A REPLY)
Data Loss Prevention (DLP) policies are used to identify and protect sensitive data, and often include a list of exceptions that allow certain types of data to be uploaded or shared. By modifying the exception list on the DLP, the security analyst can allow

the tax document to be uploaded without compromising the security of the system. (Reference: CompTIA Security+ SY0-601 Official Textbook, page 479-480)

NEW QUESTION: 191
Which of the following roles is responsible for defining the protection type and Classification type for a given set of files?
A. General counsel
B. Data owner
C. Risk manager
D. Chief Information Officer
Answer: B (LEAVE A REPLY)
Data owner is the role that is responsible for defining the protection type and classification type for a given set of files. Data owner is a person in the organization who is accountable for a certain set of data and determines how it should be protected and classified. General counsel is the role that provides legal advice and guidance to the organization. Risk manager is the role that identifies, analyzes, and mitigates risks to the organization. Chief Information Officer is the role that oversees the information technology strategy and operations of the organization
https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/data-roles-and-responsibilities/

NEW QUESTION: 192
A company owns a public-facing e-commerce website. The company outsources credit card transactions to a payment company. Which of the following BEST describes the role of the payment company?
A. Data controller
B. Data custodian
C. Data owners
D. Data processor
Answer: D (LEAVE A REPLY)
A data processor is an organization that processes personal data on behalf of a data controller. In this scenario, the company that owns the e-commerce website is the data controller, as it determines the purposes and means of processing personal data (e.g. credit card information). The payment company is a data processor, as it processes personal data on behalf of the e-commerce company (i.e. it processes credit card transactions).

NEW QUESTION: 193
A security analyst reviews web server logs and finds the following string gallerys?file-. ./../../../../. . / . ./etc/passwd Which of the following attacks was performed against the web server?
A. Directory traversal
B. CSRF
C. Pass the hash
D. SQL injection
Answer: (SHOW ANSWER)
Directory traversal is an attack that exploits a vulnerability in a web application or a file system to access files or directories that are outside the intended scope. The attacker can use special characters, such as .../ or ...\ , to navigate through the directory structure and access restricted files or directories.

NEW QUESTION: 194
A company is implementing MFA for all applications that store sensitive dat a. The IT manager wants MFA to be non-disruptive and user friendly Which of the following technologies should the IT manager use when implementing MFA?
A. One-time passwords
B. Email tokens
C. Push notifications
D. Hardware authentication
Answer: C (LEAVE A REPLY)
Push notifications are a type of technology that allows an application or a service to send messages or alerts to a user's device without requiring the user to open the application or the service. They can be used for multi-factor authentication (MFA) by sending a prompt or a code to the user's device that the user has to approve or enter to verify their identity. They can be non-disruptive and user friendly because they do not require the user to remember or type anything, and they can be delivered instantly and securely.

NEW QUESTION: 195
A company reduced the area utilized in its datacenter by creating virtual networking through automation and by creating provisioning routes and rules through scripting. Which of the following does this example describe?
A. laC
B. MSSP
C. Containers
D. SaaS
Answer: A (LEAVE A REPLY)
laaS (Infrastructure as a Service) allows the creation of virtual networks, automation, and scripting to reduce the area utilized in a datacenter. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 4

NEW QUESTION: 196
Certain users are reporting their accounts are being used to send unauthorized emails and conduct suspicious activities. After further investigation, a security analyst notices the following:
* All users share workstations throughout the day.
* Endpoint protection was disabled on several workstations throughout the network.
* Travel times on logins from the affected users are impossible.
* Sensitive data is being uploaded to external sites.
* All user account passwords were forced to be reset and the issue continued.
Which of the following attacks is being used to compromise the user accounts?
A. Brute-force
B. Keylogger
C. Dictionary
D. Rainbow
Answer: B (LEAVE A REPLY)

The symptoms suggest a keylogger is being used to compromise the user accounts, allowing the attackers to obtain the users' passwords and other sensitive information. Reference:
CompTIA Security+ Study Guide Exam SY0-601, Chapter 6

NEW QUESTION: 197
A security architect is designing a remote access solution for a business partner. The business partner needs to access one Linux server at the company. The business partner wants to avid managing a password for authentication and additional software installation. Which of the following should the architect recommend?
A. Soft token
B. Smart card
C. CSR
D. SSH key
Answer: D (LEAVE A REPLY)
SSH key is a pair of cryptographic keys that can be used for authentication and encryption when connecting to a remote Linux server via SSH protocol. SSH key authentication does not require a password and is more secure than password-based authentication. SSH key authentication also does not require additional software installation on the client or the server, as SSH is a built-in feature of most Linux distributions. A business partner can generate an SSH key pair on their own computer and send the public key to the company, who can then add it to the authorized_keys file on the Linux server. This way, the business partner can access the Linux server without entering a password or installing any software

NEW QUESTION: 198
Which of the following is a security implication of newer 1CS devices that are becoming more common in corporations?
A. Devices with celular communication capabilities bypass traditional network security controls
B. Many devices do not support elliptic-curve encryption algorithms due to the overhead they require.
C. These devices often lade privacy controls and do not meet newer compliance regulations
D. Unauthorized voice and audio recording can cause loss of intellectual property
Answer: (SHOW ANSWER)
Industrial control systems (ICS) are devices that monitor and control physical processes, such as power generation, manufacturing, or transportation. Newer ICS devices may have voice and audio capabilities that can be exploited by attackers to eavesdrop on sensitive conversations or capture confidential information. This can result in the loss of intellectual property or trade secrets. Reference: https://www.comptia.org/content/guides/what-is-industrial-control-system-security

NEW QUESTION: 199

A security engineer is setting up passwordless authentication for the first time.
INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:

NEW QUESTION: 200
A user reports trouble using a corporate laptop. The laptop freezes and responds slowly when writing documents and the mouse pointer occasional disappears.
The task list shows the following results
Which of the following is MOST likely the issue?
A. RAT
B. PUP
C. Spyware
D. Keylogger
Answer: (SHOW ANSWER)
Spyware is malicious software that can cause a computer to slow down or freeze. It can also cause the mouse pointer to disappear. The task list shows an application named "spyware.exe" running, indicating that spyware is likely the issue. Reference: CompTIA Security+ Certification Exam Objectives 6.0: Given a scenario, analyze indicators of compromise and determine the type of malware.
CompTIA Security+ Study Guide, Sixth Edition, pages 125-126

NEW QUESTION: 201
An engineer is using scripting to deploy a network in a cloud environment. Which the following describes this scenario?
A. SDLC
B. VLAN
C. SDN
D. SDV
Answer: C (LEAVE A REPLY)
SDN stands for software-defined networking, which is an approach to networking that uses software-based controllers or application programming interfaces (APIs) to communicate with underlying hardware infrastructure and direct traffic on a network. SDN decouples the network control plane from the data plane, enabling centralized management and programmability of network resources. SDN can help an engineer use scripting to deploy a network in a cloud environment by allowing them to define and automate network policies, configurations, and services through software commands.

NEW QUESTION: 202
A security administrator suspects there may be unnecessary services running on a server. Which of the following tools will the administrator most likely use to confirm the suspicions?
A. Nmap
B. Wireshark
C. Autopsy

D. DNSEnum

Answer: A (LEAVE A REPLY)

Nmap is a tool that is used to scan IP addresses and ports in a network and to detect installed applications. Nmap can help a security administrator determine the services running on a server by sending various packets to the target and analyzing the responses. Nmap can also perform various tasks such as OS detection, version detection, script scanning, firewall evasion, and vulnerability scanning.

NEW QUESTION: 203

Users report access to an application from an internal workstation is still unavailable to a specific server, even after a recent firewall rule implementation that was requested for this access. ICMP traffic is successful between the two devices. Which of the following tools should the security analyst use to help identify if the traffic is being blocked?

A. nmap

B. tracert

C. ping

D. ssh

Answer: (SHOW ANSWER)

Tracert is a command-line tool that shows the route that packets take to reach a destination on a network1. It also displays the time it takes for each hop along the way1. By using tracert, you can see if there is a router or firewall that is blocking or slowing down the traffic between the internal workstation and the specific server1.

NEW QUESTION: 204

A company uses a drone for precise perimeter and boundary monitoring. Which of the following should be MOST concerning to the company?

A. Privacy

B. Cloud storage of telemetry data

C. GPS spoofing

D. Weather events

Answer: (SHOW ANSWER)

The use of a drone for perimeter and boundary monitoring can raise privacy concerns, as it may capture video and images of individuals on or near the monitored premises. The company should take measures to ensure that privacy rights are not violated.

Reference:

CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 8

NEW QUESTION: 205

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

1. Deny cleartext web traffic
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.

The ruleset order cannot be modified due to outside constraints.

Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.

Answer:

In Firewall 1, HTTP inbound Action should be DENY. As shown below

In Firewall 2, Management Service should be DNS, As shown below.

In Firewall 3, HTTP Inbound Action should be DENY, as shown below

NEW QUESTION: 206

A company was recently breached Pan of the company's new cybersecurity strategy is to centralize? the togs horn all security devices Which of the following components forwards the logs to a central source?

A. Log enrichment

B. Log queue

C. Log parser

D. Log collector

Answer: D (LEAVE A REPLY)

A log collector is a component that forwards the logs from all security devices to a central source. A log collector can be a software tool or a hardware appliance that collects logs from various sources, such as firewalls, routers, servers, applications, or endpoints. A log collector can also perform functions such as log filtering, parsing, aggregation, normalization, and enrichment. A log collector can help centralize logging by sending the collected logs to a central log server or a security information and event management (SIEM) system for further analysis and correlation.

NEW QUESTION: 207

A security analyst needs to implement an MDM solution for BYOD users that will allow the company to retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.Which of the following would BEST meet these requirements? (Select TWO).

A. Full-device encryption

B. Network usage rules

C. Geofencing

D. Containerization

E. Application whitelisting

F. Remote control

Answer: (SHOW ANSWER)

MDM solutions emerged to solve problems created by BYOD. With MDM, IT teams can remotely wipe devices clean if they are lost or stolen. MDM also makes the life of an IT administrator a lot easier as it allows them to enforce corporate policies, apply software updates, and even ensure that password protection is used on each device. Containerization and application whitelisting are two features of MDM that can help retain control over company emails residing on the devices and limit data exfiltration that might occur if the devices are lost or stolen.

Containerization is a technique that creates a separate and secure space on the device for work-related data and applications. This way, personal and corporate data are isolated from each other, and IT admins can manage only the work container without affecting the user's privacy. Containerization also allows IT admins to remotely wipe only the work container if needed, leaving the personal data intact.

Application whitelisting is a technique that allows only authorized applications to run on the device. This way, IT admins can prevent users from installing or using malicious or unapproved applications that might compromise the security of corporate data. Application whitelisting also allows IT admins to control which applications can access corporate resources, such as email servers or cloud storage.

NEW QUESTION: 208
A security analyst receives an alert from the company's S1EM that anomalous activity is coming from a local source IP address of 192 168 34.26 The Chief Information Security Officer asks the analyst to block the originating source Several days later another employee opens an internal ticket stating that vulnerability scans are no longer being performed property. The IP address the employee provides is 192 168.34 26. Which of the following describes this type of alert?
A. True positive
B. True negative
C. False positive
D. False negative
Answer: C (LEAVE A REPLY)
A false positive is a type of alert that indicates a security incident when there is none. It can be caused by misconfigured or overly sensitive security tools or systems that generate false or irrelevant alerts. In this case, the alert from the company's SIEM that Mimikatz attempted to run on the remote systems was a false positive because it was triggered by a legitimate vulnerability scanning tool that uses Mimikatz as part of its functionality.

NEW QUESTION: 209
A security analyst reviews web server logs and notices the following line:
104.35. 45.53 -
[22/May/2020:07 : 00:58 +0100] "GET . UNION ALL SELECT
user login, user _ pass, user email from wp users-- HTTP/I.I" 200 1072 http://www.example.com/wordpress/wp-admin/ Which of the following vulnerabilities is the attacker trying to exploit?
A. SSRF
B. CSRF
C. xss
D. SQLi
Answer: D (LEAVE A REPLY)
SQLi stands for SQL injection, which is a type of web security vulnerability that allows an attacker to execute malicious SQL statements on a database server. SQLi can result in data theft, data corruption, denial of service, or remote code execution. The attacker in the web server log is trying to exploit a SQLi vulnerability by sending a malicious GET request that contains a UNION ALL SELECT statement. This statement is used to combine the results of two or more SELECT queries into a single result set. The attacker is attempting to retrieve user login, user pass, and user email from the wp users table, which is a WordPress database table that stores user information. The attacker may use this information to compromise the WordPress site or the users' accounts.

NEW QUESTION: 210

A systems administrator is considering different backup solutions for the IT infrastructure. The company is looking for a solution that offers the fastest recovery time while also saving the most amount of storage used to maintain the backups. Which of the following recovery solutions would be the BEST option to meet these requirements?

A. Snapshot

B. Differential

C. Full

D. Tape

Answer: B (LEAVE A REPLY)

Differential backup is a type of backup that backs up all data that has changed since the last full backup. This backup method offers faster recovery than a full backup, as it only needs to restore the full backup and the differential backup, reducing the amount of data that needs to be restored. It also uses less storage than a full backup as it only stores the changes made from the last full backup.

NEW QUESTION: 211

A government organization is developing an advanced AI defense system. Develop-ers are using information collected from third-party providers Analysts are no-ticing inconsistencies in the expected powers Of then learning and attribute the Outcome to a recent attack on one of the suppliers. Which of the following IS the most likely reason for the inaccuracy of the system?

A. Improper algorithms security

B. Tainted training data

C. virus

D. Cryptomalware

Answer: B (LEAVE A REPLY)

Tainted training data is a type of data poisoning attack that involves modifying or injecting malicious data into the training dataset of a machine learning or artificial intelligence system. It can cause the system to learn incorrect or biased patterns and produce inaccurate or malicious outcomes. It is the most likely reason for the inaccuracy of the system that is using information collected from third-party providers that have been compromised by an attacker.

NEW QUESTION: 212

A building manager is concerned about people going in and out of the office during non-working hours. Which of the following physical security controls would provide the best solution?

A. Cameras

B. Badges

C. Locks

D. Bollards

Answer: B (LEAVE A REPLY)

Badges are physical security controls that provide a way to identify and authenticate authorized individuals who need to access a building or a restricted are a. Badges can also be used to track the entry and exit times of people and monitor their movements within the premises. Badges can help deter unauthorized access by requiring people to present a valid credential before entering or leaving the office. Badges can also help prevent tailgating, which is when an unauthorized person follows an authorized person through a door or gate. Badges can be integrated with other security systems, such as locks, alarms, cameras, or biometrics, to enhance the level of protection.

NEW QUESTION: 213

Law enforcement officials sent a company a notification that states electronically stored information and paper documents cannot be destroyed. Which of the following explains this process?

A. Data breach notification

B. Accountability

C. Legal hold

D. Chain of custody

Answer: (SHOW ANSWER)

A legal hold is a process that requires an organization to preserve electronically stored information and paper documents that are relevant to a pending or anticipated litigation or investigation. It suspends the normal retention and destruction policies and procedures for such information and documents until the legal hold is lifted or released.

NEW QUESTION: 214

A security administrator is setting up a SIEM to help monitor for notable events across the enterprise. Which of the following control types does this BEST represent?

A. Preventive

B. Compensating

C. Corrective

D. Detective

Answer: (SHOW ANSWER)

A SIEM is a security solution that helps detect security incidents by monitoring for notable events across the enterprise. A detective control is a control that is designed to detect security incidents and respond to them. Therefore, a SIEM represents a detective control.

NEW QUESTION: 215

A large retail store's network was breached recently. and this news was made public. The Store did not lose any intellectual property, and no customer information was stolen. Although no fines were incurred as a result, the Store lost revenue after the breach. Which of the following is the most likely reason for this issue?

A. Employee training

B. Leadership changes

C. Reputation

D. Identity theft

Answer: C (LEAVE A REPLY)
Reputation is the perception or opinion that customers, partners, investors, etc., have about a company or its products and services. It can affect the revenue and profitability of a company after a network breach, even if no intellectual property or customer information was stolen, because it can damage the trust and confidence of the stakeholders and reduce their willingness to do business with the company

NEW QUESTION: 216
Which of the following models offers third-party-hosted, on-demand computing resources that can be shared with multiple organizations over the internet?
A. Public cloud
B. Hybrid cloud
C. Community cloud
D. Private cloud
Answer: A (LEAVE A REPLY)
There are three main models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)12. Each model represents a different part of the cloud computing stack and provides different levels of control, flexibility, and management.
According to one source1, a public cloud is a type of cloud deployment where the cloud resources (such as servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. A public cloud can be shared with multiple organizations or users who pay for the service on a subscription or pay-as-you-go basis.

NEW QUESTION: 217
A security researcher is tracking an adversary by noting its attacks and techniques based on its capabilities, infrastructure, and victims. Which of the following is the researcher MOST likely using?
A. The Diamond Model of Intrusion Analysis
B. The Cyber Kill Chain
C. The MITRE CVE database
D. The incident response process
Answer: A (LEAVE A REPLY)
The Diamond Model is a framework for analyzing cyber threats that focuses on four key elements: adversary, capability, infrastructure, and victim. By analyzing these elements, security researchers can gain a better understanding of the threat landscape and develop more effective security strategies.

NEW QUESTION: 218
A security team is conducting a security review of a hosted data provider. The management team has asked the hosted data provider to share proof that customer data is being appropriately protected.
Which of the following would provide the best proof that customer data is being protected?
A. SOC2
B. CSA
C. CSF
D. 1SO 31000

Answer: A (LEAVE A REPLY)
SOC2 is a type of audit report that provides assurance on the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems. It is based on the Trust Services Criteria developed by the American Institute of Certified Public Accountants (AICPA). A SOC2 report can provide proof that customer data is being appropriately protected by the hosted data provider1
https://www.csagroup.org/store/product/50072454/ 3: https://www.csagroup.org/store/product/50072454os/ 1: https://cloudsecurityalliance.org/blog/2021/08/20/star-testimonial-csa-star-soc2-from-readiness-to-attestation/

NEW QUESTION: 219
While troubleshooting a service disruption on a mission-critical server, a technician discovered the user account that was configured to run automated processes was disabled because the user's password failed to meet password complexity requirements. Which of the following would be the BEST solution to securely prevent future issues?
A. Using an administrator account to run the processes and disabling the account when it is not in use
B. Implementing a shared account the team can use to run automated processes
C. Configuring a service account to run the processes
D. Removing the password complexity requirements for the user account
Answer: C (LEAVE A REPLY)
A service account is a user account that is created specifically to run automated processes and services. These accounts are typically not associated with an individual user, and are used for running background services and scheduled tasks. By configuring a service account to run the automated processes, you can ensure that the account will not be disabled due to password complexity requirements and other user-related issues.

NEW QUESTION: 220
A security manager needs to assess the security posture of one of the organization's vendors. The contract with the vendor does not allow for auditing of the vendor's security controls. Which of (he following should the manager request to complete the assessment?
A. A service-level agreement
B. A business partnership agreement
C. A SOC 2 Type 2 report
D. A memorandum of understanding
Answer: C (LEAVE A REPLY)
SOC 2 (Service Organization Control 2) is a type of audit report that evaluates the controls of service providers to verify their compliance with industry standards for security, availability, processing integrity, confidentiality, and privacy. A Type 2 report is based on an audit that tests the effectiveness of the controls over a period of time, unlike a Type 1 report which only evaluates the design of the controls at a specific point in time.
A SOC 2 Type 2 report would provide evidence of the vendor's security controls and how effective they are over time, which can help the security manager assess the vendor's security posture despite the vendor not allowing for a direct audit.
The security manager should request a SOC 2 Type 2 report to assess the security posture of the vendor. Reference: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 5

NEW QUESTION: 221

A security engineer is installing a WAF to protect the company's website from malicious web requests over SSL. Which of the following is needed to meet the objective?

A. A reverse proxy

B. A decryption certificate

C. A spill-tunnel VPN

D. Load-balanced servers

Answer: (SHOW ANSWER)

A Web Application Firewall (WAF) is a security solution that protects web applications from various types of attacks such as SQL injection, cross-site scripting (XSS), and others. It is typically deployed in front of web servers to inspect incoming traffic and filter out malicious requests.

To protect the company's website from malicious web requests over SSL, a decryption certificate is needed to decrypt the SSL traffic before it reaches the WAF. This allows the WAF to inspect the traffic and filter out malicious requests.

NEW QUESTION: 222

A security analyst wants to verify that a client-server (non-web) application is sending encrypted traffic. Which of the following should the analyst use?

A. openssl

B. hping

C. netcat

D. tcpdump

Answer: A (LEAVE A REPLY)

To verify that a client-server (non-web) application is sending encrypted traffic, a security analyst can use OpenSSL. OpenSSL is a software library that provides cryptographic functions, including encryption and decryption, in support of various security protocols, including SSL/TLS. It can be used to check whether a client-server application is using encryption to protect traffic.

Reference:

CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION: 223

The Chief Executive Officer announced a new partnership with a strategic vendor and asked the Chief Information Security Officer to federate user digital identities using SAML-based protocols. Which of the following will this enable?

A. SSO

B. MFA

C. PKI

D. OLP

Answer: A (LEAVE A REPLY)

Federating user digital identities using SAML-based protocols enables Single Sign-On (SSO), which allows users to log in once and access multiple applications without having to enter their credentials for each one. Reference:

CompTIA Security+ Certification Exam Objectives 1.3: Explain authentication and access controls.

CompTIA Security+ Study Guide, Sixth Edition, pages 41-42

NEW QUESTION: 224

Which of the following provides a catalog of security and privacy controls related to the United States federal information systems?

A. GDPR

B. PCI DSS

C. ISO 27000

D. NIST 800-53

Answer: D (LEAVE A REPLY)

NIST 800-53 provides a catalog of security and privacy controls related to the United States federal information systems.

Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3: Architecture and Design, pp. 123-125

NEW QUESTION: 225

The Chief Information Security Officer wants to pilot a new adaptive, user-based authentication method. The concept Includes granting logical access based on physical location and proximity. Which of the following Is the BEST solution for the pilot?

A. Geofencing

B. Self-sovereign identification

C. PKI certificates

D. SSO

Answer: A (LEAVE A REPLY)

Geofencing is a location-based technology that allows an organization to define and enforce logical access control policies based on physical location and proximity. Geofencing can be used to grant or restrict access to systems, data, or facilities based on an individual's location, and it can be integrated into a user's device or the infrastructure. This makes it a suitable solution for the pilot project to test the adaptive, user-based authentication method that includes granting logical access based on physical location and proximity.

NEW QUESTION: 226

A security administrator Installed a new web server. The administrator did this to Increase the capacity (or an application due to resource exhaustion on another server. Which o(the following algorithms should the administrator use to split the number of the connections on each server In half?

A. Weighted response

B. Round-robin

C. Least connection

D. Weighted least connection

Answer: B (LEAVE A REPLY)

The administrator should use a round-robin algorithm to split the number of connections on each server in half. Round-robin is a load-balancing algorithm that distributes incoming requests to the available servers one by one in a cyclical order. This helps to evenly distribute the load across all of the servers, ensuring that no single server is overloaded.

NEW QUESTION: 227
An organization wants seamless authentication to its applications. Which of the following should the organization employ to meet this requirement?
A. SOAP
B. SAML
C. SSO
D. Kerberos
Answer: (SHOW ANSWER)
Single Sign-On (SSO) is a mechanism that allows users to access multiple applications with a single set of login credentials.
Reference: CompTIA Security+ Study Guide 601, Chapter 6

NEW QUESTION: 228
A security administrator Is evaluating remote access solutions for employees who are geographically dispersed. Which of the following would provide the MOST secure remote access? (Select TWO).
A. IPSec
B. SFTP
C. SRTP
D. LDAPS
E. S/MIME
F. SSL VPN
Answer: A,F (LEAVE A REPLY)
IPSec (Internet Protocol Security) is a technology that provides secure communication over the internet by encrypting traffic and authenticating it at both the sender and receiver. It can be used to create secure tunnels between two or more devices, allowing users to access resources securely and privately.
SSL VPN (Secure Sockets Layer Virtual Private Network) is a type of VPN that uses an SSL/TLS connection to encrypt traffic between two or more devices. It is a secure and reliable solution for providing remote access, as all traffic is encrypted and authenticated. Additionally, SSL VPNs can also be used to restrict access to certain websites and services, making them a secure and robust solution for remote access.