CompTIA.SY0-501.v2022-02-09.q543

Exam Code:	SY0-501
Exam Name:	CompTIA Security+ Certification Exam
Certification Provider:	CompTIA
Free Question Number:	543
Version:	v2022-02-09
# of views:	8206
# of Questions views:	5430
https://www.freepdfdumps.com/CompTIA.SY0-501.v2022-02-09.q543.html	

NEW QUESTION: 1
Which of the following strategies should a systems architect use to minimize availability risks due to insufficient storage capacity?
A. Load balancing
B. Scalability
C. Distributive allocation
D. High availability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 2
A security technician has been given the task of preserving emails that are potentially involved in a dispute between a company and a contractor.
Which of the following BEST describes this forensic concept?
A. Order of volatility
B. Chain of custody
C. Data acquisition
D. Legal hold
Answer: D (LEAVE A REPLY)

NEW QUESTION: 3
A Chief Security Officer (CSO) has implemented a policy to prevent the reuse of hard drives due to the risk of information spillage to unauthorized users. Which of the following would be the MOST practical process to decommission the workstations?
A. Remove all the hard drives and shred the disks.
B. Remove all the hard drives and degauss them.
C. Remove all the hard drives and purge them.
D. Remove all the hard drives and dispose of them in the trash.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 4
A security engineer deploys a certificate from a commercial CA to the RADIUS server for use with the EAP-TLS wireless network. Authentication is failing, so the engineer examines the certificate's properties:
Which of the following is the MOST likely cause of the failure?
A. The certificate has expired.
B. The certificate is self-signed.
C. The certificate is missing the proper OID.
D. The certificate is missing wire-less authentication in key usage.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 5
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:
*There is no standardization.
*Employees ask for reimbursement for their devices.
*Employees do not replace their devices often enough to keep them running efficiently.
*The company does not have enough control over the devices.
Which of the following is a deployment model that would help the company overcome these problems?
A. VDI
B. BYOD
C. CYOD
D. COPE
Answer: D (LEAVE A REPLY)

NEW QUESTION: 6
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:
A. Escalation of privileges
B. Passive reconnaissance
C. Persistence
D. Exploiting the switch
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Task: Configure the firewall (fill out the table) to allow these four rules:
* Only allow the Accounting computer to have HTTPS access to the Administrative server.

* Only allow the HR computer to be able to communicate with the Server 2 System over SCP.
* Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2

Answer:

See the solution below.

Explanation

Use the following answer for this simulation task.

Below table has all the answers required for this question.

Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria: Block the connection Allow the connection

Allow the connection only if it is secured

TCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent.

Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session.

When the session ends, the connection is torn down.

UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP.

The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications.

The primary purpose of UDP is to send small packets of information.

The application is responsible for acknowledging the correct reception of the data. Port 22 is used by both SSH and SCP with UDP.

Port 443 is used for secure web connections? HTTPS and is a TCP port.

Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between 10.4.255.10/24 (Accounting) and

10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2) Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between: 10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)

10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2)

NEW QUESTION: 8

The security administrator has installed a new firewall which implements an implicit DENY policy by default.

INSTRUCTIONS:

Click on the firewall and configure it to allow ONLY the following communication.

1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.
Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.
Hot Area:

Answer:

Explanation

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port
22Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.
References:Stewart,
James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 9

A security analyst received an after-hours alert indicating that a large number of accounts with the suffix "admin" were locked out. The accounts were all locked out after five unsuccessful login attempts, and no other accounts on the network triggered the same alert. Which of the following is the BEST explanation for these alerts?

A. The administrator accounts do not have rigid password complexity rules, and this made them easier to crack.

B. The standard naming convention makes administrator accounts easy to identify, and they were targeted for an attack.

C. The threshold for locking out administrator accounts is too high, and it should be changed from five to three to prevent unauthorized access attempts.

D. The company has implemented time-of-day restrictions, and this triggered a false positive alert when the administrators tried to log in

Answer: B (LEAVE A REPLY)

NEW QUESTION: 10

A systems administrator is implementing a remote access method for the system that will utilize GUI. Which of the following protocols would be BEST suited for this?

A. SFTP

B. TLS

C. SRTP

D. SSH

Answer: B (LEAVE A REPLY)

NEW QUESTION: 11

A company wants to host a publicly available server that performs the following functions:

* Evaluates MX record lookup

* Can perform authenticated requests for A and AAA records

* Uses RRSIG

Which of the following should the company use to fulfill the above requirements?

A. LDAPS

B. DNSSEC

C. nslookup

D. dig

E. SFTP

Answer: (SHOW ANSWER)

NEW QUESTION: 12

A forensics analyst is investigating a hard drive for evidence of suspected illegal activity. Which of the following should the analyst do FIRST?

A. Back up the pictures directory for further inspection.

B. Save a copy of the case number and date as a text file in the root directory.

C. Create a hash of the hard drive.

D. Export the Internet history.

Answer: C (LEAVE A REPLY)

NEW QUESTION: 13

When performing data acquisition on a workstation, which of the following should be captured based on memory volatility? (Select two.)

A. USB-attached hard disk

B. Mounted network storage

C. RAM

D. Swap/pagefile

E. ROM

Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 14

Which of the following would a security specialist be able to determine upon examination of a server's certificate?

A. OID

B. Server private key

C. CSR

D. CA public key

Answer: (SHOW ANSWER)

NEW QUESTION: 15

Which of the following should be put in place when negotiating with a new vendor about the timeliness of the response to a significant outage or incident?

A. NDA

B. MOU

C. SLA

D. MTTR

Answer: B (LEAVE A REPLY)

NEW QUESTION: 16

A security program manager wants to actively test the security posture of a system. The system is not yet in production and has no uptime requirement or active user base.

Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?

A. Peer review

B. Component testing

C. Penetration testing

D. Vulnerability testing

Answer: (SHOW ANSWER)

A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 17

A Chief Information Security Officer (CISO) is concerned about the organization's ability to continue business operations in the event of a prolonged DDoS attack on its local datacenter that consumes server resources. Which of the following will the CISO MOST likely recommend to mitigate this risk?

A. Implement a challenge response test on all end-user queries.

B. Migrate to a geographically dispersed cloud datacenter.

C. Switch to a complete SaaS offering to customers.

D. Implement a hot-site failover location.

E. Upgrade the bandwidth available into the datacenter.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 18

The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly. The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected. Which of the following is required to complete the certificate chain?

A. Root of trust

B. Intermediate authority

C. Certificate revocation list

D. Recovery agent

Answer: B (LEAVE A REPLY)

NEW QUESTION: 19

A member of the human resources department is searching for candidate resumes and encounters the following error message when attempting to access popular job search websites: Which of the following would resolve this issue without compromising the company's security policies?

A. Remove the proxy settings from the employee's web browser.

B. Renew the DNS settings and IP address on the employee's computer.

C. Create an exception for the job search sites in the host-based firewall on the employee's computer.

D. Add the employee to a less restrictive group on the content filter.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 20

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry: Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration.

B. Create a blocking policy based on the parameter values.
C. Change the parameter name 'Account_Name' identified in the log.
D. Create an alert to generate emails for abnormally high activity.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 21
An organization electronically processes sensitive data within a controlled facility. The Chief Information Security Officer (CISO) wants to limit emissions from emanating from the facility. Which of the following mitigates this risk?
A. Hardening the facility with a Faraday cage to contain emissions produced from data processing
B. Hardening the facility through the use of secure cabinetry to block emissions
C. Upgrading facility cabling to a higher standard of protected cabling to reduce the likelihood of emission spillage
D. Employing security guards to ensure unauthorized personnel remain outside of the facility
Answer: A (LEAVE A REPLY)

NEW QUESTION: 22
Given the following output:
Which of the following BEST describes the scanned environment?
A. A web shell was planted in company corn's content management system.
B. A host was identified as a web server that is hosting multiple domains.
C. A connection was established to a domain, and several redirect connections were identified.
D. A host was scanned, and web-based vulnerabilities were found.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 23
Users report the following message appears when browsing to the company's secure site:
This website cannot be trusted. Which of the following actions should a security analyst take to resolve these messages? (Select TWO).
A. Ensure the certificate has a .pfx extension on the server.
B. Install the updated private key on the web server.
C. Update the root certificate into the client computer certificate store.
D. Have users clear their browsing history and relaunch the session.
E. Verify the certificate has not expired on the server.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 24
A security analyst has received the following alert snippet from the HIDS appliance:
Given the above logs, which of the following is the cause of the attack?
A. There is improper Layer 2 segmentation

B. The TCP ports on destination are all open
C. TCP MSS is configured improperly
D. FIN, URG, and PSH flags are set in the packet header
Answer: D (LEAVE A REPLY)

NEW QUESTION: 25
Which of the following characteristics differentiate a rainbow table attack from a brute force attack? (Select two.)
A. Rainbow table attacks must be performed on the network.
B. Rainbow tables must include precomputed hashes.
C. Rainbow table attacks do not require access to hashed passwords.
D. Rainbow table attacks bypass maximum failed login restrictions.
E. Rainbow table attacks greatly reduce compute cycles at attack time.
Answer: (SHOW ANSWER)

NEW QUESTION: 26
An employee workstation with an IP address of 204 211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?
A. The deny statement for 204 211.38.52/24 should be changed to a permit statement
B. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
C. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP.
D. The permit statement for 204.211.38 211/24 should be changed to TCP port 631 only instead of ALL
Answer: (SHOW ANSWER)

NEW QUESTION: 27
The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.
Which of the following is the best solution for the network administrator to secure each internal website?
A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Explanation:
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

NEW QUESTION: 28
A user clicked an email link that led to a website that infected the workstation with a virus. The virus encrypted all the network shares to which the user had access. The virus was not detected or blocked by the company's email filter, website filter, or antivirus. Which of the following describes what occurred?
A. The email originated from a private email server with no malware protection
B. Improper error handling triggered a false negative in all three controls
C. The virus was a zero-day attack
D. The user's account was over-privileged
Answer: (SHOW ANSWER)

NEW QUESTION: 29
A security administrator is reviewing the following information from a file that was found on a compromised host:
Which of the following types of malware is MOST likely installed on the compromised host?
A. Spyware
B. Backdoor
C. Keylogger
D. Trojan
E. Rootkit
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
Which of the following may indicate a configuration item has reached end-of-life?
A. The device will no longer turn on and indicated an error.
B. The object has been removed from the Active Directory.
C. Logs show a performance degradation of the component.
D. The vendor has not published security patches recently.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 31
A company utilizes 802.11 for all client connectivity within a facility. Users in one part of the building are reporting they are unable to access company resources when connected to the company SSID.
Which of the following should the security administrator use to assess connectivity?

A. Sniffer
B. Honeypot
C. Routing tables
D. Wireless scanner
Answer: C (LEAVE A REPLY)
Explanation

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 32
Ann, an employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:
* Slow performance
* Word documents, PDFs, and images no longer opening
* A pop-up
Ann states the issues began after she opened an invoice that a vendor emailed to her.
Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?
A. Crypto-malware
B. Backdoor
C. Rootkit
D. Spyware
Answer: C (LEAVE A REPLY)

NEW QUESTION: 33
A security analyst is hardening a web server, which should allow a secure certificate-based session using the organization's PKI infrastructure. The web server should also utilize the latest security techniques and standards. Given this set of requirements, which of the following techniques should the analyst implement to BEST meet these requirements? (Select two.)
A. Enable and configure TLS on the server.
B. Install a certificate signed by a public CA.
C. Configure the web server to use a host header.
D. Implement a CRL using an authorized CA.
E. Install an X- 509-compliant certificate.

Answer: (SHOW ANSWER)

NEW QUESTION: 34
An organization's IRP prioritizes containment over eradication. An incident has been discovered where an attacker outside of the organization has installed cryptocurrency mining software on the organization's web servers. Given the organization's stated priorities, which of the following would be the NEXT step?
A. Delete the malicious software and determine if the servers must be reimaged.
B. Identify and apply any missing operating system and software patches.
C. Review firewall and IDS logs to identify possible source IPs.
D. Remove the affected servers from the network.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 35
A system administrator wants to provide balance between the security of a wireless network and usability.
The administrator is concerned with wireless encryption compatibility of older devices used by some
employees. Which of the following would provide strong security and backward compatibility when
accessing the wireless network?
A. WPA using a preshared key
B. WEP with a 40-bit key
C. Open wireless network and SSL VPN
D. WPA2 using a RADIUS back-end for 802.1x authentication
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?
A. The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL
B. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
C. The deny statement for 204.211.38.52/24 should be changed to a permit statement
D. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
Which of the following network vulnerability scan indicators BEST validates a successful, active scan?
A. The scan job is scheduled to run during off-peak hours.
B. The scan results identify the hostname and IP address
C. The scan data identifies the use of privileged-user credentials
D. The scan output lists SQL injection attack vectors.
Answer: (SHOW ANSWER)

NEW QUESTION: 38
While checking logs, a security engineer notices a number of end users suddenly downloading files with the
.tar.gz extension. Closer examination of the files reveals they are PE32 files. The end users state they did not initiate any of the downloads. Further investigation reveals the end users all clicked on an external email containing an infected MHT file with an hreflink a week prior. Which of the following is MOST likely occurring?
A. A logic bomb was executed and is responsible for the data transfers.
B. A RAT was installed and is transferring additional exploit tools.
C. A fireless virus is spreading in the local network environment.
D. The workstations are beaconing to a command-and-control server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 39
A business has recently deployed laptops to all sales employees. The laptops will be used primarily from home offices and while traveling, and a high amount of wireless mobile use is expected.
To protect the laptops while connected to untrusted wireless networks, which of the following would be the BEST method for reducing the risk of having the laptops compromised?
A. MAC filtering
B. OS hardening
C. Application white-listing
D. Virtualization
Answer: B (LEAVE A REPLY)

NEW QUESTION: 40
The firewall administrator is adding a new certificate for the company's remote access solution. The solution requires that the uploaded file contain the entire certificate chain for the certificate to load properly.
The administrator loads the company certificate and the root CA certificate into the file. The file upload is rejected.
Which of the following is required to complete the certificate chain?

A. Intermediate authority
B. Recovery agent
C. Root of trust
D. Certificate revocation list
Answer: A (LEAVE A REPLY)

NEW QUESTION: 41
Devices on the SCADA network communicate exclusively at Layer 2. Which of the following should be used to prevent unauthorized systems using ARP-based attacks to compromise the SCADA network?
A. Application firewall
B. Hardware encryption
C. IPSec
D. VLANS
Answer: (SHOW ANSWER)

NEW QUESTION: 42
A security administrator needs an external vendor to correct an urgent issue with an organization's physical access control system (PACS). The PACS does not currently have internet access because it is running a legacy operation system. Which of the following methods should the security administrator select the best balances security and efficiency?
A. Temporarily permit outbound internet access for the pacs so desktop sharing can be set up
B. Have the external vendor come onsite and provide access to the PACS directly
C. Set up VPN concentrator for the vendor and restrict access to the PACS using desktop sharing
D. Set up a web conference on the administrator's pc; then remotely connect to the pacs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 43
A security analyst is investigating a call from a user regarding one of the websites receiving a 503: Service Unavailable error. The analyst runs a netstat -an command to discover if the web server is up and listening.
The analyst receives the following output:
TCP 10.1.5.2:80 192.168.2.112:60973 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60974 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60975 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60976 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60977 TIME_WAIT
TCP 10.1.5.2:80 192.168.2.112:60978 TIME_WAIT
Which of the following types of attack is the analyst seeing?
A. Domain hijacking
B. Denial of service

C. Buffer overflow
D. ARP poisoning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 44
Which of the following types of keys is found in a key escrow?
A. Public
B. Private
C. Shared
D. Session
Answer: B (LEAVE A REPLY)

NEW QUESTION: 45
A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.
Answer:

NEW QUESTION: 46
An administrator is configuring access to information located on a network file server named "Bowman". The files are located in a folder named "BalkFiles". The files are only for use by the "Matthews" division and should be read-only. The security policy requires permissions for shares to be managed at the file system layer and also requires those permissions to be set according to a least privilege model. Security policy for this data type also dictates that administrator-level accounts on the system have full access to the files.
The administrator configures the file share according to the following table:
Which of the following rows has been misconfigured?
A. Row 3
B. Row 5
C. Row 2
D. Row 1
E. Row 4
Answer: E (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here:

https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 47
A company has noticed multiple instances of proprietary information on public websites. It has also
observed an increase in the number of email messages sent to random employees containing malicious
links and PDFs. Which of the following changes should the company make to reduce the risks associated
with phishing attacks? (Select TWO)
A. Install an additional firewall
B. Block access to personal email on corporate systems
C. Implement a redundant email server
D. Review access violation on the file server
E. Update the X.509 certificates on the corporate email server
F. Update corporate policy to prohibit access to social media websites
Answer: B,F (LEAVE A REPLY)

NEW QUESTION: 48
A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.
Answer:

NEW QUESTION: 49
A wireless network uses a RADIUS server that is connected to an authenticator, which in turn connects to a supplicant. Which of the following represents the authentication architecture in use?
A. 802.1x
B. Open systems authentication
C. RADIUS federation
D. Captive portal
Answer: A (LEAVE A REPLY)

NEW QUESTION: 50
An auditor is performing an assessment of a security appliance with an embedded OS that was vulnerable during the last two assessments. Which of the following BEST explains the appliance's vulnerable state?
A. The vendor has not supplied a patch for the appliance.
B. The system was configured with weak default security settings.
C. The device uses weak encryption ciphers.

D. The appliance requires administrative credentials for the assessment.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 51
A systems administrator wants to implement a secure wireless network requiring wireless clients to pre-register with the company and install a PKI client certificate prior to being able to connect to the wireless network. Which of the following should the systems administrator configure?
A. EAP with PEAP
B. EAP-TLS
C. EAP-FAST
D. EAP with MSCHAPv2
E. EAP-TTLS
Answer: (SHOW ANSWER)

NEW QUESTION: 52
Task: Determine the types of attacks below by selecting an option from the dropdown list.
Answer:
Explanation:
A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted

messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS) E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 53
An information security analyst needs to work with an employee who can answer Question analyst should seek out an employee who has the role of:
A. steward
B. systems administrator
C. owner
D. privacy officer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 54
A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO. Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Select TWO).
A. Password history
B. Password reuse restrictions
C. Account disablement
D. Password recovery
E. Password complexity requirements
F. Privileged accounts
Answer: (SHOW ANSWER)

NEW QUESTION: 55

A security administrator is investigating many recent incident of credential theft for users accessing the company's website, despite the hosting web server requiring HTTPS for access. The server's logs show the website leverages the HTTO POST method for carrying user authentication details.
Which of the following is the MOST likely reason for compromise?
A. The HTTP POST method is not protected by HTTPS.
B. The web server is running a vulnerable SSL configuration.
C. The company does not support DNSSEC.
D. The HTTP response is susceptible to sniffing.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 56
Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?
A. Organized crime
B. Hacktivist
C. Insider
D. Competitor
Answer: C (LEAVE A REPLY)

NEW QUESTION: 57
A red team initiated a DoS attack on the management interface of a switch using a known vulnerability The monitoring solution then raised an alert prompting a network engineer to log in to the switch to diagnose the issue When the engineer logged in. the red team was able to capture the credentials and subsequently log in to the switch Which of the following actions should the network team take to prevent this type of breach from reoccurring?
A. Enable Secure Shell and disable Telnet
B. Transition from SNMPv2c to SNMPv3 with AES-256
C. Encrypt all communications with TLS 1 3
D. Use a password manager with complex passwords
Answer: A (LEAVE A REPLY)

NEW QUESTION: 58
An attacker exploited a vulnerability on a mail server using the code below.
Which of the following BEST explains what the attacker is doing?
A. The attacker is replacing a document.
B. The attacker is replacing a cookie.
C. The attacker is stealing a document.
D. The attacker is deleting a cookie.
Answer: (SHOW ANSWER)

NEW QUESTION: 59
The Chief Information Security Officer (CISO) at a large company tasks a security administrator to provide additional validation for website customers. Which of the following should the security administrator implement?
A. DNSSEC
B. Captive portal
C. HTTP
D. 802.1X
Answer: (SHOW ANSWER)

NEW QUESTION: 60
The IT department is deploying new computers. To ease the transition, users will be allowed to access
their old and new systems.
The help desk is receive reports that users are experiencing the following error when attempting to log in
to their previous system:
Logon Failure: Access Denied
Which of the following can cause this issue?
A. Misconfigured devices
B. Permission issues
C. Certificate issues
D. Access violations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 61
Several systems and network administrators are determining how to manage access to a facility and enable managers to allow after-hours access. Which of the following access control methods should managers use to assign after-hours access to the employees?
A. Mandatory access control
B. Rule-based access control
C. Role-based access control
D. Discretionary access control
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here:

https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 62
A security analyst is doing a vulnerability assessment on a database server. A scanning tool returns the following information:
There have been several security breaches on the web server that accesses this database. The security team is instructed to mitigate the impact of any possible breaches. The security team is also instructed to improve the security on this database by making it less vulnerable to offline attacks. Which of the following would BEST accomplish these goals? (Choose two.)
A. Generate password hashes using SHA-256
B. Limit users to five attempted logons before they are locked out
C. Force users to change passwords the next time they log on
D. Start using salts to generate MD5 password hashes
E. Require the web server to only use TLS 1.2 encryption
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 63
An auditor wants to test the security posture of an organization by running a tool that will display the following:
Which of the following commands should be used?
A. nc
B. arp
C. ipconfig
D. nbtstat
Answer: D (LEAVE A REPLY)

NEW QUESTION: 64
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:
Answer:

NEW QUESTION: 65
A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener.
Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)
A. nslookup
B. tail

C. tracert
D. nmap
E. tcpdump
F. nc
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 66
A security administrator is analyzing a user report in which the computer exhibits odd network-related outages. The administrator, however, does not see any suspicious processes running. A prior technician's notes indicate the machines has been remediated twice, but the system still exhibits odd behavior. Files were deleted from the system recently. Which of the following is the MOST likely cause of this behavior?
A. Session hijacking
B. Rootkit
C. Logic bomb
D. Crypto-malware
Answer: (SHOW ANSWER)

NEW QUESTION: 67
An organization is expanding its network team. Currently, it has local accounts on all network devices, but with growth, it wants to move to centrally managed authentication. Which of the following are the BEST solutions for the organization? (Select TWO)
A. TACACS+
B. MSCHAPv2
C. CHAP
D. LDAP
E. RADIUS
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 68
A company hires a consulting firm to crawl its Active Directory network with a non-domain account looking for unpatched systems. Actively taking control of systems is out of scope, as is the creation of new administrator accounts. For which of the following is the company hiring the consulting firm?
A. Vulnerability scanning
B. User permission
C. Penetration testing
D. Application fuzzing
Answer: A (LEAVE A REPLY)

NEW QUESTION: 69

Upon learning about a user who has reused the same password for the past several years, a security specialist reviews the logs. The following is an extraction of the report after the most recent password change requirement:
Which of the following security controls is the user's behavior targeting?
A. Password reuse
B. Password complexity
C. Password history
D. Password expiration
Answer: (SHOW ANSWER)

NEW QUESTION: 70
A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:
Based on this data, which of the following actions should the administrator take?
A. Create a blocking policy based on the parameter values.
B. Alert the web server administrators to a misconfiguration.
C. Create an alert to generate emails for abnormally high activity.
D. Change the parameter name 'Account_Name' identified in the log.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 71
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone.
Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)
A. Tethering
B. Rooting/jailbreaking
C. Sideloading
D. Near-field communication.
E. Ad-hoc connections
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 72
A company's AUP requires:
Passwords must meet complexity requirements.
Passwords are changed at least once every six months.
Passwords must be at least eight characters long.
An auditor is reviewing the following report:

Which of the following controls should the auditor recommend to enforce the AUP?
A. Prohibit password reuse
B. Password expiration
C. Account recovery
D. Account lockout thresholds
Answer: (SHOW ANSWER)

NEW QUESTION: 73
A network technician needs to monitor and view the websites that are visited by an employee. The employee is connected to a network switch. Which of the following would allow the technician to monitor the employee's web traffic?
A. Install and configured a transparent proxy server.
B. Implement promiscuous mode on the NIC of the employee's computer.
C. Run a vulnerability scanner to capture DNS packets on the router.
D. Configure a VPN to forward packets to the technician's computer.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 74
Which of the following are considered to be "something you do"? (Choose two.)
A. Iris scan
B. Fingerprint
C. Gait
D. Handwriting
E. PIN
F. CAC card
Answer: (SHOW ANSWER)

NEW QUESTION: 75
A company has a data system with definitions for "Private" and "Public". The company's security policy outlines how data should be protected based on type. The company recently added the data type
"Proprietary". Which of the following is the MOST likely reason the company added this data type?
A. Better data classification
B. Reduced cost
C. Expanded authority of the privacy officer
D. More searchable data
Answer: (SHOW ANSWER)

NEW QUESTION: 76

A security administrator receives notice that a third-party certificate authority has been compromised, and new certificates will need to be issued. Which of the following should the administrator submit to receive a new certificate?

A. PFX
B. CSR
C. CRL
D. CA
E. OSCP

Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 77
A security administrator suspects that a DDoS attack is affecting the DNS server. The administrator accesses a workstation with the hostname of workstation01 on the network and obtains the following output from the ipconfig command:
The administrator successfully pings the DNS server from the workstation. Which of the following commands should be issued from the workstation to verify the DDoS attack is no longer occuring?

A. dig www.google.com
B. dig 192.168.1.254
C. dig workstation01.com
D. dig 192.168.1.26

Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 78
A network technician is setting up a new branch for a company. The users at the new branch will need to access resources securely as if they were at the main location. Which of the following networking concepts would BEST accomplish this?

A. Site-to-site VPN
B. Logical VLANs
C. Out-of-band access
D. Physical network segmentation

E. Virtual network segmentation
Answer: (SHOW ANSWER)

NEW QUESTION: 79
Joe, an employee, wants to show his colleagues how much he knows about smartphones. Joe demonstrates a free movie application that he installed from a third party on his corporate smartphone.
Joe's colleagues were unable to find the application in the app stores. Which of the following allowed Joe to install the application? (Select two.)
A. Rooting/jailbreaking
B. Near-field communication.
C. Ad-hoc connections
D. Tethering
E. Sideloading
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 80
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select TWO).
A. Remove the LDAP directory service role from the server.
B. Install and configure an SSH tunnel on the LDAP server.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Generate an X 509-complaint certificate that is signed by a trusted CA.
E. Ensure port 636 is open between the clients and the servers using the communication.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 81
A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.
Answer:

NEW QUESTION: 82
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select two.)
A. Password history
B. Password lockout
C. Password expiration

D. Password length
E. Password complexity
Answer: A,E (LEAVE A REPLY)

NEW QUESTION: 83
During the penetration testing of an organization, the tester was provided with the names of a few key servers, along with their IP address. Which of the following is the organization conducting?
A. Gray box testing
B. White box testing
C. Isolated container testing
D. Vulnerability testing
E. Black box testing
Answer: (SHOW ANSWER)

NEW QUESTION: 84
A company is performing an analysis of the corporate enterprise network with the intent of identifying any one system, person, function, or service that, when neutralized, will cause or cascade disproportionate damage to the company's revenue, referrals, and reputation. Which of the following is an element of the BIA that this action is addressing?
A. Identication of critical systems
B. Value assessment
C. Risk register
D. Single point of failure
Answer: A (LEAVE A REPLY)

NEW QUESTION: 85
A system's administrator has finished configuring firewall ACL to allow access to a new web server.
The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:
The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?
A. Misconfigured firewall
B. Implicit deny
C. Clear text credentials
D. Default configuration
Answer: (SHOW ANSWER)

NEW QUESTION: 86
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices

used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. WPA using a preshared key

B. WPA2 using a RADIUS back-end for 802.1x authentication

C. Open wireless network and SSL VPN

D. WEP with a 40-bit key

Answer: B (LEAVE A REPLY)

NEW QUESTION: 87

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

Answer:

Explanation:

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a password, codes, PINs, combinations, or secret phrases.

Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

Something you do includes your typing rhythm, a secret handshake, or a private knock

http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle

http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 88

A new hire wants to use a personally owned phone to access company resources. The new hire expresses concern about what happens to the data on the phone when they leave the company. Which of the following portions of the company's mobile device management configuration would allow the company data to be removed from the device without touching the new hire's data?

A. Asset control

B. Device access control

C. Storage lock out

D. Storage segmentation

Answer: D (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 89

You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.

Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.

.

Answer:
Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artifacts.

NEW QUESTION: 90
Which of the following is a document that contains detailed information about actions that include how something will be done, when the actions will be performed, and penalties for failure?
A. MOU
B. ISA
C. BPA
D. SLA
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 91
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:
Ann states the issues began after she opened an invoice that a vendor emailed to her.
Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?
A. Crypto-malware
B. Rootkit
C. Spyware
D. Backdoor
Answer: D (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 92

The security administrator has installed a new firewall which implements an implicit DENY policy by default.
INSTRUCTIONS:
Click on the firewall and configure it to allow ONLY the following communication.
1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.
2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port
3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.
Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.
Hot Area:

Answer:

Explanation

Section: Network Security

Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port
22Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69.
References:Stewart,
James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 26, 44
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 93

For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:

Answer:

Explanation

NEW QUESTION: 94

A security analyst is performing a manual audit of captured data from a packet analyzer. The analyst looks forbase64 encoded strings and applies the filter http.authbasic. Which of the following describes what the analysts looking for?

A. SSL certificate issues
B. Authentication tokens
C. Unencrypted credentials
D. Unauthorized software
Answer: (SHOW ANSWER)

NEW QUESTION: 95
A Chief Information Officer (CIO) wants to eliminate the number of calls the help desk is receiving for password resets when users log on to internal portals. Which of the following is the BEST solution?
A. Implement a self-service portal
B. Decrease lockout threshold
C. Deploy mandatory access control
D. Increase password length
Answer: A (LEAVE A REPLY)

NEW QUESTION: 96
A security administrator learns that PII, which was gathered by the organization, has been found in an open forum. As a result, several C-level executives found their identities were compromised, and they were victims of a recent whaling attack. Which of the following would prevent these problems in the future? (Select TWO).
A. Implement a HIDS.
B. Implement a host-based firewall.
C. Implement a spam filter.
D. Implement a reverse proxy.
E. Implement an email DLP.
Answer: C,E (LEAVE A REPLY)

NEW QUESTION: 97
A security administrator has found a hash in the environment known to belong to malware. The administrator then finds this file to be in in the preupdate area of the OS, which indicates it was pushed from the central patch system.
File: winx86_adobe_flash_upgrade.exe
Hash: 99ac28bede43ab869b853ba62c4ea243
The administrator pulls a report from the patch management system with the following output:
Given the above outputs, which of the following MOST likely happened?
A. The file was corrupted after it left the patch system.
B. The file was embedded with a logic bomb to evade detection.
C. The file was infected when the patch manager downloaded it.
D. The file was not approved in the application whitelist system.
Answer: (SHOW ANSWER)

NEW QUESTION: 98
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential dat a. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.
2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.
3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References: http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

NEW QUESTION: 99

A technician is investigating a report of unusual behavior and slow performance on a company-owned laptop. The technician runs a command and reviews the following information:
Based on the above information, which of the following types of malware should the technician report?
A. Rootkit
B. Spyware
C. Logic bomb
D. RAT
Answer: (SHOW ANSWER)

NEW QUESTION: 100
A security analyst is investigating a vulnerability In which a default file permission was set incorrectly. The company uses non-credentialed scanning for vulnerability management. Which of the following tools can the analyst use to verify the permissions?
A. ssh
B. chmod
C. ls
D. nessus
E. nc
F. setuid
Answer: (SHOW ANSWER)

NEW QUESTION: 101
An organization has created a review process to determine how to best handle data with different sensitivity levels. The process includes the following requirements:
* Soft copy Pll must be encrypted.
* Hard copy Pll must be placed In a locked container.
* Soft copy PHI must be encrypted and audited monthly.
* Hard copy PHI must be placed in a locked container and inventoried monthly.
Locked containers must be approved and designated for document storage. Any violations must be reported to the Chief Security Officer {CSO}.
While searching for coffee in the kitchen, an employee unlocks a cabinet and discovers a list of customer names and phone numbers. Which of the following actions should the employee take?
A. Take custody of the document, secure it at a desk, and report the incident to the CSO.
B. Put the document back in the cabinet, lock the cabinet, and report the incident to the CSO.
C. Put the document back in the cabinet, inventory the contents, lock the cabinet, and report the incident to the CSO.
D. Take custody of the document and immediately report the incident to the CSO.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 102

A security administrator is trying to eradicate a worm, which is spreading throughout the organization, using an old remote vulnerability in the SMB protocol. The worm uses Nmap to identify target hosts within the company. The administrator wants to implement a solution that will eradicate the current worm and any future attacks that may be using zero-day vulnerabilities. Which of the following would BEST meet the requirements when implemented?

A. File integrity checking
B. Host-based firewall
C. Network-based intrusion prevention system
D. Enterprise patch management system
E. Application blacklisting
Answer: (SHOW ANSWER)

NEW QUESTION: 103
A newly purchased corporate WAP needs to be configured in the MOST secure manner possible.
INSTRUCTIONS
Please click on the below items on the network diagram and configure them accordingly:
* WAP
* DHCP Server
* AAA Server
* Wireless Controller
* LDAP Server
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:

NEW QUESTION: 104
An organization has an internal PKI that utilizes client certificates on each workstation. When deploying a new wireless network, the security engineer has asked that the new network authenticate clients by utilizes the existing client certificates. Which of the following authentication mechanisms should be utilized to meet this goal?

A. PEAP
B. EAP-FAST
C. LEAP
D. EAP-TLS
Answer: (SHOW ANSWER)

NEW QUESTION: 105
A security engineer is configuring a system that requires the X.509 certificate information to be pasted into a form field in Base64 encoded format to import it into the system. Which of the following certificate formats should the engineer use to obtain the information in the required format?

A. PFX
B. CER
C. DER
D. PEM
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
During an assessment a security analyst was asked to use a service account to perform a vulnerability scan against the main application server. Which of the following BEST classifies this type of test?
A. Initial exploitation test
B. Escalation of privilege test
C. Credentialed test
D. Non-intrusive test
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 107
An audit takes place after company-wide restricting, in which several employees changed roles. The following deficiencies are found during the audit regarding access to confidential data:
Which of the following would be the BEST method to prevent similar audit findings in the future?
A. Implement regular permission auditing and reviews.
B. Implement rule-based access controls on the human resources server.
C. Implement separation of duties for the payroll department.
D. Implement a DLP solution on the payroll and human resources servers.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 108
A company is developing a new secure technology and requires computers being used for development to be isolated.
Which of the following should be implemented to provide the MOST secure environment?
A. A honeypot residing in a DMZ
B. An ad hoc network with NAT

C. A bastion host
D. A perimeter firewall and IDS
E. An air gapped computer network
Answer: E (LEAVE A REPLY)

NEW QUESTION: 109
A systems engineer is configuring a wireless network. The network must not require installation of third-party software. Mutual authentication of the client and the server must be used. The company has an internal PKI.
Which of the following configurations should the engineer choose?
A. EAP-TLS
B. EAP-TTLS
C. PEAP
D. EAP-MD5
E. EAP-FAST
Answer: A (LEAVE A REPLY)

NEW QUESTION: 110
A security administrator installed a new network scanner that identifies new host systems on the network. Which of the following did the security administrator install?
A. Vulnerability scanner
B. Network-based IDS
C. Configuration compliance scanner
D. Rogue system detection
Answer: D (LEAVE A REPLY)

NEW QUESTION: 111
A web server, which is configured to use TLS with AES-GCM-256, SHA-384, and ECDSA, recently
suffered an information loss breach.
Which of the following is MOST likely the cause?
A. Weak cipher suite
B. Poor implementation
C. Insufficient key bit length
D. Unauthenticated encryption method
Answer: B (LEAVE A REPLY)

NEW QUESTION: 112
A security assessment determines DES and 3DES are still being used on recently deployed production servers. Which of the following did the assessment Identify?
A. Default settings

B. Open permissions
C. Unsecure protocols
D. Weak encryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 113
Which of the following is being used when a malicious actor searches various social media websites to find information about a company's system administrators and help desk staff?
A. Social engineering
B. Initial exploitation
C. Passive reconnaissance
D. Vulnerability scanning
Answer: (SHOW ANSWER)

NEW QUESTION: 114
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:
Answer:
Explanation

NEW QUESTION: 115
A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.
Answer:

NEW QUESTION: 116
A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?
A. A perimeter firewall and IDS
B. An air gapped computer network
C. A honeypot residing in a DMZ
D. An ad hoc network with NAT
E. A bastion host
Answer: B (LEAVE A REPLY)
Explanation

NEW QUESTION: 117

An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server. Which of the following should a security analyst do FIRST?

A. Run a virus scan.

B. Turn off the workstation.

C. Consult information security policy.

D. Make a copy of everything in memory on the workstation.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 118

An analyst wants to implement a more secure wireless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?

A. RADIUS

B. EAP

C. WPA2

D. PEAP

Answer: C (LEAVE A REPLY)

NEW QUESTION: 119

A security consultant discovers that an organization is using the PCL protocol to print documents, utilizing the default driver and print settings. Which of the following is the
MOST likely risk in this situation?

A. SNMP data leaving the printer will not be properly encrypted.

B. Attackers can use the PCL protocol to bypass the firewall of client computers.

C. An MITM attack can reveal sensitive information.

D. An attacker can easily inject malicious code into the printer firmware.

E. An attacker can access and change the printer configuration.

Answer: (SHOW ANSWER)

NEW QUESTION: 120

Task: Determine the types of attacks below by selecting an option from the dropdown list.

Answer:

Explanation:

A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.

B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS) E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 121
Legal authorities notify a company that its network has been compromised for the second time in two years.
The investigation shows the attackers were able to use the same vulnerability on different systems in both attacks. Which of the following would have allowed the security team to use historical information to protect against the second attack?
A. Key risk indicators
B. Lessons learned
C. Tabletop exercise

D. Recovery point objectives
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 122
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
Answer:

NEW QUESTION: 123
A technician is designing a solution that will be required to process sensitive information, including classified government data. The system needs to be common criteria certified. Which of the following should the technician select?
A. Trusted operating system
B. Open-source software applications
C. Hybrid cloud solution
D. Security baseline
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
A security engineer is setting up passwordless authentication for the first time.
INSTRUCTIONS
Use the minimum set of commands to set this up and verify that it works. Commands cannot be reused.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:
Explanation

NEW QUESTION: 125

A security analyst is performing a forensic investigation involving compromised account credentials. Using the Event Viewer, the analyst was able to defect the following message: "Special privileges assigned to new logon.' Several of these messages did not have a valid logon associated with the user before these privileges were assigned. Which of the following attacks is MOST likely being detected?

A. Cross-site scripting

B. Pass-the-hash

C. Session replay

D. Buffer overflow

Answer: D (LEAVE A REPLY)

NEW QUESTION: 126

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

Answer:

Explanation:

* Standard naming convention
* Group policy
* Usage auditing and review
* Permission auditing and review

NEW QUESTION: 127

A security administrator receives alerts from the perimeter UTM. Upon checking the logs, the administrator finds the following output:

Time: 12/25 0300

From Zone: Untrust

To Zone: DMZ

Attacker: externalip.com

Victim: 172.16.0.20

To Port: 80

Action: Alert

Severity: Critical

When examining the PCAP associated with the event, the security administrator finds the following information:

<script> alert ("Click

here for important information regarding your account! http://externalip.com/account.php

"); </script>

Which of the following actions should the security administrator take?

A. Manually copy the <script> data from the PCAP file and generate a blocking signature in the HIDS to block the traffic for future events.

B. Upload the PCAP to the IDS in order to generate a blocking signature to block the traffic.
C. Submit a change request to modify the XSS vulnerability signature to TCP reset on future attempts.
D. Implement a host-based firewall rule to block future events of this type from occurring.
Answer: (SHOW ANSWER)

NEW QUESTION: 128
A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:
Based on this data, which of the following actions should the administrator take?
A. Create a blocking policy based on the parameter values
B. Create an alert to generate emails for abnormally high activity.
C. Change the parameter name 'Account_Name' identified in the log.
D. Alert the web server administrators to a misconfiguration
Answer: (SHOW ANSWER)

NEW QUESTION: 129
A company is executing a strategy to encrypt and sign all proprietary data in transit. The company recently deployed PKI services to support this strategy.
Which of the following protocols supports the strategy and employs certificates generated by the PKI?
(Choose three.)
A. SFTP
B. IPSec
C. SIP
D. TLS
E. Kerberos
F. SAML
G. S/MIME
Answer: A,D,G (LEAVE A REPLY)

NEW QUESTION: 130
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:
Answer:

NEW QUESTION: 131
Which of the following encryption methods does PKI typically use to securely protect keys?
A. Elliptic curve

B. Digital signatures
C. Obfuscation
D. Asymmetric
Answer: (SHOW ANSWER)

NEW QUESTION: 132
An in-house penetration tester is using a packet capture device to listen in on network communications. This is an example of:
A. Exploiting the switch
B. Persistence
C. Escalation of privileges
D. Passive reconnaissance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 133
A user clicked an email link that led to a website than infected the workstation with a virus. The virus
encrypted all the network shares to which the user had access. The virus was not deleted or blocked by
the company's email filter, website filter, or antivirus. Which of the following describes what occurred?
A. The email originated from a private email server with no malware protection.
B. Improper error handling triggered a false negative in all three controls.
C. The user's account was over-privileged.
D. The virus was a zero-day attack.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 134
Task: Determine the types of attacks below by selecting an option from the dropdown list.
Answer:
Explanation
A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers,

executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS) E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security.
Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 135
Given the log output:
Max 15 00:15:23.431 CRT: #SEC_LOGIN-5-LOGIN_SUCCESS:
Login Success [user: msmith] [Source: 10.0.12.45]
[localport: 23] at 00:15:23:431 CET Sun Mar 15 2015
Which of the following should the network administrator do to protect data security?
A. Configure an AAA server
B. Configure port security for logons
C. Disable password and enable RSA authentication
D. Disable telnet and enable SSH
Answer: (SHOW ANSWER)

NEW QUESTION: 136
A security administrator has received multiple calls from the help desk about customers who are unable to access the organization's web server. Upon reviewing the log files the security administrator determines multiple open requests have been made from multiple IP addresses, which is consuming system resources. Which of the following attack types does this BEST describe?
A. DoS
B. Zero day
C. DDoS
D. Logic bomb
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 137
An organization wants to conduct secure transactions of large data files. Before encrypting and exchanging the data files, the organization wants to ensure a secure exchange of keys.
Which of the following algorithms is appropriate for securing the key exchange?
A. Blowfish
B. DSA
C. Diffie-Hellman
D. 3DES
E. DES
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
DRAG DROP
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan-Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simul- ation, please select the Done button to submit.
Answer:
Explanation:

Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas.
CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access.
Locking cabinets can be used to protect backup media, documentation and other physical artefacts.
References:
Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 369

NEW QUESTION: 139
A system's administrator has finished configuring firewall ACL to allow access to a new web server.
The security administrator confirms form the following packet capture that there is network traffic from the
internet to the web server:
The company's internal auditor issues a security finding and requests that immediate action be taken. With
which of the following is the auditor MOST concerned?
A. Implicit deny
B. Misconfigured firewall
C. Default configuration
D. Clear text credentials
Answer: (SHOW ANSWER)

NEW QUESTION: 140
An organization is collecting logs from its critical infrastructure and a large number of the events are common system activities with identical logs This is causing the SI EM to consume a large amount of disk space, which may result in the organization having to purchase additional disks to store the logs. Which of the following should the organization do to help mitigate this problem?
A. Enable log aggregation
B. Enable log correlation
C. Enable log filtering.
D. Enable event deduplication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 141
Drag and Drop Question
Task: Determine the types of attacks below by selecting an option from the dropdown list.
Answer:

Explanation:
A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS).
E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security. Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 142
A technician suspects that a desktop was compromised with a rootkit. After removing lhe hard drive from the desktop and running an offline le integrity check, the technician reviews the following output:
Based on the above output, which of the following is the malicious file?
A. notepad.exe
B. kernel.dll
C. lsass.exe
D. httpd.axe
Answer: (SHOW ANSWER)

NEW QUESTION: 143
Which of the following use the SSH protocol?
A. SNMP
B. Stelnet
C. SSL
D. SFTP
E. SCP
F. FTPS
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 144
For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases.
Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something
you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 145
Which of the following technologies employ the use of SAML? (Select TWO).
A. Single sign-on
B. LDAP

C. Secure token
E RADIUS
D. Federation
Answer: (SHOW ANSWER)

NEW QUESTION: 146
A user from the financial aid office is having trouble interacting with the finaid directory on the university's ERP system. The systems administrator who took the call ran a command and received the following output:
Subsequently, the systems administrator has also confirmed the user is a member of the finaid group on the ERP system.
Which of the following is the MOST likely reason for the issue?
A. The permissions on the finaid directory should be drwxrwxrwx.
B. The finaid directory should be d---rwx---
C. The problem is local to the user, and the user should reboot the machine.
D. The files on the finaid directory has an improper group assignment.
Answer: (SHOW ANSWER)

NEW QUESTION: 147
Two users need to send each other emails over unsecured channels. The system should support the
principle of non-repudiation. Which of the following should be used to sign the user's certificates?
A. CA
B. CSR
C. CRL
D. RA
Answer: (SHOW ANSWER)

NEW QUESTION: 148
Which of the following controls is implemented in lieu of the primary security controls?
A. Compensating
B. Deterrent
C. Detective
D. Corrective
Answer: (SHOW ANSWER)

NEW QUESTION: 149
A technician is implementing 802 1X with dynamic VLAN assignment based on a user Active Directory group membership Which of the following configurations supports the VLAN definitions?
A. Shibboleth IdP
B. LDAP path

C. SAML tag
D. RADIUS attribute
Answer: (SHOW ANSWER)

NEW QUESTION: 150
Which of the following are examples of two-factor authentication? (Select THREE)
A. Proximity reader and password
B. Password and TOTP
C. Voice recognition and fingerprint
D. Smart card and ID badge
E. User ID and password
F. Smart card and PIN
Answer: A,B,F (LEAVE A REPLY)

NEW QUESTION: 151
Proprietary information was sent by an employee to a distribution list that included external email addresses.
Which of the following BEST describes the incident that occurred and the threat actor in this scenario?
A. Unintentional disclosure by an insider
B. Corporate espionage by a competitor
C. MITM attack by a script kiddle
D. Social engineering by a hacktivist
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 152
An organization wants to separate permissions for individuals who perform system changes from individuals who perform auditing of those system changes. Which of the following access control approaches is BEST suited for this?
A. Assign administrators and auditors to different groups and restrict permissions on system log files to read- only for the auditor group.

B. Assign administrators and auditors to the same group, but ensure they have different permissions based on the function they perform.
C. Create two groups and ensure each group has representation from both the auditors and the administrators so they can verify any changes that were made.
D. Assign file and folder permissions on an individual user basis and avoid group assignment altogether.
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 153
Which of the following generates reports that show the number of systems that are associated with POODLE, 3DES, and SMBv1 listings?
A. A honeypot
B. A UTM appliance
C. A vulnerability scanner
D. A protocol analyzer
Answer: C (LEAVE A REPLY)

NEW QUESTION: 154
A systems administrator is configuring a new network switch for TACACS+ management and authentication.
Which of the following must be configured to provide authentication between the switch and the TACACS+ server?
A. 802.1X
B. SSH
C. Shared secret
D. SNMPv3
E. CHAP
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 155
A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him.
Which of the following BEST describes what occurred?
A. The hacker used a pass-the-hash attack.
B. The hacker used a race condition.
C. The hacker-exploited importer key management.
D. The hacker exploited weak switch configuration.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 156
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:
Answer:

NEW QUESTION: 157
A security administrator needs to create a RAID configuration that is focused on high read speeds and fault tolerance. It is unlikely that multiple drives will fail simultaneously. Which of the following RAID configurations should the administrator use?
A. RAID 0
B. RAID 1
C. RAID 5
D. RAID 10
Answer: (SHOW ANSWER)
RAID 10, also known as RAID 1+0, is a RAID configuration that combines disk mirroring and disk striping to protect data. It requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved.

NEW QUESTION: 158
A security administrator must implement a system to ensure that invalid certificates are not used by a custom developed application. The system must be able to check the validity of certificates even when internet access is unavailable.
Which of the following MUST be implemented to support this requirement?
A. CRL
B. SSH
C. CSR
D. OCSP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 159
A systems administrator is attempting to recover from a catastrophic failure in the datacenter. To recover
the domain controller, the systems administrator needs to provide the domain administrator credentials.
Which of the following account types is the systems administrator using?
A. Local account
B. Guest account
C. User account
D. Service account
Answer: (SHOW ANSWER)

NEW QUESTION: 160
An organization needs to implement a large PKI. Network engineers are concerned that repeated transmission of the OCSP will impact network performance. Which of the following should the security analyst recommend is lieu of an OCSP?
A. OID
B. CSR
C. CA
D. CRL
Answer: D (LEAVE A REPLY)

NEW QUESTION: 161
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?
A. Redundancy
B. Elasticity
C. High availability
D. Scalability
Answer: C (LEAVE A REPLY)

NEW QUESTION: 162
A systems administrator is reviewing the following information from a compromised server:
Given the above information, which of the following processes was MOST likely exploited via a remote buffer overflow attack?
A. LSASS
B. TFTP
C. Apache
D. MySQL
Answer: C (LEAVE A REPLY)

NEW QUESTION: 163
When connected to a secure WAP, which of the following encryption technologies is MOST likely to be configured when connecting to WPA2-PSK?
A. WEP
B. AES
C. MD5
D. DES
Answer: B (LEAVE A REPLY)

NEW QUESTION: 164

You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.
The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.
Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Answer:

NEW QUESTION: 165
Which of the following is the main difference an XSS vulnerability and a CSRF vulnerability?
A. XSS does not need the victim to be authenticated to the trusted server.
B. CSRF needs the victim to be authenticated to the trusted server.
C. XSS needs the attacker to be authenticated to the trusted server.
D. CSRF does not need the attacker to be authenticated to the trusted server.
E. CSRF does not need the victim to be authenticated to the trusted server.
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 166
A security analyst is testing both Windows and Linux systems for unauthorized DNS zone transfers within a LAN on comptia.org from example.org. Which of the following commands should the security analyst use? (Select two.)
A. Option B
B. Option F
C. Option C
D. Option D
E. Option A
F. Option E
Answer: C,E (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 167
An information system owner has supplied a new requirement to the development team that calls for increased non-repudiation within the application. After undergoing several audits, the owner determined that current levels of non-repudiation were insufficient.
Which of the following capabilities would be MOST appropriate to consider implementing is response to the new requirement?
A. Two-factor authentication
B. Digital signatures
C. Transitive trust
D. One-time passwords
E. Symmetric encryption
Answer: (SHOW ANSWER)

NEW QUESTION: 168
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.
The IT security department finds the following security configuration for the accounts payable module:
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?
A. Option C
B. Option B
C. Option D
D. Option A
Answer: D (LEAVE A REPLY)

NEW QUESTION: 169

Ann, a new employee, received an email from an unknown source indicating she needed to click on the provided link to update her company's profile. Once Ann clicked the link, a command prompt appeared with the following output:
Which of the following types of malware was executed?
A. Adware
B. Spyware
C. Ransomware
D. Virus
Answer: C (LEAVE A REPLY)

NEW QUESTION: 170
A new network administrator is establishing network circuit monitoring guidelines to catch potentially malicious traffic. The administrator begins monitoring the NetFlow statistics tor the critical Internet circuit and notes the following data after two weeks.
However, after checking the statistics from the weekend following the compiled statistics the administrator notices a spike in traffic to 250Mbps sustained for one hour The administrator is able to track the source of the spike to a server in the DMZ Which of the following is the next BEST course of action the administrator should take?
A. Consult the NetFlow logs on the NetFlow server to determine what data was being transferred
B. Immediately open a Seventy 1 case with the security analysts to address potential data exfiltration
C. Rerun the baseline data gathering for an additional four weeks and compare the results
D. Enable a packet capture on the firewall to catch the raw packets on the next occurrence
Answer: (SHOW ANSWER)

NEW QUESTION: 171
Which of the following should a company require prior to performing a penetration test?
A. Data classification
B. NDA
C. List of threats
D. CVE score
Answer: B (LEAVE A REPLY)

NEW QUESTION: 172
A junior systems administrator noticed that one of two hard drives in a server room had a red error notification. The administrator removed the hard drive to replace it but was unaware that the server was configured in an array. Which of the following configurations would ensure no data is lost?
A. RAID 3
B. RAID 1
C. RAID 0

D. RAID 2
Answer: B (LEAVE A REPLY)

NEW QUESTION: 173
An organization has implemented an IPSec VPN access for remote users.
Which of the following IPSec modes would be the MOST secure for this organization to implement?
A. Tunnel mode
B. Transport mode
C. AH-only mode
D. ESP-only mode
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation:
In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

NEW QUESTION: 174
The president of a company that specializes in military contracts receives a request for an interview. During the interview, the reporter seems more interested in discussing the president's family life and personal history than the details of a recent company success. Which of the following security concerns is this MOST likely an example of?
A. Insider threat
B. Social engineering
C. Passive reconnaissance
D. Phishing
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 175
A vulnerability scan was run multiple times. The first lime, the scan detected multiple operating system flaws The second time the scan indicated that a few third-party application programs required patching and no operating system flaws. Which of the following is the MOST likely cause tor the different scan results?
A. The initial scan used credentials mat had limited access to system resources
B. The first scan had full-system scanning capabilities
C. The second scan used credentials that were configured for time-of-day scanning
D. The vulnerability scanner was not configured with the common vulnerability and exposure database
Answer: B (LEAVE A REPLY)

NEW QUESTION: 176
An administrator requests a new VLAN be created to support the installation of a new SAN. Which of the following data transport?
A. Sonet
B. SAS
C. ISCSI
D. Fibre Channel
Answer: (SHOW ANSWER)

NEW QUESTION: 177
Two companies need to exchange a large number of confidential files Both companies run high availability UTM devices They do not want to use email systems to exchange the data Since the data needs to be exchanged m both directions, which of the following solutions should a security analyst recommend7
A. Exchanging data by using a free cloud-storage product
B. Establishing a site-to-site VPN between the two companies
C. Configuring an FTP server in one company
D. Configuring the remote access feature on both UTMs
Answer: (SHOW ANSWER)

NEW QUESTION: 178
A security analyst wants to obfuscate some code and decides to use ROT13. Which of the following is an example of the text "HELLO WORLD" in ROT13?
A. URYYB JBEYQ
B. DLROWOLLEH
C. QYEBJ BYYRU
D. KHOOR ZRUOG
Answer: A (LEAVE A REPLY)

NEW QUESTION: 179
A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission. Which of the following is an element of a BIA that is being addressed?
A. Mission-essential function
B. Single point of failure
C. backup and restoration plans
D. Identification of critical systems
Answer: A (LEAVE A REPLY)
Explanation
The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the

impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

NEW QUESTION: 180
A security engineer wants to further secure a sensitive VLAN on the network by introducing MFA. Which of the following is the BEST example of this?
A. Secret Question: 01 01 and CAPTCHA
B. fingerprint scanner and voice recognition
C. PSK and PIN
D. RSA token and password
Answer: (SHOW ANSWER)

NEW QUESTION: 181
A computer on a company network was infected with a zero-day exploit after an employee accidently
opened an email that contained malicious content. The employee recognized the email as malicious and
was attempting to delete it, but accidently opened it.
Which of the following should be done to prevent this scenario from occurring again in the future?
A. Install host-based firewalls on all computers that have an email client installed
B. Install end-point protection on all computers that access web email
C. Set the email program default to open messages in plain text
D. Create new email spam filters to delete all messages from that sender
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 182
A systems administrator is increasing the security settings on a virtual host to ensure users on one VM cannot access information from another VM. Which of the following is the administrator protecting against?
A. VM escape
B. VM sandboxing
C. VM migration

D. VM sprawl
Answer: D (LEAVE A REPLY)

NEW QUESTION: 183
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords. Which of the following technical controls would help prevent these policy violations? (Select two.)
A. Password length
B. Password lockout
C. Password history
D. Password complexity
E. Password expiration
Answer: (SHOW ANSWER)

NEW QUESTION: 184
DRAG DROP
Drag and drop the correct protocol to its default port.
Answer:
Explanation:
FTP uses TCP port 21.
Telnet uses port 23.
SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file- transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).
SMTP uses TCP port 25.
Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 42, 45, 51
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 185
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.
Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?

A. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.
B. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.
C. Apply MAC filtering and see if the router drops any of the systems.
D. Physically check each of the authorized systems to determine if they are logged onto the network.
Answer: (SHOW ANSWER)

NEW QUESTION: 186
A company has won an important government contract. Several employees have been transferred from their existing projects to support a new contract. Some of the employees who have transferred will be working long hours and still need access to their project information to transition work to their replacements.
Which of the following should be implemented to validate that the appropriate offboarding process has been followed?
A. Mandatory access control
B. Permission auditing
C. Time-of-day restrictions
D. Separation of duties
Answer: B (LEAVE A REPLY)

NEW QUESTION: 187
A company is developing a new secure technology and requires computers being used for development to be isolated. Which of the following should be implemented to provide the MOST secure environment?
A. An ad hoc network with NAT
B. A bastion host
C. An air gapped compiler network
D. A honeypot residing in a DMZ
E. A perimeter firewall and IDS
Answer: D (LEAVE A REPLY)

NEW QUESTION: 188
An attacker compromises a public CA and issues unauthorized X.509 certificates for Company.com. In the future, Company.com wants to mitigate the impact of similar incidents.
Which of the following would assist Company.com with its goal?
A. Certificate with extended validation
B. Certificate chaining
C. Certificate pinning
D. Certificate stapling

Answer: (SHOW ANSWER)

NEW QUESTION: 189
An information security specialist is reviewing the following output from a Linux server.
Based on the above information, which of the following types of malware was installed on the server?
A. Trojan
B. Logic bomb
C. Backdoor
D. Rootkit
E. Ransomware
Answer: B (LEAVE A REPLY)

NEW QUESTION: 190
A security analyst runs a monthly file integrity check on the main web server. When analyzing the logs, the analyst observed the following entry:
No OS patches were applied to this server during this period. Considering the log output, which of the following is the BEST conclusion?
A. The iexplore.exe was executed on the scanned server between the two dates. An incident ticket should be created.
B. The cmd.exe was executed on the scanned server between the two dates. An incident ticket should be created
C. The iexplore.exe was updated on the scanned server. An incident ticket should be created.
D. The cmd.exe was updated on the scanned server. An incident ticket should be created
Answer: D (LEAVE A REPLY)

NEW QUESTION: 191
An administrator performs a workstation audit and finds one that has non-standard software installed. The administrator then requests a report to see if a change request was completed for the installed software. The report shows a request was completed. Which of the following has the administrator found?
A. A license compliance violation
B. A baseline deviation
C. Unauthorized software
D. An insider threat
Answer: B (LEAVE A REPLY)

NEW QUESTION: 192
A cybersecurity analyst is looking into the payload of a random packet capture file that was selected for analysis. The analyst notices that an internal host had a socket established with another internal host over a non-standard port.

Upon investigation, the origin host that initiated the socket shows this output:
Given the above output, which of the following commands would have established the questionable socket?
A. traceroute 8.8.8.8
B. nc -1 192.168.5.1 -p 9856
C. ping -1 30 8.8.8.8 -a 600
D. pskill pid 9487
Answer: B (LEAVE A REPLY)

NEW QUESTION: 193
A company is deploying smartphones for its mobile salesforce. These devices are for personal and business use but are owned by the company. Sales personnel will save new customer data via a custom application developed for the company. This application will integrate with the contact information stored in the smartphones and will populate new customer records onto it. The customer application's data is encrypted at rest, and the application's connection to the back office system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer contact information may be accidentally leaked due to the limited security capabilities of the devices and the planned controls. Which of the following will be the MOST efficient security control to implement to lower this risk?
A. Restrict contact information storage dataflow so it is only shared with the customer application.
B. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact information.
C. Require complex passwords for authentication when accessing the contact information.
D. Restrict screen capture features on the devices when using the custom application and the contact information.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 194
An incident response analyst in a corporate security operations center receives a phone call from an SOC analyst. The SOC analyst explains the help desk recently reimaged a workstation that was suspected of being infected with an unknown type of malware; however, event after reimaging, the host continued to generate SIEM alerts. Which of the following types of malware is MOST likely responsible for producing the SIEM alerts?
A. Logic bomb
B. Ransomware
C. Rootkit
D. Adware
Answer: (SHOW ANSWER)

NEW QUESTION: 195
Question: 149

A. CRL
B. CER
C. PEM
D. OCSP
E. PFX
F. SCEP
Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 196
A security administrator is reviewing the following report from an organization's patch management system that has only wired workstations which are utilized daily:
Which of the following is the GREATEST security concern for the administrator?
A. The browser version on ACCT-1 is newer than the rest.
B. ACCT-2 is no longer connecting from the organization's network
C. The status of ACCT-1 is not accurately reported
D. SALES-2 does not have the finance application installed
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 197
A technician suspects that a desktop was compromised with a rootkit. After removing lhe hard drive from the desktop and running an offline le integrity check, the technician reviews the following output:
Based on the above output, which of the following is the malicious file?
A. lsass.exe
B. notepad.exe
C. kernel.dll
D. httpd.axe
Answer: (SHOW ANSWER)

NEW QUESTION: 198
Ann. An employee in the payroll department, has contacted the help desk citing multiple issues with her device, including:

Ann states the issues began after she opened an invoice that a vendor emailed to her. Upon opening the invoice, she had to click several security warnings to view it in her word processor. With which of the following is the device MOST likely infected?

A. Backdoor

B. Crypto-malware

C. Spyware

D. Rootkit

Answer: A (LEAVE A REPLY)

NEW QUESTION: 199

A technician wants to configure a wireless router at a small office that manages a family-owned dry cleaning business. The router will support five laptops, potential smartphones, a wireless printer, and occasional guests.

Which of the following wireless configuration is BEST implemented in this scenario?

A. 802.1X with guest VLAN

B. Captive portal with two-factor authentication

C. Single SSID with WPA2-Enterprise

D. Dual SSID with WPA2-PSK

Answer: (SHOW ANSWER)

NEW QUESTION: 200

SIMULATION

A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.

You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.

Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

See the solution below.

Explanation:

Database server was attacked, actions should be to capture network traffic and Chain of Custody.

IDS Server Log:

Web Server Log:

Database Server Log:
Users PC Log:

NEW QUESTION: 201
A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned with the new website and provides the following log to support the concern:
Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?
A. Changing the account standard naming convention
B. Implementing account lockouts
C. Increasing the minimum password length from eight to ten characters
D. Discontinuing the use of privileged accounts
Answer: A (LEAVE A REPLY)

NEW QUESTION: 202
A company wants to ensure confidential data from storage media is sanitized in such a way that the drive cannot be reused. Which of the following method should the technician use?
A. Overwriting
B. Low-level formatting
C. Repartitioning
D. Wiping
E. Shredding
Answer: E (LEAVE A REPLY)

NEW QUESTION: 203
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artifacts.

NEW QUESTION: 204

A forensic analyst is asked to respond to an ongoing network attack on a server. Place the items in the list below in the correct order in which the forensic analyst should preserve them.

Answer:

Explanation

When dealing with multiple issues, address them in order of volatility (OOV); always deal with the most volatile first. Volatility can be thought of as the amount of time that you have to collect certain data before a window of opportunity is gone. Naturally, in an investigation you want to collect everything, but some data will exist longer than others, and you cannot possibly collect all of it once. As an example, the OOV in an investigation may be RAM, hard drive data, CDs/DVDs, and printouts.

Order of volatility: Capture system images as a snapshot of what exists, look at network traffic and logs, capture any relevant video/screenshots/hashes, record time offset on the systems, talk to witnesses, and track total man-hours and expenses associated with the investigation.

NEW QUESTION: 205

A security analyst is investigating a potential reach. Upon gathering, documenting, and securing the evidence, which of the following actions is the NEXT step to minimize the business impact?

A. Initiate the incident response plan

B. Remove malware and restore the system to normal operation

C. Launch an investigation to identify the attacking host

D. Review lessons learned captured in the process

Answer: B (LEAVE A REPLY)

NEW QUESTION: 206

Systems administrator and key support staff come together to simulate a hypothetical interruption of service. The team updates the disaster recovery processes and documentation after meeting. Which of the following describes the team's efforts?

A. Order of restoration

B. Business impact analysis

C. Tabletop exercise

D. Continuity of operation

Answer: (SHOW ANSWER)

NEW QUESTION: 207

A security administrator is given the security and availability profiles for servers that are being deployed.

* Match each RAID type with the correct configuration and MINIMUM number of drives.

* Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:

* All drive definitions can be dragged as many times as necessary

* Not all placeholders may be filled in the RAID configuration boxes

* If parity is required, please select the appropriate number of parity checkboxes
* Server profiles may be dragged only once
RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity. RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.
RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.
RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.
http://www.adaptec.com/en-us/solutions/raid_levels.html
Answer:

NEW QUESTION: 208
A security administrator is implementing a SIEM and needs to ensure events can be compared against each other based on when the events occurred and were collected. Which of the following does the administrator need to implement to ensure this can be accomplished?
A. TOTP
B. TKJP
C. HOTP
D. NTP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 209
You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.
The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.

In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.
Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Answer:

NEW QUESTION: 210
Which of the following involves the use of targeted and highly crafted custom attacks against a population of users who may have access to a particular service or program?
A. Vishing
B. Phishing
C. Hoaxing
D. Spear phishing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 211
The POODLE attack is an MITM exploit that affects:
A. TLS1.0 with CBC mode cipher
B. SSLv2.0 with CBC mode cipher
C. SSLv3.0 with CBC mode cipher
D. SSLv3.0 with ECB mode cipher
Answer: (SHOW ANSWER)
Explanation
A flaw was found in the way SSL 3.0 handled padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode.
How To Protect your Server Against the POODLE SSLv3 Vulnerability On October 14th, 2014, a vulnerability in version 3 of the SSL encryption protocol was disclosed. This vulnerability, dubbed POODLE (Padding Oracle On Downgraded Legacy Encryption), allows an attacker to read information encrypted with this version of the protocol in plain text using a man-in-the-middle attack.
Although SSLv3 is an older version of the protocol which is mainly obsolete, many pieces of software still fall back on SSLv3 if better encryption options are not available. More importantly, it is possible for an attacker to force SSLv3 connections if it is an available alternative for both participants attempting a connection.
The POODLE vulnerability affects any services or clients that make it possible to communicate using SSLv3.

Because this is a flaw with the protocol design, and not an implementation issue, every piece of software that uses SSLv3 is vulnerable.
To find out more information about the vulnerability, consult the CVE information found at CVE-2014-3566.
What is the POODLE Vulnerability?
The POODLE vulnerability is a weakness in version 3 of the SSL protocol that allows an attacker in a man-inthe-middle context to decipher the plain text content of an SSLv3 encrypted message.
Who is Affected by this Vulnerability?
This vulnerability affects every piece of software that can be coerced into communicating with SSLv3. This means that any software that implements a fallback mechanism that includes SSLv3 support is vulnerable and can be exploited.
Some common pieces of software that may be affected are web browsers, web servers, VPN servers, mail servers, etc.
How Does It Work?
In short, the POODLE vulnerability exists because the SSLv3 protocol does not adequately check the padding bytes that are sent with encrypted messages.
Since these cannot be verified by the receiving party, an attacker can replace these and pass them on to the intended destination. When done in a specific way, the modified payload will potentially be accepted by the recipient without complaint.
An average of once out of every 256 requests will accepted at the destination, allowing the attacker to decrypt a single byte. This can be repeated easily in order to progressively decrypt additional bytes. Any attacker able to repeatedly force a participant to resend data using this protocol can break the encryption in a very short amount of time.
How Can I Protect Myself?
Actions should be taken to ensure that you are not vulnerable in your roles as both a client and a server. Since encryption is usually negotiated between clients and servers, it is an issue that involves both parties.
Servers and clients should should take steps to disable SSLv3 support completely. Many applications use better encryption by default, but implement SSLv3 support as a fallback option. This should be disabled, as a malicious user can force SSLv3 communication if both participants allow it as an acceptable method.

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 212
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.
The systems administrator reviews the output below:
Based on the above information, which of the following types of malware was installed on the user's computer?
A. Worm
B. Bot
C. Keylogger
D. RAT
E. Spyware
Answer: (SHOW ANSWER)

NEW QUESTION: 213
An attack has occurred against a company.
INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1)
Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging them to the correct server. (Answer area 2)
All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:
Explanation:

NEW QUESTION: 214
A member of the human resources department received the following email message after sending an email containing benefit and tax information to a candidate:
"Your message has been quarantined for the following policy violation: external potential_PII. Please contact the IT security administrator for further details".
Which of the following BEST describes why this message was received?
A. The DLP system flagged the message.
B. The mail gateway prevented the message from being sent to personal email addresses.
C. The file integrity check failed for the attached files.
D. The company firewall blocked the recipient's IP address.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 215

A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized.
Which of the following solutions would BEST meet these requirements?
A. Multifactor authentication
B. PKI
C. Federation
D. SSO
E. Biometrics
Answer: D (LEAVE A REPLY)

NEW QUESTION: 216
Which of the following differentiates a collision attack from a rainbow table attack?
A. In a collision attack, the hash and the input data are equivalent
B. In a collision attack, the same input results in different hashes
C. A rainbow table attack performs a hash lookup
D. A rainbow table attack uses the hash as a password
Answer: C (LEAVE A REPLY)

NEW QUESTION: 217
A network administrator is attempting to troubleshoot an issue regarding certificates on a secure website.
During the troubleshooting process, the network administrator notices that the web gateway proxy on the local network has signed all of the certificates on the local machine.
Which of the following describes the type of attack the proxy has been legitimately programmed to perform?
A. Replay
B. Transitive access
C. Spoofing
D. Man-in-the-middle
Answer: D (LEAVE A REPLY)

NEW QUESTION: 218
Leveraging the information supplied below, complete the CSR for the server to set up TLS (HTTPS)
* Hostname: ws01
* Domain: comptia.org
* IPv4: 10.1.9.50
* IPV4: 10.2.10.50
* Root: home.aspx
* DNS CNAME:homesite.

Instructions:
Drag the various data points to the correct locations within the CSR. Extension criteria belong in the let hand column and values belong in the corresponding row in the right hand column.
Answer:

NEW QUESTION: 219
For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases.
Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 220
A small enterprise decides to implement a warm site to be available for business continuity in case of a disaster. Which of the following BEST meets its requirements?
A. A fully operational site that has all the equipment in place and full data backup tapes on site
B. A site used for its data backup storage that houses a full-time network administrator
C. An operational site requiring some equipment to be relocated as well as data transfer to the site
D. A site staffed with personnel requiring both equipment and data to be relocated there in case of disaster
Answer: C (LEAVE A REPLY)
Explanation
Cold site
Space and associated infrastructure (e.g., power, telecoms and environmental controls to support IT systems), which will only be installed when disaster recovery (DR) services are activated.
Warm site
Site that's partially equipped with some of the equipment (e.g., computing hardware and software, and supporting personnel); organizations install additional equipment, computing hardware and software, and supporting personnel when DR services are activated.
Hot site

Fully equipped site with the required equipment, computing hardware/software and supporting personnel; it's also fully functional and manned on a 24x7 basis so that it's ready for organizations to operate their IT systems when DR services are activated.

NEW QUESTION: 221
A security administrator is reviewing the following network capture:
192.168.20.43:2043 -> 10.234.66.21:80
POST "192.168.20.43
https://www.banksite.com<ENTER>JoeUsr<BackSPACE>erPassword<ENTER>"
Which of the following malware is MOST likely to generate the above information?
A. Ransomware
B. Keylogger
C. adware
D. Logic bomb
Answer: A (LEAVE A REPLY)

NEW QUESTION: 222
After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.
The systems administrator reviews the output below:
Based on the above information, which of the following types of malware was installed on the user's computer?
A. RAT
B. Keylogger
C. Spyware
D. Worm
E. Bot
Answer: A (LEAVE A REPLY)
The winserver.exe file is a remote access Trojan (RAT). All of the other executable names displayed by netstat are valid.
The RAT acronym stands for Remote Administration Tool. A RAT is a software, popularly used to control other computers remotely.
To hack a computer remotely using a RAT, you have to create a server and then send this server to the victim whose computer you're trying to hack. Generally, this server is binded to any file, like a picture or song, so that whenever the victim opens the file on his computer, our server is installed. This server opens a port on the victim's computer, allowing you to remotely hack the device via the open port.
Some examples of RATs are:
Prorat
Turkojan
Yuri RAT and many other.

A worm is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction.
A logic bomb is a string of code embedded into an application or script that will execute in response to an event.
Ransomware is a specific type of Trojan that typically encrypts the user's data until the user pays a ransom.
Ransomware that encrypts data is often called crypto-malware.
Because winserver.exe is known malware, the netstat output does indicate malware is running.

NEW QUESTION: 223
Which of the following is a risk that is specifically associated with hosting applications in the public cloud?
A. Unsecured root accounts
B. Zero-day
C. Insider threat
Insider Threat
An attack from inside your organization may seem unlikely, but the insider threat does exist. Employees can use their authorized access to an organization's cloud-based services to misuse or access information such as customer accounts, financial forms, and other sensitive information.
Additionally, these insiders don't even need to have malicious intentions.
A study by Imperva, "Inside Track on Insider Threats" found that an insider threat was the misuse of information through malicious intent, accidents or malware. The study also examined four best practices companies could follow to implement a secure strategy, such as business partnerships, prioritizing initiatives, controling access, and implementing technology.
D. Shared tenancy
Answer: C (LEAVE A REPLY)

NEW QUESTION: 224
A security administrator discovers that an attack has been completed against a node on the corporate network.
All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset

button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

See the solution below.

Explanation

Database server was attacked, actions should be to capture network traffic and Chain of Custody.

IDS Server Log:

Web Server Log:

Database Server Log:

Users PC Log:

NEW QUESTION: 225

A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web

server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:

Which of the following rules would be BEST to resolve the issue?

A:

B:

C:

D:

A. Option C

B. Option A

C. Option D

D. Option B

Answer: (SHOW ANSWER)

NEW QUESTION: 226

An organization is using a tool to perform a source code review. Which of the following describes the case in which the tool incorrectly identifies the vulnerability?

A. False negative

B. True positive

C. False positive

D. True negative

Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501

exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 227
Which of the following BEST describes a defense-in-depth strategy?
A. The security team configures an application-whitelisting program on endpoints and installs NIDS.
B. A security administrator places a web server behind two firewalls from two different vendors with only ports 80 and 443 open
C. Outbound traffic travels through a proxy and a stateful firewall with ports 80 and 443 open
D. The security architect scans servers daily with a vulnerability scanner and conducts weekly penetration-testing exercises
Answer: A (LEAVE A REPLY)

NEW QUESTION: 228
A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:
Which of the following would be the BEST method for preventing this type of suspected attack in the future?
A. Implement restrictions on shared credentials
B. Implement time-of-day restrictions on this server
C. Implement password expirations
D. Implement account lockout settings
Answer: D (LEAVE A REPLY)

NEW QUESTION: 229
A network administrator adds an ACL to allow only HTTPS connections form host 192.168.2.3 to web server 192.168.5.2. After applying the rule, the host is unable to access the server. The network administrator runs the output and notices the configuration below:
Which of the following rules would be BEST to resolve the issue?
A:
B:
C:
D:
A. Option D
B. Option A
C. Option B
D. Option C

Answer: B (LEAVE A REPLY)

NEW QUESTION: 230
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?
A. LDAP services
B. Kerberos services
C. NTLM services
D. CHAP services
Answer: B (LEAVE A REPLY)
Explanation
Only Kerberos that can do Mutual Auth and Delegation.

NEW QUESTION: 231
A company has a backup site with equipment on site without any data. This is an example of:
A. a hot site.
B. a hot standby.
C. a cold site.
D. a warrn site.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 232
Which of the following could an attacker use to overwrite instruction pointers in order to execute malicious code?
A. Buffer overow
B. SQL injection
C. Resource exhaustion
D. Memory leak
Answer: A (LEAVE A REPLY)

NEW QUESTION: 233
It determining when it may be necessary to perform a credentialed scan against a system instead of a non-credentialed scanner requirements is MOST likely to influence this decision?
A. The scanner must be able to footprint the network.
B. The scanner must be able to enumerate the host OS of devices scanned.
C. The scanner must be able to audit file system permissions.
D. The scanner must be able to check for open ports with listening services.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 234

Which of the following terms BEST describes an exploitable vulnerability that exists but has not been publicly disclosed yet?
A. Zero-day
B. Design weakness
C. Logic bomb
D. Trojan
Answer: (SHOW ANSWER)

NEW QUESTION: 235
A company needs to fix some audit findings related to its physical security. A key finding was that multiple people could physically enter a location at :ne same time. Which of the following is the BEST control to address this audit finding?
A. Biometrics
B. Mantrap
C. Faraday cage
D. Proximity cards
Answer: B (LEAVE A REPLY)

NEW QUESTION: 236
An organization wants to set up a wireless network in the most secure way. Budget is not a major consideration, and the organization is willing to accept some complexity when clients are connecting. It is also willing to deny wireless connectivity for clients who cannot be connected in the most secure manner. Which of the following would be the MOST secure setup that conforms to the organization's requirements?
A. Use WPA2-PSK with a 24-character complex password and change the password monthly.
B. Enable WPA2-PSK, disable all other modes, and implement MAC filtering along with port security.
C. Enable WPA2-PSK for older clients and WPA2-Enterprise for all other clients.
D. Use WPA2-Enterprise with RADIUS and disable pre-shared keys.
Answer: (SHOW ANSWER)

NEW QUESTION: 237
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.
Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
Answer:

NEW QUESTION: 238

Which of the following uses tokens between the identity provider and the service provider to authenticate and authorize users to resources?

A. OAuth

B. RADIUS

C. SSH

D. MSCHAP

Answer: A (LEAVE A REPLY)

NEW QUESTION: 239

A security administrator wants to implement a company-wide policy to empower data owners to manage and enforce access control rules on various resources. Which of the following should be implemented?

A. Discretionary access control

B. Role based access control

C. Rule-based access control

D. Mandatory access control

Answer: A (LEAVE A REPLY)

NEW QUESTION: 240

An organization requires three separate factors for authentication to sensitive systems. Which of the following would BEST satisfy the requirement?

A. Fingerprint. voice recognition, and password

B. One-time password sent to a smartphone thumbprint. and home street address

C. Password, one-time password sent to a smartphone. and text message sent to a smartphone

D. Fingerprint. PIN. and mother's maiden name

Answer: B (LEAVE A REPLY)

NEW QUESTION: 241

After a user reports stow computer performance, a systems administrator detects a suspicious file, which was installed as part of a freeware software package.

The systems administrator reviews the output below:

Based on the above information, which of the following types of malware was installed on the user's computer?

A. Spyware

B. RAT

C. Keylogger

D. Bot

E. Worm

Answer: E (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 242
A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Answer:
Database server was attacked, actions should be to capture network traffic and Chain of Custody.
IDS Server Log:
Web Server Log:
Database Server Log:
Users PC Log:

NEW QUESTION: 243
Which of the following is MOST likely happening?
A. A hacker attempted to pivot using the web server interface.
B. A server is experiencing DoS, and the request Is timing out.
C. A potential hacker could be banner grabbing to determine what architecture is being used
D. The DNS is misconfigured for the server's IP address.
Answer: (SHOW ANSWER)

NEW QUESTION: 244
Joe, a backup administrator, wants to implement a solution that will reduce the restoration time of physical servers. Which of the following is the BEST method for Joe to use?

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

NEW QUESTION: 245
A computer forensics analyst collected a thumb drive that contained a single file with 500 pages of text To ensure the file maintains its confidentiality, which of the following should the analyst use?
A. SLA
B. NOA
C. SHA
D. AES
Answer: D (LEAVE A REPLY)

NEW QUESTION: 246
A technician has installed a new AAA server, which will be used by the network team to control access to a company's routers and switches. The technician completes the configuration by adding the network team members to the NETWORK_TEAM group, and then adding the NETWORK_TEAM group to the appropriate ALLOW_ACCESS access list. Only members of the network team should have access to the company's routers and switches.
Members of the network team successfully test their ability to log on to various network devices configured to use the AAA server. Weeks later, an auditor asks to review the following access log sample:
Which of the following should the auditor recommend based on the above information?
A. Move the NETWORK_TEAM group to the top of the ALLOW_ACCESS access list.
B. Disable groups nesting for the ALLOW_ACCESS group in the AAA server.
C. Remove the DOMAIN_USERS group from ALLOW_ACCESS group.
D. Configure the ALLOW_ACCESS group logic to use AND rather than OR.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 247
A user is unable to obtain an IP address from the corporate DHCP server. Which of the following is MOST likely the cause?
A. Improper input handling
B. Memory overflow
C. Default configuration
D. Resource exhaustion
Answer: D (LEAVE A REPLY)

NEW QUESTION: 248
Which of the following is an example of resource exhaustion?
A. A SQL injection attack returns confidential data back to the browser.
B. Server CPU utilization peaks at 100% during the reboot process
C. System requirements for a new software package recommend having 12GB of RAM, but only 8GB are available.
D. A penetration tester requests every available IP address from a DHCP server.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 249
An auditor wants to test the security posture of an organization by running a tool that will display the following:
Which of the following commands should be used?
A. nbtstat
B. arp
C. nc
D. ipconfig
Answer: (SHOW ANSWER)

NEW QUESTION: 250
After deploying an antivirus solution on some network-isolated industrial computers, the service desk team received a trouble ticket about the following message being displayed on then computer's screen:
Which of the following would be the SAFEST next step to address the issue?
A. Immediately delete the detected file from the quarantine to secure the environment and clear the alert from the antivirus console
B. Centrally activate a full scan for the entire set of industrial computers, looking for new threats
C. Perform a manual antivirus signature update directly from the antivirus vendor's cloud
D. Check the antivirus vendor's documentation about the security modules, incompatibilities, and software whitelisting.
Answer: (SHOW ANSWER)

NEW QUESTION: 251
Which of the following would verify that a threat does exist and security controls can easily be bypassed without actively testing an application?
A. Protocol analyzer
B. Vulnerability scan
C. Penetration test
D. Port scanner
Answer: B (LEAVE A REPLY)

A vulnerability scan is the automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers.
Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.
Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet but can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

NEW QUESTION: 252
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially.
Which of the following would explain the situation?
A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
D. Asymmetric encryption is being used
Answer: D (LEAVE A REPLY)
Explanation/Reference:
Explanation:
Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

NEW QUESTION: 253
A security administrator returning from a short vacation receives an account lock-out message when attempting to log into the computer. After getting the account unlocked the security administrator immediately notices a large amount of emails alerts pertaining to several different user accounts being locked out during the past three days. The security administrator uses system logs to determine that the lock-outs were due to a brute force attack on all accounts that has been previously logged into that machine.
Which of the following can be implemented to reduce the likelihood of this attack going undetected?
A. Account lockout policies
B. Continuous monitoring
C. Password complexity rules

D. User access reviews
Answer: (SHOW ANSWER)

NEW QUESTION: 254
A company help desk has received several reports that employees have experienced identity theft and compromised accounts. This occurred several days after receiving an email asking them to update their personal bank information. Which of the following is a vulnerability that has been exploited?
A. Phishing
B. Forged certificates
C. Improperly configured accounts
D. Untrained users
E. Trojan horses
Answer: D (LEAVE A REPLY)

NEW QUESTION: 255
For each of the given items, select the appropriate authentication category from the drop down choices.
Select the appropriate authentication type for the following items:
Answer:

NEW QUESTION: 256
A coffee company has hired an IT consultant to set up a WiFi network that will provide Internet access to customers who visit the company's chain of cafes. The coffee company has provided no requirements other than that customers should be granted access after registering via a web form and accepting the terms of service. Which of the following is the MINIMUM acceptable configuration to meet this single requirement?
A. Captive portal
B. WPA with PSK
C. Open WiFi
D. WPS
Answer: A (LEAVE A REPLY)
Explanation
A captive portal is a web page accessed with a web browser that is displayed to newly connected users of a Wi-Fi or wired network before they are granted broader access to network resources.

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest**

Actual4test.com SY0-501 dumps with Test Engine here:
https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: **Freepdfdumps**)

NEW QUESTION: 257
A technician suspects that a desktop was compromised with a rootkit. After removing lhe hard drive from the desktop and running an offline file integrity check, the technician reviews the following output:
Based on the above output, which of the following is the malicious file?
A. lsass.exe
B. kernel.dll
C. notepad.exe
D. httpd.axe
Answer: (SHOW ANSWER)

NEW QUESTION: 258
A security engineer needs to obtain a recurring log of changes to system files. The engineer is most concerned with detecting unauthorized changes to system data. Which of the following tools can be used to fulfill the requirements that were established by the engineer?
A. File integrity monitor
B. TPM
C. Trusted operating system
D. UEFI
E. FDE
Answer: (SHOW ANSWER)

NEW QUESTION: 259
An organization wants to upgrade its enterprise-wide desktop computer solution. The organization currently has
500 PCs active on the network. The Chief Information Security Officer (CISO) suggests that the organization employ desktop imaging technology for such a large-scale upgrade. Which of the following is a security benefit of implementing an imaging solution?
A. It reduces the number of vulnerabilities.
B. It allows for faster deployment.
C. It provides a consistent baseline.
D. It decreases the boot time.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 260
A system administrator wants to provide balance between the security of a wireless network and usability.

The administrator is concerned with wireless encryption compatibility of older devices used by some employees. Which of the following would provide strong security and backward compatibility when accessing the wireless network?

A. WEP with a 40-bit key

B. WPA2 using a RADIUS back-end for 802.1x authentication

C. WPA using a preshared key

D. Open wireless network and SSL VPN

Answer: B (LEAVE A REPLY)

NEW QUESTION: 261

A network operations manager has added a second row of server racks in the datacenter. These racks

face the opposite direction of the first row of racks.

Which of the following is the reason the manager installed the racks this way?

A. To maximize fire suppression capabilities

B. To lower energy consumption by sharing power outlets

C. To create environmental hot and cold isles

D. To eliminate the potential for electromagnetic interference

Answer: (SHOW ANSWER)

NEW QUESTION: 262

In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand.

Which of the following characteristics BEST describes what the CIO has requested?

A. Redundancy

B. Elasticity

C. Scalability

D. High availability

Answer: B (LEAVE A REPLY)

NEW QUESTION: 263

An attacker exploited a vulnerability on a mail server using the code below.

Which of the following BEST explains what the attacker is doing?

A. The attacker is replacing a document.

B. The attacker is stealing a document.

C. The attacker is replacing a cookie.

D. The attacker is deleting a cookie.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 264

After being alerted to potential anomalous activity related to trivial DNS lookups, a security analyst looks at the following output of implemented firewall rules:
The analyst notices that the expected policy has no hit count for the day. Which of the following MOST likely occurred?
A. The VLAN is not trunked properly
B. The firewall policy is misconfigured
C. There is a policy violation for DNS lookups
D. Data execution prevention is enabled
Answer: B (LEAVE A REPLY)

NEW QUESTION: 265
An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?
A. The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL
B. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
C. The deny statement for 204.211.38.52/24 should be changed to a permit statement
D. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
Answer: D (LEAVE A REPLY)

NEW QUESTION: 266
While reviewing the monthly internet usage it is noted that there is a large spike in traffic classified as "unknown" and does not appear to be within the bounds of the organizations Acceptable Use Policy.
Which of the following tool or technology would work BEST for obtaining more information on this traffic?
A. Firewall logs
B. Increased spam filtering
C. IDS logs
D. Protocol analyzer
Answer: (SHOW ANSWER)

NEW QUESTION: 267
Which of the following describes the ability of code to target a hypervisor from inside a guest OS?
A. Image forgery
B. Software-defined networking
C. VM escape

D. Container breakout
E. Fog computing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 268
After running an online password cracking tool, an attacker recovers the following password:
gh;jSKSTOi;618&
Based on the above information, which of the following technical controls have been implemented (Select TWO).
A. Complexity
B. Stretching
C. Hashing
D. Salting
E. Encryption
F. Length
Answer: (SHOW ANSWER)

NEW QUESTION: 269
While reviewing system logs, a security analyst notices that a large number of end users are changing their passwords four times on the day the passwords are set to expire. The analyst suspects they are cycling their passwords to circumvent current password controls. Which of the following would provide a technical control to prevent this activity from occurring?
A. Implement password complexity requirements.
B. Create an AUP that prohibits password reuse.
C. Increase the password history from three to five.
D. Set password aging requirements.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 270
DRAG DROP
Drag and drop the correct protocol to its default port.
Answer:
Explanation:
FTP uses TCP port 21.
Telnet uses port 23.
SSH uses TCP port 22. All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP). Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP).
SMTP uses TCP port 25.
Port 69 is used by TFTP.

SNMP makes use of UDP ports 161 and 162.
References:
Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp. 42, 45, 51
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 271
A network administrator wants to gather information on the security of the network servers in the DMZ. The administrator runs the following command:
Which of the following actions is the administrator performing?
A. Harvesting cleartext credentials
B. Logging into the web server
C. Accessing the web server management console
D. Grabbing the web server banner
Answer: D (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 272
A new employee has been hired to perform system administration duties across a large enterprise comprised of multiple separate security domains. Each remote location implements a separate security domain. The new employee has successfully responded to and fixed computer issues for the main office. When the new employee tries to perform work on remote computers, the following messages appears. You need permission to perform this action. Which of the following can be implemented to provide system administrators with the ability to perform administrative tasks on remote computers using their uniquely assigned account?
A. Verify that system administrators are in the domain administrator group in the main office
B. Enable the trusted OS feature across all enterprise computers
C. Install and configure the appropriate CA certificate on all domain controllers
D. Implement transitive trust across security domains
Answer: (SHOW ANSWER)

NEW QUESTION: 273

Which of the following Is a resiliency strategy that allows a system to automatically adapt to workload changes?

A. Elasticity

B. Fault tolerance

C. High availability

D. Redundancy

Answer: A (LEAVE A REPLY)

NEW QUESTION: 274

A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.

Answer:

Explanation

NEW QUESTION: 275

A company has critical systems that are hosted on an end-of-life OS. To maintain operations and mitigate potential vulnerabilities, which of the following BEST accomplishes this objective?

A. Disable the default administrator account.

B. Implement full-disk encryption.

C. Employ patch management.

D. Use application whitelisting.

Answer: D (LEAVE A REPLY)

NEW QUESTION: 276

A technician must configure a firewall to block external DNS traffic from entering a network. Which of the following ports should they block on the firewall?

A. 143

B. 110

C. 443

D. 53

Answer: D (LEAVE A REPLY)

NEW QUESTION: 277

A recent penetration test revealed several issues with a public-facing website used by customers. The Testers were able to:

* Enter long lines of code and special characters
* Crash the system
* Gain unauthorized access to the internal application server
* Map the internal network

The deployment team has stated they will need to rewrite a significant portion of the code used, and it will take more than a year to deliver the finished product. Which of the following would be the BEST solution to introduction in the Interim?

A. WAF

B. Content filtering

C. TLS

D. IPS/IDS

E. UTM

Answer: C (LEAVE A REPLY)

NEW QUESTION: 278

An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?

A. WPA+TWP

B. WPA2+TWP

C. WPA2+CCMP

Answer: B (LEAVE A REPLY)

NEW QUESTION: 279

A government contractor has a security requirement that any service in use must not be accessible by a non-governmental agency. The contractor is trying to reduce costs by moving the on-premises virtual servers to the cloud in a single-tenant environment. Which of the following would BEST meet the requirements?

A. Public laaS

B. Public PaaS

C. Private PaaS

D. Private laaS

E. Private SaaS

F. Public SaaS

Answer: (SHOW ANSWER)

NEW QUESTION: 280

A remote user (User1) is unable to reach a newly provisioned corporate windows workstation. The system administrator has been given the following log files from the VPN, corporate firewall and workstation host.

Which of the following is preventing the remote user from being able to access the workstation?

A. Lack of network time synchronization is causing authentication mismatches

B. User1 has been locked out due to too many failed passwords

C. The workstation has been compromised and is accessing known malware sites
D. The workstation host firewall is not allowing remote desktop connections
E. Network latency is causing remote desktop service request to time out
Answer: B (LEAVE A REPLY)

NEW QUESTION: 281
A security analyst has been asked to perform a review of an organization's software development lifecycle.
The analyst reports that the lifecycle does not contain a phase in which team members evaluate and
provide critical feedback of another developer's code.
Which of the following assessment techniques is BEST described in the analyst's report?
A. Whitebox testing
B. Architecture evaluation
C. Baseline reporting
D. Peer review
Answer: (SHOW ANSWER)

NEW QUESTION: 282
An incident responder receives a call from a user who reports a computer is exhibiting symptoms consistent with a malware infection. Which of the following steps should the responder perform NEXT?
A. Request the user capture and provide a screenshot or recording of the symptoms
B. Capture and document necessary information to assist m the response
C. Ask the user to back up files for later recovery
D. Use a remote desktop client to collect and analyze the malware m real time
Answer: C (LEAVE A REPLY)

NEW QUESTION: 283
A Security analyst is diagnosing an incident in which a system was compromised from an external IP address. The socket identified on the firewall was traced to 207.46.130.6666. Which of the following should the security analyst do to determine if the compromised system still has an active connection?
A. netstat
B. Ping
C. tracert
D. nslookup
Answer: (SHOW ANSWER)

NEW QUESTION: 284

Two users need to send each other emails over unsecured channels. The system should support the principle of non-repudiation. Winch of the following should be used to sign the users' certificates?

A. CA

B. CRL

C. CSR

Answer: C (LEAVE A REPLY)

NEW QUESTION: 285

A Security analyst has received an alert about PII being sent via email. The analyst's Chief Information Security Officer (CISO) has made it clear that PII must be handled with extreme care. From which of the following did the alert MOST likely originate?

A. S/MIME

B. DLP

C. IMAP

D. HIDS

Answer: (SHOW ANSWER)

Explanation

An intrusion detection system is a device or software application that monitors a network or systems for malicious activity or policy violations. Any intrusion activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

NEW QUESTION: 286

A security administrator is implementing a new WAF solution and has placed some of the web servers behind the WAF, with the WAF set to audit mode. When reviewing the audit logs of external requests and posts to the web servers, the administrator finds the following entry:

Based on this data, which of the following actions should the administrator take?

A. Alert the web server administrators to a misconfiguration

B. Create a blocking policy based on the parameter values

C. Create an alert to generate emails for abnormally high activity.

D. Change the parameter name 'Account_Name' identified in the log.

Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here:

https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 287
An employee workstation with an IP address of 204.211.38.211/24 reports it is unable to submit print jobs to a network printer at 204.211.38.52/24 after a firewall upgrade. The active firewall rules are as follows:
Assuming port numbers have not been changed from their defaults, which of the following should be modified to allow printing to the network printer?
A. The permit statement for 204.211.38.52/24 should be changed to TCP port 631 instead of UDP
B. The permit statement for 204.211.38.52/24 should be changed to UDP port 443 instead of 631
C. The deny statement for 204.211.38.52/24 should be changed to a permit statement
D. The permit statement for 204.211.38.211/24 should be changed to TCP port 631 only instead of ALL
Answer: A (LEAVE A REPLY)

NEW QUESTION: 288
A company has migrated to two-factor authentication for accessing the corporate network, VPN, and SSO.
Several legacy applications cannot support multifactor authentication and must continue to use usernames and passwords. Which of the following should be implemented to ensure the legacy applications are as secure as possible while ensuring functionality? (Choose two.)
A. Account disablement
B. Password recovery
C. Password complexity requirements
D. Priveleged accounts
E. Password reuse restrictions
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 289
A systems administrator recently issued a public/private key pair that will be used for the company's DNSSEC implementation Which of the following configurations should the systems administrator implement NEXT?
A. Create DNSKEY resources with the public key.
B. Add TCP port 443 to the DNS listener
C. instant private key using the RRSIG record
D. Point the OS record to the company authoritative servers
Answer: A (LEAVE A REPLY)

NEW QUESTION: 290

A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center.
Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation

NEW QUESTION: 291
During a risk assessment, results show that a fire in one of the company's datacenters could cost up to S20 million in equipment damages and lost revenue. As a result, the company insures the datacenter for up to S20 million in damages for the cost of 530,000 a year. Which of the following risk response techniques has the company chosen?
A. Acceptance
B. Mitigation
C. Transference
D. Avoidance
Answer: (SHOW ANSWER)

NEW QUESTION: 292
For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases.
Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 293
A company has a data system with definitions for "Private" and "Public". The company's security policy outlines how data should be protected based on type. The company recently added the data type "Proprietary". Which of the following is the MOST likely reason the company added this data type?
A. Expanded authority of the privacy officer
B. More searchable data

C. Reduced cost
D. Better data classification
Answer: B (LEAVE A REPLY)

NEW QUESTION: 294
Which of the following policies would help an organization identify and mitigate potential single points of failure in the company's IT/security operations?
A. Separation of duties
B. Least privilege
C. Mandatory vacation
D. Awareness training
Answer: A (LEAVE A REPLY)

NEW QUESTION: 295
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artifacts.

NEW QUESTION: 296
A network administrator was to implement a solution that will allow authorized traffic, deny unauthorized traffic and ensure that appropriate ports are being used for a number of TCP and UDP protocols. Which of the following network controls would meet these requirements?
A. Stateful firewall
B. proxy server
C. Web security gateway
D. URL filter
E. web application firewall
Answer: (SHOW ANSWER)

NEW QUESTION: 297
A wireless network has the following design requirements:
* Authentication must not be dependent on enterprise directory service
* It must allow background reconnection for mobile users

* It must not depend on user certificates
Which of the following should be used in the design to meet the requirements? (Choose two.)
A. EAP-TLS
B. Open systems authentication
C. PEAP
D. PSK
E. Captive portals
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 298
Which of the following is the purpose of an industry-standard framework?
A. To promulgate compliance requirements for sales of common IT systems
B. To provide legal relief to participating organizations in the event of a security breach
C. To promulgate security settings on a vendor-by-vendor basis
D. To provide guidance across common system implementations
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 299
For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases.
Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 300
A security analyst wants to limit the use of USB and external drives to protect against malware. as well as protect les leaving a user's computer. Which of the following is the BEST method to use?
A. Firewall
B. Data loss prevention
C. Antivirus software
D. Router
Answer: (SHOW ANSWER)

NEW QUESTION: 301
Having adequate lighting on the outside of a building is an example of which of the following security controls?
A. Deterrent
B. Compensating
C. Detective
D. Preventative
Answer: A (LEAVE A REPLY)
Explanation/Reference:

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 302
A dumpster diver was able 10 retrieve hard drives from a competitor's trash bin. After installing the and hard drives and running common date recovery software. Sensitive information was recovered. In which of the following ways did the competitor apply media sanitation?
A. Encrypting
B. Formatting
C. Pulverizing
D. Degaussing
Answer: (SHOW ANSWER)

NEW QUESTION: 303
A security analyst is reviewing an assessment report that includes software versions, running services, supported encryption algorithms, and permission settings. Which of the following produced the report?
A. Protocol analyzer
B. Vulnerability scanner
C. Network mapper
D. Web inspector
Answer: (SHOW ANSWER)

NEW QUESTION: 304

An in-house penetration tester is using a packet capture device to listen in on network communications.
This is an example of:
A. Exploiting the switch
B. Persistence
C. Passive reconnaissance
D. Escalation of privileges
Answer: (SHOW ANSWER)

NEW QUESTION: 305
A user is presented with the following items during the new-hire onboarding process:
-Laptop
-Secure USB drive
-Hardware OTP token
-External high-capacity HDD
-Password complexity policy
-Acceptable use policy
-HASP key
-Cable lock
Which of the following is one component of multifactor authentication?
A. Secure USB drive
B. Cable lock
C. Hardware OTP token
D. HASP key
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 306
A security program manager wants to actively test the security posture of a system.
The system is not yet in production and has no uptime requirement or active user base.
Which of the following methods will produce a report which shows vulnerabilities that were actually exploited?
A. Peer review
B. Component testing
C. Penetration testing
D. Vulnerability testing
Answer: (SHOW ANSWER)
A penetration test, or pen test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities.

NEW QUESTION: 307

An organization's Chief Executive Officer (CEO) directs a newly hired computer technician to install an OS on the CEO's: personal laptop. The technician performs the installation, and a software audit later in the month indicates a violation of the EULA occurred as a result. Which of the following would address this violation going forward?
A. AUP
B. Security conguration baseline
C. Separation of duties
D. NDA
Answer: A (LEAVE A REPLY)

NEW QUESTION: 308
A security administrator found the following piece of code referenced on a domain controller's task scheduler:
$var = GetDomainAdmins
If $var != 'fabio'
SetDomainAdmins = NULL
With which of the following types of malware is the code associated?
A. Logic bomb
B. RAT
C. Crypto-malware
D. Backdoor
Answer: (SHOW ANSWER)

NEW QUESTION: 309
A business sector is highly competitive, and safeguarding trade secrets and critical information is paramount.
On a seasonal basis, an organization employs temporary hires and contractor personnel to accomplish its mission objectives. The temporary and contract personnel require access to network resources only when on the clock.
Which of the following account management practices are the BEST ways to manage these accounts?
A. Employ a random key generator strategy.
B. Employ a password lockout policy
C. Employ password complexity.
D. Employ an account expiration strategy.
E. Employ time-of-day restrictions.
Answer: E (LEAVE A REPLY)

NEW QUESTION: 310
Which of the following development models entails several iterative and incremental software development methodologies such as Scrum?

A. Spiral
B. Rapid
C. Agile
D. Waterfall
Answer: C (LEAVE A REPLY)

NEW QUESTION: 311
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

NEW QUESTION: 312
A security analyst is attempting to identify vulnerabilities in a customer's web application without impacting the system or its data. Which of the following BEST describes the vulnerability scanning concept performed?
A. Aggressive scan
B. Passive scan
C. Non-credentialed scan
D. Compliance scan
Answer: B (LEAVE A REPLY)
Explanation
Passive scanning is a method of vulnerability detection that relies on information gleaned from network data that is captured from a target computer without direct interaction.
Packet sniffing applications can be used for passive scanning to reveal information such as operating system, known protocols running on non-standard ports and active network applications with known bugs. Passive scanning may be conducted by a network administrator scanning for security vulnerabilities or by an intruder as a preliminary to an active attack.
For an intruder, passive scanning's main advantage is that it does not leave a trail that could alert users or administrators to their activities. For an administrator, the main advantage is that it doesn't risk causing undesired behavior on the target computer, such as freezes. Because of these advantages, passive scanning need not be limited to a narrow time frame to minimize risk or disruption, which means that it is likely to return more information.

Passive scanning does have limitations. It is not as complete in detail as active vulnerability scanning and cannot detect any applications that are not currently sending out traffic; nor can it distinguish false information put out for obfuscation.

NEW QUESTION: 313
After segmenting the network, the network manager wants to control the traffic between the segments. Which of the following should the manager use to control the network traffic?
A. An ACL
B. A VLAN
C. A VPN
D. A DMZ
Answer: (SHOW ANSWER)

NEW QUESTION: 314
In determining when it may be necessary to perform a credentialed scan against a system instead of a
non-credentialed scan, which of the following requirements is MOST likely to influence this decision?
A. The scanner must be able to audit file system permissions
B. The scanner must be able to enumerate the host OS of devices scanned.
C. The scanner must be able to check for open ports with listening services.
D. The scanner must be able to footprint the network.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 315
A technician has installed new vulnerability scanner software on a server that is joined to the company domain. The vulnerability scanner is able to provide visibility over the patch posture of all company's clients. Which of the following is being used?
A. Bypassing security controls
B. Passive scan
C. Gray box vulnerability testing
D. Credentialed scan
Answer: (SHOW ANSWER)

NEW QUESTION: 316
A pass-the-hash attack is commonly used to:
A. modify the IP address of the targeted computer.
B. modify DNS records to point to a different domain.
C. laterally move across the network.
D. execute java script to capture user credentials.
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 317
A company that processes sensitive information has implemented a BYOD policy and an MDM solution to secure sensitive data that is processed by corporate and personally owned mobile devices. Which of the following should the company implement to prevent sensitive data from being stored on mobile devices?
A. VDI
B. Storage segmentation
C. Containerization
D. USB OTG
E. Geofencing
Answer: B (LEAVE A REPLY)
Storage segmentation: Storage segmentation offers a special feature whereby the user can artificially categorize different types of data on a mobile device's storage media. By default, a device uses storage segmentation to divide the device's preinstalled apps and operating system from the user data and user-installed apps.

NEW QUESTION: 318
A developer is building a new web portal for internal use. The web portal will only the accessed by internal users and will store operational documents. Which of the following certificate types should the developer install if the company is MOST interested in minimizing costs?
A. Root
B. Code signing
C. Wildcard
D. Self-signed
Answer: (SHOW ANSWER)

NEW QUESTION: 319
A security administrator is given the security and availability profiles for servers that are being deployed.
* Match each RAID type with the correct configuration and MINIMUM number of drives.

* Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:
* All drive definitions can be dragged as many times as necessary
* Not all placeholders may be filled in the RAID configuration boxes
* If parity is required, please select the appropriate number of parity checkboxes
* Server profiles may be dragged only once
If at any time you would like to bring back the initial state of the simulation, please select the Reset button.
When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

Explanation
RAID-0 is known as striping. It is not a fault tolerant solution but does improve disk performance for read/write operations. Striping requires a minimum of two disks and does not use parity. RAID-0 can be used where performance is required over fault tolerance, such as a media streaming server.
RAID-1 is known as mirroring because the same data is written to two disks so that the two disks have identical data. This is a fault tolerant solution that halves the storage space. A minimum of two disks are used in mirroring and does not use parity. RAID-1 can be used where fault tolerance is required over performance, such as on an authentication server. RAID-5 is a fault tolerant solution that uses parity and striping. A minimum of three disks are required for RAID-5 with one disk's worth of space being used for parity information. However, the parity information is distributed across all the disks. RAID-5 can recover from a sing disk failure.
RAID-6 is a fault tolerant solution that uses dual parity and striping. A minimum of four disks are required for RAID-6. Dual parity allows RAID-6 to recover from the simultaneous failure of up to two disks. Critical data should be stored on a RAID-6 system.
http://www.adaptec.com/en-us/solutions/raid_levels.html

NEW QUESTION: 320
A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

Answer:

NEW QUESTION: 321
A company wants to host a publicity available server that performs the following functions:
Which of the following should the company use to fulfill the above requirements?

A. dig
B. LDAPS
C. SFTP
D. DNSSEC

E. nslookup
Answer: (SHOW ANSWER)

NEW QUESTION: 322
Which of the following penetration testing concepts is being used when an attacker uses public Internet databases to enumerate and learn more about a target?
A. Pivoting
B. Vulnerability scanning
C. White box testing
D. Reconnaissance
E. Initial exploitation
Answer: (SHOW ANSWER)

NEW QUESTION: 323
A security analyst needs to be proactive in understanding the types of attacks that could potentially target the company's executives. Which of the following intelligence sources should the security analyst review?
A. Structured threat information expression
B. Vulnerability feeds
C. Industry information-sharing and collaboration groups
D. Trusted automated exchange of indicator information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 324
An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?
A. Processes in running memory
B. Swap space
C. Processor cache
D. Application files on hard disk
Answer: (SHOW ANSWER)

NEW QUESTION: 325
A company recently updated its website to increase sales. The new website uses PHP forms for leads and provides a directory with sales staff and their phone numbers. A systems administrator is concerned about the new website and provides the following log to support the concern:
Which of the following is the systems administrator MOST likely to suggest to the Chief Information Security Officer (CISO) based on the above?
A. Increasing the minimum password length from eight to ten characters
B. Changing the account standard naming convention

C. Implementing account lockouts
D. Discontinuing the use of privileged accounts
Answer: B (LEAVE A REPLY)

NEW QUESTION: 326
A security administrator is reviewing the following firewall configuration after receiving reports that users are unable to connect to remote websites:
Which of the following is the MOST secure solution the security administrator can implement to fix this issue?
A. Add the following rule to the firewall: 5 PERMIT FROM:ANY TO:ANY PORT:53
B. Replace rule number 10 with the following rule: 10 PERMIT FROM:ANY TO:ANY PORT:22
C. Remove the following rule from the firewall: 30 DENY FROM:ANY TO:ANY PORT:ANY
D. Insert the following rule in the firewall: 25 PERMIT FROM:ANY TO:ANY PORTS:ANY
Answer: B (LEAVE A REPLY)

NEW QUESTION: 327
A database backup schedule consists of weekly full backups performed on Saturday at
1 2:00 a.m. and daily differential backups also performed at 12:00 a.m. If the database is restored on Tuesday afternoon, which of the following is the number of individual backups that would need to be applied to complete the database recovery?
A. 3
B. 1
C. 4
D. 2
Answer: D (LEAVE A REPLY)

NEW QUESTION: 328
A technician has installed new vulnerability scanner software on a server that is joined to the company domain.
The vulnerability scanner is able to provide visibility over the patch posture of all company's clients.
Which of the following is being used?
A. Gray box vulnerability testing
B. Passive scan
C. Credentialed scan
D. Bypassing security controls
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 329

A company just implemented a new telework policy that allows employees to use personal devices for official email and file sharing while working from home. Some of the requirements are:
* Employees must provide an alternate work location (i.e., a home address).
* Employees must install software on the device that will prevent the loss of proprietary data but will not restrict any other software from being installed.
Which of the following BEST describes the MDM options the company is using?
A. Geofencing, content management, remote wipe, containerization, and storage segmentation
B. Content management, remote wipe, geolocation, context-aware authentication, and containerization
C. Application management, remote wipe, geofencing, context-aware authentication, and containerization
D. Remote wipe, geolocation, screen locks, storage segmentation, and full-device encryption
Answer: C (LEAVE A REPLY)
Explanation

NEW QUESTION: 330
A systems administrator has implemented multiple websites using host headers on the same server. The server hosts two websites that require encryption and other websites where encryption is optional. Which of the following should the administrator implement to encrypt web traffic for the required websites?
A. Wildcard certificate
B. OCSP stapling
C. TLS host certificate
D. Extended domain validation
Answer: C (LEAVE A REPLY)

NEW QUESTION: 331
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.
3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References:
http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 332
An incident involving a workstation that is potentially infected with a virus has occurred. The workstation may have sent confidential data to an unknown internet server.
Which of the following should a security analyst do FIRST?
A. Run a virus scan.
B. Make a copy of everything in memory on the workstation.

C. Consult information security policy.
D. Turn off the workstation.
Answer: (SHOW ANSWER)

NEW QUESTION: 333
A Chief Information Officer (CIO) recently saw on the news that a significant security flaws exists with a specific version of a technology the company uses to support many critical application. The CIO wants to know if this reported vulnerability exists in the organization and, if so, to what extent the company could be harmed. Which of the following would BEST provide the needed information?
A. Patching assessment report
B. Penetration test
C. Active reconnaissance
D. Vulnerability scan
Answer: B (LEAVE A REPLY)

NEW QUESTION: 334
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion. Which of the following technologies would BEST be suited to accomplish this?
A. Transport Encryption
B. Stream Encryption
C. Digital Signature
D. Steganography
Answer: D (LEAVE A REPLY)
Explanation
Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

NEW QUESTION: 335
Virtualization that allows an operating system kernel to run multiple isolated instances of the guest is called:
A. Process segregation
B. Containers
C. Software defined network
D. Sandboxing
Answer: B (LEAVE A REPLY)

NEW QUESTION: 336

The Chief Technology Officer (CTO) of a company, Ann, is putting together a hardware budget for the next
10 years. She is asking for the average lifespan of each hardware device so that she is able to calculate when she will have to replace each device.
Which of the following categories BEST describes what she is looking for?
A. MTTF
B. MTTR
C. MTBF
D. ALE
Answer: A (LEAVE A REPLY)

NEW QUESTION: 337
A state-sponsored threat actor has launched several successful attacks against a corporate network. Although the target has a robust patch management program in place, the attacks continue in depth and scope, and the security department has no idea how the attacks are able to gain access. Given that patch management and vulnerability scanners are being used, which of the following would be used to analyze the attack methodology?
A. Penetration test
B. Next-generation firewall
C. Honeypots
D. Rogue system detection
Answer: C (LEAVE A REPLY)

NEW QUESTION: 338
DRAG DROP
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:

NEW QUESTION: 339
An organization is updating its access control standards for SSL VPN login to include multifactor authentication The security administrator assigned to this project has been given the following guidelines to use when selecting a solution
* High security
* Lowest false acceptance rate
* Quick provisioning time for remote users and offshore consultants
Which of the following solutions will BEST fit this organization's requirements?
A. Iris scanners
B. Software tokens

C. AES-256 key fobs
D. Fingerprint scanners
Answer: B (LEAVE A REPLY)

NEW QUESTION: 340
During a lessons learned meeting regarding a previous incident, the security team receives a follow-up action item with the following requirements:
* Allow authentication from within the United States anytime
* Allow authentication if the user is accessing email or a shared file system
* Do not allow authentication if the AV program is two days out of date
* Do not allow authentication if the location of the device is in two specific countries
Given the requirements, which of the following mobile deployment authentication types is being utilized?
A. Two-factor authentication
B. Context-aware authentication
C. Biometric authentication
D. Geofencing authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 341
Ann is the IS manager for several new systems in which the classifications of the systems' data are being decided. She is trying to determine the sensitivity level of the data being processed.
Which of the following people should she consult to determine the data classification?
A. Owner
B. Custodian
C. User
D. Steward
Answer: A (LEAVE A REPLY)

NEW QUESTION: 342
A systems administrator wants to provide for and enforce wireless access accountability during events where external speakers are invited to make presentations to a mixed audience of employees and non-employees.
Which of the following should the administrator implement?
A. Shared accounts
B. Least privilege
C. Sponsored guest
D. Preshared passwords
Answer: C (LEAVE A REPLY)

NEW QUESTION: 343

An email recipient is unable to open a message encrypted through PKI that was sent from another organization.
Which of the following does the recipient need to decrypt the message?
A. The CA's root certificate
B. The recipient's private key
C. The sender's public key
D. An updated CRL
E. The recipient's public key
F. The sender's private key
Answer: C (LEAVE A REPLY)

NEW QUESTION: 344
A security analyst is reviewing the following packet capture of an attack directed at a company's server located in the DMZ:
Which of the following ACLs provides the BEST protection against the above attack and any further attacks from the same IP, while minimizing service interruption?
A. DENY TCO From ANY to 172.31.64.4
B. Deny TCP from 192.168.1.10 to 172.31.67.4
C. Deny UDP from 192.168.1.0/24 to 172.31.67.0/24
D. Deny IP from 192.168.1.10/32 to 0.0.0.0/0
Answer: B (LEAVE A REPLY)

NEW QUESTION: 345
When trying to log onto a company's new ticketing system, some employees receive the following message: Access denied: too many concurrent sessions. The ticketing system was recently installed on a small VM with only the recommended hardware specifications.
Which of the following is the MOST likely cause for this error message?
A. The firewall is misconfigured.
B. The software is out of licenses.
C. Network resources have been exceeded.
D. The VM does not have enough processing power.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 346
When viewing IPS logs the administrator see systems all over the world scanning the network for servers with port 22 open. The administrator concludes that this traffic is a(N):
A. Threat
B. Risk
C. Vulnerability
D. Exploit
Answer: A (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 347
A security analyst is hardening a server with the directory services role installed. The analyst must ensure
LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the
following should the analyst implement to meet these requirements? (Select two.)
A. Ensure port 389 is open between the clients and the servers using the communication.
B. Generate an X.509-compliant certificate that is signed by a trusted CA.
C. Install and configure an SSH tunnel on the LDAP server.
D. Ensure port 636 is open between the clients and the servers using the communication.
E. Remote the LDAP directory service role from the server.
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 348
A software development company needs to augment staff by hiring consultants for a high-stakes project The project has the following requirements:
* Consultants will have access to flighty confidential, proprietary data.
* Consultants will not be provided with company-owned assets.
* Work needs to start Immediately.
* Consultants will be provided with Internal email addresses for communications.
Which of the following solutions is the BEST method lor controlling data exfiltration during this project?
A. Require the consultants to conned to the company VPN when accessing confidential resources.
B. Require updated antivirus. USB blocking, and a host-based firewall on all consultant devices.
C. Require that all consultant activity be restricted to a secure VDI environment.
D. Require the consultants to sign an agreement stating they will only use the company-provided email address for communications during the project.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 349

An employee opens a web browser and types a URL into the address bar. Instead of reaching the requested site, the browser opens a completely different site. Which of the following types of attacks have MOST likely occurred? (Choose two.)

A. Cross-site scripting

B. Session hijacking

C. Man-in-the-browser

D. Domain hijacking

E. DNS hijacking

Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 350

During incident response procedures, technicians capture a unique identifier for a piece of malware running in memory. This captured information is referred to as

A. the SSID.

B. a system image.

C. a hash value.

D. the GUID.

Answer: (SHOW ANSWER)

NEW QUESTION: 351

The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9. and the destination IP is 10.17.36.5. The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:

Which of the following should the security analyst request NEXT based on the UTM firewall analysis?

A. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.

B. Request the application team to reconfigure the application and allow RPC communication.

C. Request the application team to allow TCP port 87 to listen on 10.17.36.5.

D. Request the network team to turn of IPS for 10.13.136.8 going to 10.17.36.5.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 352

Joe, a user, has been trying to send Ann, a different user, an encrypted document via email. Ann has not received the attachment but is able to receive the header information.

Which of the following is MOST likely preventing Ann from receiving the encrypted file?

A. Permission issues

B. Unencrypted credentials

C. Weak cipher suite

D. Authentication issues

Answer: D (LEAVE A REPLY)

NEW QUESTION: 353
A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.
INSTRUCTIONS
Click on each firewall to do the following:
1. Deny cleartext web traffic
2. Ensure secure management protocols are used.
3. Resolve issues at the DR site.
The ruleset order cannot be modified due to outside constraints.
Hat any time you would like to bring back the initial state of the simulation, please dick the Reset All button.

Answer:
Check the answer in explanation.
Explanation
In Firewall 1, HTTP inbound Action should be DENY. As shown below
In Firewall 2, Management Service should be DNS, As shown below.
In Firewall 3, HTTP Inbound Action should be DENY, as shown below

NEW QUESTION: 354
You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.
The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.
Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:

See the solution below.
Explanation
Solution as

NEW QUESTION: 355
Joe is exchanging encrypted email with another party. Joe encrypts the initial email with a key. When Joe receives a response, he is unable to decrypt the response with the same key he used initially. Which of the following would explain the situation?
A. An ephemeral key was used for one of the messages
B. A stream cipher was used for the initial email; a block cipher was used for the reply
C. Out-of-band key exchange has taken place
D. Asymmetric encryption is being used
Answer: D (LEAVE A REPLY)
Asymmetric algorithms use two keys to encrypt and decrypt data. These asymmetric keys are referred to as the public key and the private key. The sender uses the public key to encrypt a message, and the receiver uses the private key to decrypt the message; what one key does, the other one undoes.

NEW QUESTION: 356
A company is evaluating cloud providers to reduce the cost of its internal IT operations. The company's aging systems are unable to keep up with customer demand. Which of the following cloud models will the company MOST likely select?
A. PaaS
B. SaaS
C. IaaS
D. BaaS
Answer: C (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 357
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.
Which of the following is being described?
A. Service level agreement
B. Memorandum of understanding
C. Business partner agreement
D. Interoperability agreement
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 358
An administrator has configured a new Linux server with the FTP service. Upon verifying that the service was configured correctly, the administrator has several users test the FTP service. Users report that they are able to connect to the FTP service and download their personal files, however, they cannot transfer new files to the
server. Which of the following will most likely fix the uploading issue for the users?
A. Reconfigure the ftp daemon to operate without utilizing the PSAV mode
B. Configure the FTP daemon to utilize PAM authentication pass through user permissions
C. Create an ACL to allow the FTP service write access to user directories
D. Set the Boolean selinux value to allow FTP home directory uploads
Answer: C (LEAVE A REPLY)

NEW QUESTION: 359
A security administrator discovers that an attack has been completed against a node on the corporate network. All available logs were collected and stored.
You must review all network logs to discover the scope of the attack, check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. The environment is a critical production environment; perform the LEAST disruptive actions on the network, while still performing the appropriate incid3nt responses.
Instructions: The web server, database server, IDS, and User PC are clickable. Check the box of the node(s) that have been compromised and drag and drop the appropriate actions to complete the incident response on the network. Not all actions may be used, and order is not important. If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
A. Database server was attacked, actions should be to capture network traffic and Chain of Custody.
IDS Server Log:
Web Server Log:
Database Server Log:
Users PC Log:
B. Database server was attacked, actions should be to capture network traffic and Chain of Custody.
IDS Server Log:
Web Server Log:
Database Server Log:
Users PC Log:
Answer: (SHOW ANSWER)

NEW QUESTION: 360
The Chief Security Officer (CSO) for an online retailer received a report from a penetration test that was performed against the company's servers. After reviewing the report, the CSO decided not to implement the recommended changes due to cost; instead, the CSO increased insurance coverage for data breaches. Which of the following describes how the CSO managed the risk?
A. Acceptance
B. Transference
C. Avoidance
D. Ignorance
Answer: B (LEAVE A REPLY)

NEW QUESTION: 361
A consumer purchases an exploit from the dark web. The exploit targets the online shopping cart of a popular website, allowing the shopper to modify the price of an item as checkout. Which of the following BEST describes this type of user?
A. Script kiddie
B. APT
C. Insider
D. Competitor
E. Hacktivist
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 362
Refer to the following code:
Which of the following vulnerabilities would occur if this is executed?
A. Page exception
B. Pointer dereference
C. NullPointerException
D. Missing null check
Answer: D (LEAVE A REPLY)

NEW QUESTION: 363

A bank is experiencing a DoS attack against an application designed to handle 500 IP-based sessions.
in addition, the perimeter router can only handle 1Gbps of traffic.
Which of the following should be implemented to prevent a DoS attacks in the future?
A. Use redundancy across all network devices and services
B. Increase the capacity of the perimeter router to 10 Gbps
C. Deploy multiple web servers and implement a load balancer
D. Install a firewall at the network to prevent all attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 364
An authorized user is conducting a penetration scan of a system for an organization. The tester has a set of network diagrams. Source code, version numbers of applications. and other information about the system. Including hostnames and network addresses. Which of the following BEST describes this type of penetration test?
A. Black-boxtestlng
B. Blue team exercise
C. White-box testing
D. Red team exercise
E. Gray-box testing
Answer: C (LEAVE A REPLY)

NEW QUESTION: 365
Which of the following systems, if compromised may cause a denial of service to the use of a smart TV?
A. SCADA
B. UAV
C. IoT
D. HVAC
Answer: C (LEAVE A REPLY)

NEW QUESTION: 366
An organization uses multifactor authentication to restrict local network access. It requires a PIV and a PIN.
Which of the following factors is the organization using?
A. Something you have, something you know
B. Something you do, something you are
C. Something you know, something you do
D. Something you have; something you are
Answer: A (LEAVE A REPLY)

NEW QUESTION: 367
A security analyst is hardening a server with the directory services role installed. The analyst must ensure LDAP traffic cannot be monitored or sniffed and maintains compatibility with LDAP clients. Which of the following should the analyst implement to meet these requirements? (Select two.)
A. Remote the LDAP directory service role from the server.
B. Generate an X.509-compliant certificate that is signed by a trusted CA.
C. Ensure port 389 is open between the clients and the servers using the communication.
D. Install and configure an SSH tunnel on the LDAP server.
E. Ensure port 636 is open between the clients and the servers using the communication.
Answer: D,E (LEAVE A REPLY)

NEW QUESTION: 368
A company recently experienced data exfiltration via the corporate network. In response to the breach, a security analyst recommends deploying an out-of-band IDS solution. The analyst says the solution can be implemented without purchasing any additional network hardware. Which of the following solutions will be used to deploy the IDS?
A. Network tap
B. Network proxy
C. Port mirroring
D. Honeypot
Answer: (SHOW ANSWER)

NEW QUESTION: 369
Despite having implemented password policies, users continue to set the same weak passwords and reuse old passwords.
Which of the following technical controls would help prevent these policy violations? (Select two.)
A. Password complexity
B. Password history
C. Password lockout
D. Password expiration
E. Password length
Answer: A,B (LEAVE A REPLY)

NEW QUESTION: 370
A user receives an email from ISP indicating malicious traffic coming from the user's home network is detected.
The traffic appears to be Linux-based, and it is targeting a website that was recently featured on the news as being taken offline by an Internet attack. The only Linux device on the network is a home surveillance camera system.
Which of the following BEST describes what is happening?

A. The camera system is infected with a bot.
B. The camera system is infected with a Trojan.
C. The camera system is infected with a RAT.
D. The camera system is infected with a backdoor.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 371
An organization uses SSO authentication for employee access to network resources. When an employee
resigns, as per the organization's security policy, the employee's access to all network resources is
terminated immediately. Two weeks later, the former employee sends an email to the help desk for a
password reset to access payroll information from the human resources server. Which of the following
represents the BEST course of action?
A. Approve the former employee's request, as there would not be a security issue with the former employee gaining access to network resources.
B. Deny the former employee's request, as a password reset would give the employee access to all
network resources.
C. Deny the former employee's request, since the password reset request came from an external email
address.
D. Approve the former employee's request, as a password reset would give the former employee access
to only the human resources server.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 372
A new network administrator is establishing network circuit monitoring guidelines to catch potentially malicious traffic. The administrator begins monitoring the NetFlow statistics tor the critical Internet circuit and notes the following data after two weeks.
However, after checking the statistics from the weekend following the compiled statistics the administrator notices a spike in traffic to 250Mbps sustained for one hour The administrator is able to track the source of the spike to a server in the DMZ Which of the following is the next BEST course of action the administrator should take?
A. Immediately open a Seventy 1 case with the security analysts to address potential data exfiltration
B. Enable a packet capture on the firewall to catch the raw packets on the next occurrence
C. Consult the NetFlow logs on the NetFlow server to determine what data was being transferred

D. Rerun the baseline data gathering for an additional four weeks and compare the results
Answer: B (LEAVE A REPLY)

NEW QUESTION: 373
Task: Determine the types of attacks below by selecting an option from the dropdown list.
Answer:
Explanation
A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS) E: Social engineering is a non-technical method of intrusion hackers use that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security.
Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.

http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 374
A developer is building a new web portal for internal use. The web portal will only the accessed by internal users and will store operational documents. Which of the following certicate types should the developer install if the company is MOST interested in minimizing costs?
A. Root
B. Code signing
C. Self-signed
D. Wildcard
Answer: (SHOW ANSWER)

NEW QUESTION: 375
You have just received some room and WiFi access control recommendations from a security consulting company. Click on each building to bring up available security controls. Please implement the following requirements:
The Chief Executive Officer's (CEO) office had multiple redundant security measures installed on the door to the office. Remove unnecessary redundancies to deploy three-factor authentication, while retaining the expensive iris render.
The Public Cafe has wireless available to customers. You need to secure the WAP with WPA and place a passphrase on the customer receipts.
In the Data Center you need to include authentication from the "something you know" category and take advantage of the existing smartcard reader on the door.
In the Help Desk Office, you need to require single factor authentication through the use of physical tokens given to guests by the receptionist.
The PII Office has redundant security measures in place. You need to eliminate the redundancy while maintaining three-factor authentication and retaining the more expensive controls.
Instructions: The original security controls for each office can be reset at any time by selecting the Reset button. Once you have met the above requirements for each office, select the Save button. When you have completed the entire simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.

Answer:
See the solution below.
Explanation
Solution as

NEW QUESTION: 376

A security analyst is reviewing the password policy for a service account that is used for a critical network service. The password policy for this account is as follows:
Which of the following adjustments would be the MOST appropriate for the service account?
A. Disable account lockouts
B. Increase password length to 18 characters
C. Set the maximum password age to 15 days
D. Set the minimum password age to seven days
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 377
Penetration testing is distinct from vulnerability scanning primarily because penetration testing:
A. involve multiple active exploitation technique
B. relies on misconfiguration of security controls.
C. relies exclusively on passive exploitation attempts for pivoting
D. leverages credentials scanning to obtain persistence.
Answer: (SHOW ANSWER)

NEW QUESTION: 378
A forensic investigator has run into difficulty recovering usable files from a SAN drive. Which of the
following SAN features might have caused the problem?
A. Storage multipaths
B. Data snapshots
C. iSCSI initiator encryption
D. Deduplication
Answer: (SHOW ANSWER)

NEW QUESTION: 379
A security administrator is Implementing a secure method that allows developers to place files or objects onto a Linux server Developers ate required to log In using a username. password, and asymmetric key. Which of the following protocols should be implemented?
A. SSL/TLS

B. SFTP
C. SRTP
D. IPSec
Answer: B (LEAVE A REPLY)

NEW QUESTION: 380
A company is deploying a file-sharing protocol access a network and needs to select a protocol for authenticating clients. Management requests that the service be configured in the most secure way possible. The protocol must also be capable of mutual authentication, and support SSO and smart card logons. Which of the following would BEST accomplish this task?
A. Implement Kerberos
B. Store credentials in LDAP
C. Use NTLM authentication
D. Use MSCHAP authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 381
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security and backward compatibility when accessing the wireless network?
A. Open wireless network and SSL VPN
B. WEP with a 40-bit key
C. WPA2 using a RADIUS back-end for 802.1x authentication
D. WPA using a preshared key
Answer: D (LEAVE A REPLY)

NEW QUESTION: 382
A security technician would like to obscure sensitive data within a file so that it can be transferred without causing suspicion.
Which of the following technologies would BEST be suited to accomplish this?
A. Transport Encryption
B. Stream Encryption
C. Digital Signature
D. Steganography
Answer: D (LEAVE A REPLY)
Steganography is the process of hiding a message in another message so as to obfuscate its importance. It is also the process of hiding a message in a medium such as a digital image, audio file, or other file. In theory, doing this prevents analysts from detecting the real message. You could encode your message in another file or message and use that file to hide your message.

NEW QUESTION: 383
An organization's Chief Information Officer (CIO) read an article that identified leading hacker trends and attacks, one of which is the alteration of URLs to IP addresses resulting in users being redirected to malicious websites. To reduce the chance of this happening in the organization, which of the following secire protocols should be implemented?
A. DNSSEC
B. LDAPS
C. IPSec
D. HTTPS
Answer: A (LEAVE A REPLY)

NEW QUESTION: 384
To get the most accurate results on the security posture of a system, which of the following actions should the security analyst do prior to scanning?
A. Update the web plugins
B. Patch the scanner
C. Log all users out of the system
D. Reboot the target host
Answer: B (LEAVE A REPLY)

NEW QUESTION: 385
An analyst wants to implement a more secure wifeless authentication for office access points. Which of the following technologies allows for encrypted authentication of wireless clients over TLS?
A. PEAP
B. EAP
C. WPA2
D. RADIUS
Answer: A (LEAVE A REPLY)
EAP by itself is only an authentication framework.
PEAP (Protected Extensible Authentication Protocol) fully encapsulates EAP and is designed to work within a TLS (Transport Layer Security) tunnel that may be encrypted but is authenticated. The primary motivation behind the creation of PEAP was to help correct the deficiencies discovered within EAP since that protocol assumes that the communications channel are protected. As a result, when EAP messages are able to be discovered in the "clear" they do not provide the protection that was assumed when the protocol was originally authored.
PEAP, EAP-TTLS, and EAP-TLS "protect" inner EAP authentication within SSL/TLS sessions.

NEW QUESTION: 386

A company is deploying smartphones for its mobile salesforce. These devices are for personal and
business use but are owned by the company. Sales personnel will save new customer data via a custom
application developed for the company. This application will integrate with the contact information stored in
the smartphones and will populate new customer records onto it.
The customer application's data is encrypted at rest, and the application's connection to the back office
system is considered secure. The Chief Information Security Officer (CISO) has concerns that customer
contact information may be accidentally leaked due to the limited security capabilities of the devices and
the planned controls.
Which of the following will be the MOST efficient security control to implement to lower this risk?
A. Implement a mobile data loss agent on the devices to prevent any user manipulation with the contact
information.
B. Restrict contact information storage dataflow so it is only shared with the customer application.
C. Restrict screen capture features on the devices when using the custom application and the contact
information.
D. Require complex passwords for authentication when accessing the contact information.
Answer: (SHOW ANSWER)

NEW QUESTION: 387
A department head at a university resigned on the first day of the spring semester. It was subsequently determined that the department head deleted numerous files and directories from the server-based home directory while the campus was closed. Which of the following policies or procedures could have prevented this from occurring?
A. Time-of-day restrictions
B. Offboarding
C. Account expiration
D. Permission auditing and review
Answer: B (LEAVE A REPLY)

NEW QUESTION: 388
An IT manager is estimating the mobile device budget for the upcoming year. Over the last five years, the number of devices that were replaced due to loss, damage, or theft steadily increased by 10%. Which of the following would BEST describe the estimated number of devices to be replaced next year?

A. RPO
B. SLE
C. ALE
D. ARO
Answer: B (LEAVE A REPLY)

NEW QUESTION: 389
A vice president at a manufacturing organization is concerned about desktops being connected to the network.
Employees need to log onto the desktops' local account to verify that a product is being created within specifications; otherwise, the desktops should be as isolated as possible. Which of the following is the BEST way to accomplish this?
A. Join the desktops to an ad-hoc network.
B. Air gap the desktops.
C. Put the desktops in the DMZ.
D. Create a separate VLAN for the desktops.
Answer: (SHOW ANSWER)

NEW QUESTION: 390
Which of the following vulnerabilities can lead to unexpected system behavior, including the bypassing of security controls, due to differences between the time of commitment and the time of execution?
A. Buffer overflow
B. DLL injection
C. Pointer dereference
D. Race condition
Answer: C (LEAVE A REPLY)
Explanation
Buffer overflow protection is any of various techniques used during software development to enhance the security of executable programs by detecting on stack-allocated variables, and preventing them from causing program misbehavior or from becoming serious security vulnerabilities.
DLL injection is a technique which to run arbitrary code in the context of the address space of another process. If this process running with excessive privileges then it could be abused by an attacker in order to execute malicious code in the form of a file in order to elevate privileges.

NEW QUESTION: 391
A security analyst is hardening an authentication server. One of the primary requirements is to ensure there is mutual authentication and delegation. Given these requirements, which of the following technologies should the analyst recommend and configure?
A. LDAP services

B. CHAP services
C. Kerberos services
D. NTLM services
Answer: D (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 392
The Chief Executive Officer (CEO) received an email from the Chief Financial Ofcer (CFO), asking the CEO to send nancial details. The CEO thought it was strange that the CFO would ask for the nancial details via email. The email address was correct in the "From "section of the email. The CEO clicked the form and sent the financial information as requested. Which of the following caused the incident?
A. SPF not enabled
B. MX records rerouted
C. Malicious insider
D. Domain hijacking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 393
Which of the following is used to encrypt web application data?
A. MD5
B. AES
C. SHA
D. DHA
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 394
A staff member contacts the help desk because the staff member's device is currently experiencing the following symptoms:
* Long delays when launching applications
* Timeout errors when loading some websites
* Errors when attempting to open local Word documents and photo files

* Pop-up messages in the task bar stating that antivirus is out-of-date
* VPN connection that keeps timing out, causing the device to lose connectivity
Which of the following BEST describes the root cause of these symptoms?
A. The user has disabled the antivirus software on the device, and the hostchecker for the VPN is preventing access.
B. The proxy server for accessing websites has a rootkit installed, and this is causing connectivity issues.
C. The device is infected with crypto-malware, and the files on the device are being encrypted.
D. A patch has been incorrectly applied to the device and is causing issues with the wireless adapter on the device.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 395
Task: Determine the types of attacks below by selecting an option from the dropdown list.
Answer:
Explanation
A: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
B: Whaling is a specific kind of malicious hacking within the more general category of phishing, which involves hunting for data that can be used by the hacker. In general, phishing efforts are focused on collecting personal data about users. In whaling, the targets are high-ranking bankers, executives or others in powerful positions or job titles. Hackers who engage in whaling often describe these efforts as "reeling in a big fish," applying a familiar metaphor to the process of scouring technologies for loopholes and opportunities for data theft. Those who are engaged in whaling may, for example, hack into specific networks where these powerful individuals work or store sensitive data. They may also set up keylogging or other malware on a work station associated with one of these executives. There are many ways that hackers can pursue whaling, leading C-level or top-level executives in business and government to stay vigilant about the possibility of cyber threats.
C: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
D: SPIM is a term sometimes used to refer to spam over IM (Instant Messaging). It's also called just spam, instant spam, or IM marketing. No matter what the name, it consists of unwanted messages transmitted through some form of instant messaging service, which can include Short Message Service (SMS) E: Social engineering is a non-technical method of intrusion hackers use

that relies heavily on human interaction and often involves tricking people into breaking normal security procedures. It is one of the greatest threats that organizations today encounter. A social engineer runs what used to be called a "con game." For example, a person using social engineering to break into a computer network might try to gain the confidence of an authorized user and get them to reveal information that compromises the network's security.
Social engineers often rely on the natural helpfulness of people as well as on their weaknesses. They might, for example, call the authorized employee with some kind of urgent problem that requires immediate network access. Appealing to vanity, appealing to authority, appealing to greed, and old-fashioned eavesdropping are other typical social engineering techniques.
http://www.webopedia.com/TERM/P/phishing.html
http://www.techopedia.com/definition/28643/whaling
http://www.webopedia.com/TERM/V/vishing.html
http://searchsecurity.techtarget.com/definition/social-engineering

NEW QUESTION: 396
A company's MOM policy outlines the following requirements:
* Devices can be securely sanitized.
* Devices must only utilize secure Wifi.
* Devices must have biometric and PIN code setup.
The employees must also agree that all devices set up within the MDM have location services turned on. Which of the following options will address AT LEAST two of these requirements?
A. Full-device encryption, sideloading
BYOO. geolocation
B. Geofencing, CYOO
C. Geolocation. remote wipe
Answer: C (LEAVE A REPLY)

NEW QUESTION: 397
A security analyst monitors the syslog server and notices the following:
A. Memory leak
B. Buffer overflow
C. Null pointer deference
D. Integer overflow
Answer: B (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 398
Which of the following can be provided to an AAA system for the identification phase?
A. Username
B. Permissions
C. One-time token

D. Private certificate
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 399
A cryptographer has developed a new proprietary hash function for a company and solicited employees to test the function before recommending its implementation. An employee takes the plaintext version of a document and hashes it, then changes the original plaintext document slightly and hashes it, and continues repeating this process until two identical hash values are produced from two different documents. Which of the following BEST describes this cryptographic attack?
A. Brute force
B. Known plaintext
C. Replay
D. Collision
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 400
A company uses wireless for ail laptops and keeps a very detailed record of its assets, along with a comprehensive list of devices that are authorized to be on the wireless network. The Chief Information Officer (CIO) is concerned about a script kiddie potentially using an unauthorized device to brute force the wireless PSK and obtain access to the internal network. Which of the following should the company implement to BEST prevent this from occurring?
A. IP filtering
B. WPA-EAP
C. A WIDS
D. A BPDU guard
Answer: C (LEAVE A REPLY)

NEW QUESTION: 401
Which of the following BEST explains the reason why a server administrator would place a document named password.txt on the desktop of an administrator account on a server?
A. The document is a standard file that the OS needs to verify the login credentials.
B. The document is a honeyfile and is meant to attract the attention of a cyberintruder.
C. The document is a backup file if the system needs to be recovered
D. The document is a keylogger that stores all keystrokes should the account be compromised.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 402

A security administrator is trying to encrypt communication. For which of the following reasons should administrator take advantage of the Subject Alternative Name (SAM) attribute of a certificate?

A. It can protect multiple domains

B. It provides extended site validation

C. It does not require a trusted certificate authority

D. It protects unlimited subdomains

Answer: A (LEAVE A REPLY)

SAN or multi-domain SSLs are ideal for environments such as Microsoft Exchange Server when you need to secure multiple websites with different domain names. B is wrong because there's no extended site validation certificate but rather extended validation certificates, as the name suggests, require more validation of the certificate holder; thus, they provide more security.

NEW QUESTION: 403

A company wants to implement an access management solution that allows employees to use the same usernames and passwords for multiple applications without having to keep multiple credentials synchronized. Which of the following solutions would BEST meet these requirements?

A. Multifactor authentication

B. Biometrics

C. SSO

D. PKI

E. Federation

Answer: (SHOW ANSWER)

NEW QUESTION: 404

Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?

A. Shibboleth

B. OAuth

C. OpenID connect

D. RADIUS federation

E. SAML

Answer: D (LEAVE A REPLY)

NEW QUESTION: 405

A workstation puts out a network request to locate another system. Joe, a hacker on the network, responds before the real system does, and he tricks the workstation into communicating with him. Which of the following BEST describes what occurred?

A. The hacker used a pass-the-hash attack.

B. The hacker exploited weak switch configuration.

C. The hacker-exploited importer key management.
D. The hacker used a race condition.
Answer: (SHOW ANSWER)

NEW QUESTION: 406
The process of applying a salt and cryptographic hash to a password then repeating the process many times is known as which of the following?
A. Collision resistance
B. Key stretching
C. Brute force attack
D. Rainbow table
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 407
Given the output:
Which of the following account management practices should the security engineer use to mitigate the identified risk?
A. Implement two-factor authentication.
B. Implement least privilege.
C. Eliminate shared accounts.
D. Eliminate password reuse.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 408
Joe, a user, wants to send Ann, another user, a confidential document electronically. Which of the following should Joe do to ensure the document is protected from eavesdropping?
A. Encrypt it with Ann's public key
B. Encrypt it with Joe's public key
C. Encrypt it with Ann's private key
D. Encrypt it with Joe's private key
Answer: A (LEAVE A REPLY)

NEW QUESTION: 409
A security, who is analyzing the security of the company's web server, receives the following output:
Which of the following is the issue?
A. Stored procedures
B. Access violations
C. Code signing
D. Unencrypted credentials
Answer: D (LEAVE A REPLY)

NEW QUESTION: 410
Six months into development, the core team assigned to implement a new internal piece of software must convene to discuss a new requirement with the stake holders. A stakeholder identified a missing feature critical to the organization, which must be implemented. The team needs to validate the feasibility of the newly introduced requirement and ensure it does not introduce new vulnerabilities to the software and other applications that will integrate with it.
Which of the following BEST describes what the company?
A. The system integration phase of the SDLC
B. The system development phase of the SDLC
C. The system analysis phase of SSDSLC
D. The system design phase of the SDLC
Answer: (SHOW ANSWER)

NEW QUESTION: 411
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
Answer:

NEW QUESTION: 412
A penetration tester is checking to see if an internal system is vulnerable to an attack using a remote listener. Which of the following commands should the penetration tester use to verify if this vulnerability exists? (Choose two.)
A. nmap
B. tail
C. tcpdump
D. nc
E. nslookup
F. tracert

Answer: A,D (LEAVE A REPLY)

NEW QUESTION: 413
Which of the following serves to warn users against downloading and installing pirated software on company devices?
A. NDA
B. ISA
C. AUP
D. BPA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 414
Using an ROT13 cipher to protect confidential information for unauthorized access is known as:
A. steganography.
B. obfuscation.
C. non-repudiation.
D. diffusion.
Answer: (SHOW ANSWER)
Explanation/Reference:

NEW QUESTION: 415
A call center company wants to implement a domain policy primarily for its shift workers. The call center has large groups with different user roles. Management wants to monitor group performance. Which of the following is the BEST solution for the company to implement?
A. Reduced failed logon attempts
B. Increased account lockout time
C. Time-of-day restrictions
D. Mandatory password changes
Answer: C (LEAVE A REPLY)

NEW QUESTION: 416
A user suspects someone has been accessing a home network without permission by spoofing the MAC address of an authorized system. While attempting to determine if an authorized user is logged into the home network, the user reviews the wireless router, which shows the following table for systems that are currently on the home network.
Which of the following should be the NEXT step to determine if there is an unauthorized user on the network?
A. Apply MAC filtering and see if the router drops any of the systems.
B. Physically check each of the authorized systems to determine if they are logged onto the network.

C. Conduct a ping sweep of each of the authorized systems and see if an echo response is received.
D. Deny the "unknown" host because the hostname is not known and MAC filtering is not applied to this host.
Answer: (SHOW ANSWER)

NEW QUESTION: 417
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:
Which of the following did the security administrator discover?
A. Trojan
B. Logic bomb
C. Ransomeware
D. Backdoor
Answer: B (LEAVE A REPLY)

NEW QUESTION: 418
A security analyst is investigating a suspected security breach and discovers the following in the logs of the potentially compromised server:
Which of the following would be the BEST method for preventing this type of suspected attack in the future?
A. Implement account lockout settings
B. Implement password expirations
C. Implement restrictions on shared credentials
D. Implement time-of-day restrictions on this server
Answer: (SHOW ANSWER)

NEW QUESTION: 419
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artefacts.

NEW QUESTION: 420
In determining when it may be necessary to perform a credentialed scan against a system instead of a non- credentialed scan, which of the following requirements is MOST likely to influence its decisions?
A. The scanner must be able to audit file system permissions
B. The scanner must be able to footprint the network
C. The scanner must be able to check for open ports with listening services
D. The scanner must be able to enumerate the host OS of devices scanner
Answer: (SHOW ANSWER)

NEW QUESTION: 421
537 A company uses an enterprise desktop imaging solution to manage deployment of its desktop computers. Desktop computer users are only permitted to use software that is part of the baseline image. Which of the following technical solutions was MOST likely deployed by the company to ensure only known-good software can be installed on corporate desktops?
A. Network access control
B. Configuration manager
C. File integrity checks
D. Application whitelisting
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 422
A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.
Answer:

NEW QUESTION: 423
A dumpster diver recovers several hard drives from a company and is able to obtain confidential data from one of the hard drives. The company then discovers its information is posted online. Which of the following methods would have MOST likely prevented the data from being exposed?
A. Using software to repeatedly rewrite over the disk space

B. Using magnetic fields to erase the data
C. Using Blowfish encryption on the hard drives
D. Removing the hard drive from its enclosure
Answer: B (LEAVE A REPLY)

NEW QUESTION: 424
Company A agrees to provide perimeter protection, power, and environmental support with measurable goals for Company B, but will not be responsible for user authentication or patching of operating systems within the perimeter.
Which of the following is being described?
A. Interoperability agreement
B. Memorandum of understanding
C. Service level agreement
D. Business partner agreement
Answer: C (LEAVE A REPLY)

NEW QUESTION: 425
An organization has implemented a two-step verification process to protect user access to data that is stored in the cloud. Each employee now uses an email address or mobile number to receive a code to access the data.
Which of the following authentication methods did the organization implement?
A. HOTP
B. Push notification
C. Static code
D. Token key
Answer: A (LEAVE A REPLY)

NEW QUESTION: 426
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.

2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.
3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.
4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References:
http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

NEW QUESTION: 427
An administrator is replacing a wireless router. The configuration of the old wireless router was not documented before it stopped functioning. The equipment connecting to the wireless network uses older legacy equipment that was manufactured prior to the release of the 802.11i standard. Which of the following configuration options should the administrator select for the new wireless router?
A. WPA2+TWP
B. WPA2+CCMP
C. WPA+TWP
D. WPA+CCMP
Answer: A (LEAVE A REPLY)

NEW QUESTION: 428

An incident responder is preparing to acquire images and files from a workstation that has been compromised. The workstation is still powered on and running. Which of the following should be acquired LAST?

A. Processes in running memory

B. Swap space

C. Processor cache

D. Application files on hard disk

Answer: D (LEAVE A REPLY)

NEW QUESTION: 429

The website of a bank that an organization does business with is being reported as untrusted by the organization's web browser. A security analyst has been assigned to investigate. The analyst discovers the bank recently merged with another local bank and combined names. Additionally, the user's bookmark automatically redirects to the website of the newly named bank. Which of the following is the MOST likely cause of the issue?

A. The website's certificate still has the old bank's name

B. The company's web browser is not up to date

C. The website was created too recently to be trusted

D. The website's certificate has expired

Answer: A (LEAVE A REPLY)

NEW QUESTION: 430

A security auditor is reviewing the following output from file integrity monitoring software installed on a very busy server at a large service provider. The server has not been updates since it was installed. Drag and drop the log entry that identifies the first instance of server compromise.

Answer:

NEW QUESTION: 431

A hacker has a packet capture that contains:

Which of the following tools will the hacker use against this type of capture?

A. Password cracker

B. Vulnerability scanner

C. DLP scanner

D. Fuzzer

Answer: A (LEAVE A REPLY)

NEW QUESTION: 432

A network administrator is creating a new network for an office. For security purposes, each department should have its resources isolated from every other department but be able to communicate back to central servers.

Which of the following architecture concepts would BEST accomplish this?

A. Air gapped network
B. Load balanced network
C. Network address translation
D. Network segmentation
Answer: D (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 433
While troubleshooting a client application connecting to the network, the security administrator notices the following error: Certificate is not valid.
Which of the following is the BEST way to check if the digital certificate is valid?
A. IPSec
B. CSR
C. PKI
D. CRL
Answer: (SHOW ANSWER)

NEW QUESTION: 434
A software developer wants to ensure that the application is verifying that a key is valid before establishing SSL connections with random remote hosts on the Internet. Which of the following should be used in the code? (Select TWO.)
A. Remote server public key
B. OCSP
C. SSL symmetric encryption key
D. Escrowed keys
E. Software code private key
Answer: B,E (LEAVE A REPLY)

NEW QUESTION: 435
A systems administrator is installing and configuring an application service that requires access to read and write to log and configuration files on a local hard disk partition reduce the attack surface added by the service and account? (Select TWO).
A. Add the account to the local administrators group
B. Enable and review account audit logs.
C. Use a guest account placed in a non-privileged users group.
D. Enforce least possible privileges for the account
E. Utilize a generic password for authenticating
F. Use a unique managed service account
Answer: D,F (LEAVE A REPLY)

NEW QUESTION: 436

A member of the admins group reports being unable to modify the "changes" file on a server. The permissions on the file are as follows:
Permissions User Group File
-rwxrw-r--+ Admins Admins changes
Based on the output above, which of the following BEST explains why the user is unable to modify the
"changes" file?
A. An FACL has been added to the permissions for the file.
B. The SELinux mode on the server is set to "enforcing."
C. The admins group does not have adequate permissions to access the file.
D. The SELinux mode on the server is set to "permissive."
Answer: A (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 437
An administrator has concerns regarding the traveling sales team who works primarily from smart phones.
Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?
A. Enable GPS tracking on all smart phones so that they can be quickly located and recovered
B. Configure the smart phones so that the stored data can be destroyed from a centralized location
C. Enable screensaver locks when the phones are not in use to prevent unauthorized access
D. Configure the smart phones so that all data is saved to removable media and kept separate from the device
Answer: B (LEAVE A REPLY)

NEW QUESTION: 438
A security analyst has received the following alert snippet from the HIDS appliance:
Given the above logs, which of the following is the cause of the attack?
A. The TCP ports on destination are all open
B. There is improper Layer 2 segmentation
C. FIN, URG, and PSH flags are set in the packet header

D. TCP MSS is configured improperly
Answer: C (LEAVE A REPLY)

NEW QUESTION: 439
A company occupies the third floor of a leased building that has other tenants. The path from the demarcation point to the company's controlled space runs through unsecured areas managed by other companies. Which of the following could be used to protect the company's cabling as it passes through uncontrolled spaces?
A. Plenum-rated cables
B. Conduits
C. Cable locks
D. Bayonet Neill-Concelman
Answer: C (LEAVE A REPLY)

NEW QUESTION: 440
Joe, an employee, asks a coworker how long ago Ann started working at the help desk. The coworker expresses surprise since nobody named Ann works at the help desk. Joe mentions that Ann called several people in the customer service department 10 help reset their passwords over the phone due to unspecified "server issues.' Which of the following has occurred?
A. Social engineering
B. Whaling
C. Password cracking
D. Watering hots attack
Answer: A (LEAVE A REPLY)

NEW QUESTION: 441
A security architect has convened a meeting to discuss an organization's key management policy. The organization has a reliable internal key management system, and some argue that it would be best to manage the cryptographic keys internally as opposed to using a solution from a third party. The company should use:
A. a software solution including secure key escrow capabilities.
B. the current internal key management system.
C. a third-party key management system that will reduce operating costs.
D. risk benefits analysis results to make a determination.
Answer: (SHOW ANSWER)

NEW QUESTION: 442
An attachment that was emailed to finance employees contained an embedded message. The security administrator investigates and finds the intent was to conceal the embedded information from public view.
Which of the following BEST describes this type of message?

A. Obfuscation
B. Stenography
C. Diffusion
D. BCRYPT
Answer: A (LEAVE A REPLY)
Explanation/Reference:

NEW QUESTION: 443
User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?
A. Trust model
B. Stapling
C. Intermediate CA
D. Key escrow
Answer: A (LEAVE A REPLY)
Explanation

NEW QUESTION: 444
A malicious system continuously sends an extremely large number of SYN packets to a server. Which of the following BEST describes the resulting effect?
A. The server's firewall will be unable to effectively filter traffic due to the amount of data transmitted
B. The server will exhaust its memory maintaining half-open connections
C. The server will crash when trying to reassemble all the fragmented packets
D. The server will be unable to server clients due to lack of bandwidth
Answer: B (LEAVE A REPLY)

NEW QUESTION: 445
An analyst generates the following color-coded table shown in the exhibit to help explain the risk of potential incidents in the company. The vertical axis indicates the likelihood or an incident, while the horizontal axis indicates the impact.
Which of the following is this table an example of?
A. Supply chain assessment
B. Qualitative risk assessment
C. Internal threat assessment
D. Privacy impact assessment
Answer: B (LEAVE A REPLY)

NEW QUESTION: 446

The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.
Which of the following is the best solution for the network administrator to secure each internal website?
A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server
Answer: A (LEAVE A REPLY)
If a company has a Microsoft server, they can become their own CA at no cost and hand out certs to their servers. Each server could also have a self signed certificate at no cost. If I were going with the best solution, I would choose A because a self signed certificate cannot be revoked. Also, for both of the scenarios, each time you run across a new CA as a client, you get a popup that asks you to accept that CA. Not really sure if this is true about self signed certs but I would suspect that each time you go to another server, you have another popup. But if the company issues it, it would appear once, the company's CA would be listed in the accepted CA table, and you could go to all of the server.

NEW QUESTION: 447
When considering a third-party cloud service provider, which of the following criteria would be the BEST to include in the security assessment process? (Choose two.)
A. Breadth of applications support
B. Data retention policies
C. Use of performance analytics
D. Size of the corporation
E. Adherence to regulatory compliance
Answer: (SHOW ANSWER)

NEW QUESTION: 448
A penetration tester is conducting an assessment on Comptia.org and runs the following command from a coffee shop while connected to the public Internet: c:\nslookup -querytype=MX comptia.org Server: Unknown Address: 198.51.100.45 comptia.org MX preference=10, mail exchanger = 92.68.102.33 comptia.org MX preference=20, mail exchanger = exchg1.comptia.org exchg1.comptia.org internet address = 192.168.102.67 Which of the following should the penetration tester conclude about the command output?
A. The DNS SPF records have not been updated for Comptia.org.
B. 192.168.102.67 is a backup mail server that may be more vulnerable to attack.
C. The public/private views on the Comptia.org DNS servers are misconfigured.
D. Comptia.org is running an older mail server, which may be vulnerable to exploits.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 449
Which of the following best describes routine in which semicolons, dashes, quotes, and commas are removed from a string?
A. Input validation to protect against SQL injection.
B. Error handling to protect against program exploitation
C. Padding to protect against string buffer overflows.
D. Exception handling to protect against XSRF attacks.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 450
A security administrator begins assessing a network with software that checks for available exploits against a known database using both credentials and external scripts A report will be compiled and used to confirm patching levels This is an example of
A. vulnerability scanning
B. penetration testing
C. fuzzing
D. static code analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 451
A company is implementing a system to transfer direct deposit information to a financial institution. One of the requirements is that the financial institution must be certain that the deposit amounts within the file have not been changed. Which of the following should be used to meet the requirement?
A. Transport encryption
B. Digital signatures
C. Key escrow
D. Perfect forward secrecy
E. File encryption
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 452
A company's loss control department identifies theft as a recurring loss type over the past year. Based on the department's report, the Chief Information Officer (CIO) wants to detect theft of datacenter equipment.
Which of the following controls should be implemented?
A. Mantraps
B. Biometrics
C. Motion detectors
D. Cameras
Answer: (SHOW ANSWER)

NEW QUESTION: 453
A security specialist is notified about a certificate warning that users receive when using a new internal website. After being given the URL from one of the users and seeing the warning, the security specialist inspects the certificate and realizes it has been issued to the IP address, which is how the developers reach the site.
Which of the following would BEST resolve the issue?
A. PEM
B. OID
C. OSCP
D. SAN
Answer: (SHOW ANSWER)

NEW QUESTION: 454
An attacker uses a network sniffer to capture the packets of a transaction that adds $20 to a gift card.
The attacker then user a function of the sniffer to push those packets back onto the network again, adding another $20 to the gift card. This can be done many times.
Which of the following describes this type of attack?
A. Smurf attack
B. Replay attack
C. Cross-site scripting attack
D. Integer overflow attack
E. Buffer overflow attack
Answer: B (LEAVE A REPLY)

NEW QUESTION: 455
An organization's internal auditor discovers that large sums of money have recently been paid to a vendor that management does not recognize. The IT security department is asked to investigate the organizations the organization's ERP system to determine how the accounts payable module has been used to make these vendor payments.

The IT security department finds the following security configuration for the accounts payable module:
New Vendor Entry - Required Role: Accounts Payable Clerk
New Vendor Approval - Required Role: Accounts Payable Clerk
Vendor Payment Entry - Required Role: Accounts Payable Clerk
Vendor Payment Approval - Required Role: Accounts Payable Manager
Which of the following changes to the security configuration of the accounts payable module would BEST mitigate the risk?
A:
B:
C:
D:
A. Option D
B. Option B
C. Option C
D. Option A
Answer: (SHOW ANSWER)

NEW QUESTION: 456
A security analyst wishes to increase the security of an FTP server. Currently, all traffic to the FTP server is unencrypted. Users connecting to the FTP server use a variety of modern FTP client software.
The security analyst wants to keep the same port and protocol, while also still allowing unencrypted connections. Which of the following would BEST accomplish these goals?
A. Use implicit TLS on the FTP server.
B. Use SSH tunneling to encrypt the FTP traffic.
C. Require the SFTP protocol to connect to the file server.
D. Use explicit FTPS for connections.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 457
The network information for a workstation is as follows:
When the workstation's user attempts to access www.example.com. the URL that actually opens is www.notexample.com. The user successfully connects to several other legitimate URLs. Which of the following have MOST likely occurred? (Select TWO)
A. Buffer overflow
B. DNS poisoning
C. Domain hijacking
D. ARP poisoning
E. IP spoofing

Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 458
A systems administrator is configuring a system that uses data classification labels.
Which of the following will the administrator need to implement to enforce access control?
A. Role-based access control
B. Discretionary access control
C. Rule-based access control
D. Mandatory access control
Answer: D (LEAVE A REPLY)

NEW QUESTION: 459
An organization has decided to host its web application and database in the cloud. Which of the following
BEST describes the security concerns for this decision?
A. Access to the organization's servers could be exposed to other cloud-provider clients.
B. Vendor support will cease when the hosting platforms reach EOL.
C. Outsourcing the code development adds risk to the cloud provider.
D. The cloud vendor is a new attack vector within the supply chain.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 460
You have been tasked with designing a security plan for your company. Drag and drop the appropriate security controls on the floor plan.
Instructions: All objects must be used and all place holders must be filled. Order does not matter. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
Cable locks - Adding a cable lock between a laptop and a desk prevents someone from picking it up and walking away Proximity badge + reader Safe is a hardware/physical security measure Mantrap can be used to control access to sensitive areas. CCTV can be used as video surveillance.
Biometric reader can be used to control and prevent unauthorized access. Locking cabinets can be used to protect backup media, documentation and other physical artifacts.

NEW QUESTION: 461
Drag and drop the correct protocol to its default port.
Answer:
Explanation
FTP uses TCP port 21. Telnet uses port 23.

SSH uses TCP port 22.
All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22.
Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).
Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.
Port 69 is used by TFTP.
SNMP
makes use of UDP ports 161 and 162.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 462
Which of the following occurs when the security of a web application relies on JavaScript for input validation?
A. The application is vulnerable to race conditions.
B. The security of the application relies on antivirus.
C. The integrity of the data is at risk.
D. A host-based firewall is required.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 463
The application team within a company is asking the security team to investigate why its application is slow after an upgrade. The source of the team's application is 10.13.136.9. and the destination IP is 10.17.36.5. The security analyst pulls the logs from the endpoint security software but sees nothing is being blocked. The analyst then looks at the UTM firewall logs and sees the following:
Which of the following should the security analyst request NEXT based on the UTM firewall analysis?
A. Request the network team to open port 1433 from 10.13.136.9 to 10.17.36.5.
B. Request the application team to allow TCP port 87 to listen on 10.17.36.5.
C. Request the application team to reconfigure the application and allow RPC communication.
D. Request the network team to turn of IPS for 10.13.136.8 going to 10.17.36.5.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 464
A company is performing an analysis of the corporate enterprise network with the intent of identifying what will cause losses in revenue, referrals, and/or reputation when out of commission.
Which of the following is an element of a BIA that is being addressed?
A. Mission-essential function
B. Single point of failure

C. backup and restoration plans
D. Identification of critical systems
Answer: A (LEAVE A REPLY)
Explanation/Reference:
Explanation:
The BIA is composed of the following three steps: Determine mission/business processes and recovery criticality. Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime.

NEW QUESTION: 465
A security administrator is implementing a secure method that allows developers to place files or objects onto a Linux Server. Developers are required to log in using a username, password, and asymmetric key. Which of the following protocols should be implemented?
A. IPSec
B. SRTP
C. SFTP
D. SSL/TLS
Answer: C (LEAVE A REPLY)

NEW QUESTION: 466
A security administrator is reviewing the following PowerShell script referenced in the Task Scheduler on a database server:
$members = GetADGroupMemeber -Identity "Domain Admins" -Recursive |
Select - ExpandProperty name
if ($members -notcontains "JohnDoe"){
Remove-Item -path C:\Database -recurse -force
}
Which of the following did the security administrator discover?
A. Logic bomb
B. Ransomeware
C. Trojan
D. Backdoor
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here:

https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: **Freepdfdumps**)

NEW QUESTION: 467
Company A has acquired Company B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure. Which of the following methods would allow the two companies to access one another's resources?
A. Single sign-on
B. Attestation
C. Federation
D. Kerberos
Answer: C (LEAVE A REPLY)

NEW QUESTION: 468
An organization wants to implement a solution that allows for automated logical controls for network defense. An engineer plans to select an appropriate network security component, which automates response actions based on security threats to the network. Which of the following would be MOST appropriate based on the engineer's requirements?
A. NAC
B. NIPS
C. HIDS
D. Elastic load balancer
E. Web proxy
Answer: (SHOW ANSWER)

NEW QUESTION: 469
In performing an authorized penetration test of an organization's system security, a penetration tester collects information pertaining to the application versions that reside on a server. Which of the following is the best way to collect this type of information?
A. Code review
B. Banner grabbing
C. Protocol analyzer
D. Port scanning
Answer: B (LEAVE A REPLY)

NEW QUESTION: 470
A security technician has been receiving alerts from several servers that indicate load balancers have had a significant increase in traffic. The technician initiates a system scan. The scan results illustrate that the disk space on several servers has reached capacity. The scan also indicates that incoming internet traffic to the servers has increased.

Which of the following is the MOST likely cause of the decreased disk space?
A. Authentication issues
B. Unauthorized software
C. Misconfigured devices
D. Logs and events anomalies
Answer: B (LEAVE A REPLY)

NEW QUESTION: 471
An application developer has neglected to include input validation checks in the design of the company's new web application. An employee discovers that repeatedly submitting large amounts of data, including custom code, to an application will allow the execution of the custom code at the administrator level. Which of the following BEST identifies this application attack?
A. Buffer overflow
B. Replay
C. Cross-site scripting
D. Clickjacking
Answer: A (LEAVE A REPLY)

NEW QUESTION: 472
An external attacker can modify the ARP cache of an internal computer. Which of the following types of attacks is described?
A. Replay
B. Client-side attack
C. Spoofing
D. DNS poisoning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 473
A security analyst believes an employee's workstation has been compromised. The analyst reviews the system logs, but does not find any attempted logins. The analyst then runs the diff command, comparing the C:\Windows\System32 directory and the installed cache directory. The analyst finds a series of files that look suspicious.
One of the files contains the following commands:
Which of the following types of malware was used?
A. Backdoor
B. Worm
C. Spyware
D. Logic bomb
Answer: (SHOW ANSWER)

NEW QUESTION: 474

Which of the following attack types BEST describes a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser?
A. MITM
B. Buffer overflow
C. XSS
D. SQLi
Answer: C (LEAVE A REPLY)

NEW QUESTION: 475
An administrator has concerns regarding the traveling sales team who works primarily from smart phones. Given the sensitive nature of their work, which of the following would BEST prevent access to the data in case of loss or theft?
A. Enable screensaver locks when the phones are not in use to prevent unauthorized access
B. Enable GPS tracking on all smart phones so that they can be quickly located and recovered
C. Configure the smart phones so that the stored data can be destroyed from a centralized location
D. Configure the smart phones so that all data is saved to removable media and kept separate from the device
Answer: C (LEAVE A REPLY)

NEW QUESTION: 476
A systems administrator needs to configure an SSL remote access VPN according to the following organizational guidelines:
* The VPN must support encryption of header and payload.
* The VPN must route all traffic through the company's gateway.
Which of the following should be configured on the VPN concentrator?
A. Transport mode
B. Full tunnel
C. Tunnel mode
D. IPSec
Answer: (SHOW ANSWER)

NEW QUESTION: 477
An organization has implemented an IPSec VPN access for remote users.
Which of the following IPSec modes would be the MOST secure for this organization to implement?
A. Tunnel mode
B. Transport mode
C. AH-only mode
D. ESP-only mode
Answer: (SHOW ANSWER)

In both ESP and AH cases with IPSec Transport mode, the IP header is exposed. The IP header is not exposed in IPSec Tunnel mode.

NEW QUESTION: 478
Which of the following is used to encrypt web application data?
A. SHA
B. DHA
C. MD5
D. AES
Answer: C (LEAVE A REPLY)

NEW QUESTION: 479
The Chief Executive Officer (CEO) of an organization would like staff members to have the flexibility to work from home anytime during business hours, including during a pandemic or crisis. However, the CEO is concerned that some staff members may take advantage of the flexibility and work from high-risk countries while on holiday or outsource work to a third-party organization in another country. The Chief Information Officer (CIO) believes the company can implement some basic controls to mitigate the majority of the risk.
Which of the following would be BEST to mitigate the CEO's concerns? (Choose two.)
A. Geolocation
B. Time-of-day restrictions
C. Certificates
D. Tokens
E. Geotagging
F. Role-based access controls
Answer: (SHOW ANSWER)
Explanation

NEW QUESTION: 480
An analyst is currently looking at the following output:
Which of the following security issues has been discovered based on the output?
A. License compliance violation
B. Miscongured admin permissions
C. Unauthorized software
D. Insider threat
Answer: (SHOW ANSWER)

NEW QUESTION: 481
A systems administrator has created network file shares for each department with associated security groups for each role within the organization. Which of the following security concepts is the systems administrator implementing?

A. Permission auditing
B. Least privilege
C. Separation of duties
D. Standard naming convention
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 482
Which of the following cryptographic algorithms can be used for full-disk encryption?
A. PBKDF2
B. SHA-256
C. AES
D. RSA
Answer: C (LEAVE A REPLY)

NEW QUESTION: 483
An organization wants to deliver streaming audio and video from its home office to remote locations all over the world. It wants the stream to be delivered securely and protected from intercept and replay attacks.
Which of the following protocols is BEST suited for this purpose?
A. SIP
B. SSH
C. SRTP
D. S/MIME
Answer: (SHOW ANSWER)

NEW QUESTION: 484
A retail executive recently accepted a job with a major competitor. The following week, a security analyst reviews the security logs and Identifies successful logon attempts to access the departed executive's accounts. Which of the following security practices would have addressed the issue?
A. An acceptable use policy
B. A non-disclosure agreement
C. Off boarding

D. Least privilege
Answer: D (LEAVE A REPLY)

NEW QUESTION: 485
A buffer overflow can result in:
A. privilege escalation caused by TPM override.
B. loss of data caused by unauthorized command execution
C. repeated use of one-time keys.
D. reduced key strength due to salt manipulation
Answer: (SHOW ANSWER)

NEW QUESTION: 486
A security administrator determined that users within the company are installing unapproved software. Company policy dictates that only certain applications may be installed or ran on the user's computers without exception. Which of the following should the administrator do to prevent all unapproved software from running on the user's computer?
A. Configure the firewall to prevent the downloading of executable files
B. Prevent users from running as administrator so they cannot install software.
C. Create an application whitelist and use OS controls to enforce it
D. Deploy antivirus software and configure it to detect and remove pirated software
Answer: C (LEAVE A REPLY)

NEW QUESTION: 487
A company is using a mobile device deployment model in which employees use their personal devices for work at their own discretion. Some of the problems the company is encountering include the following:
Which of the following is a deployment model that would help the company overcome these problems?
A. VDI
B. CYOD
C. BYOD
D. COPE
Answer: (SHOW ANSWER)

NEW QUESTION: 488
Which of the following control types are alerts sent from a SIEM fulfilling based on vulnerably signatures?
A. Compensating
B. Preventive
C. Corrective
D. Detective

Answer: D (LEAVE A REPLY)

NEW QUESTION: 489
Following a breach, a forensic analyst reviewed system logs and determined that an attacker used an unknown account with elevated privileges on a computer to access organization files
Which of the following MOST likely occurred to allow the attacker to access the files?
A. The attacker renamed a domain administrator account on the computer and used it to access the files
B. The attacker used a pass-the-hash attack to access the network location and access the files
C. The attacker used an active default administrator account to create new accounts with rights to access the files
D. The attacker used Metasploit to identify the location of the organization's files and access them
Answer: C (LEAVE A REPLY)

NEW QUESTION: 490
Which of the following is MOST likely the security impact of continuing to operate end-of-life systems?
A. Support for legacy protocols
B. Lack of vendor support for decommissioning
C. Higher total cost of ownership due to support costs
D. Denial of service due to patch availability
Answer: (SHOW ANSWER)

NEW QUESTION: 491
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)
A. Transport encryption
B. Hashing
C. Block level encryption
D. Multifactor authentication
E. Predefined challenge questions
F. SAML authentication
Answer: (SHOW ANSWER)

NEW QUESTION: 492
An incident response manager has started to gather all the facts related to a SIEM alert showing multiple systems may have been compromised.
The manager has gathered these facts:
The breach is currently indicated on six user PCs
One service account is potentially compromised
Executive management has been notified

In which of the following phases of the IRP is the manager currently working?
A. Identification
B. Eradication
C. Recovery
D. Containment
Answer: (SHOW ANSWER)

NEW QUESTION: 493
Which of the following threat actors is MOST likely to steal a company's proprietary information to gain a market edge and reduce time to market?
A. Insider
B. Competitor
C. Organized crime.
D. Hacktivist
Answer: B (LEAVE A REPLY)

NEW QUESTION: 494
A security analyst is emailing Pll in a spreadsheet file to an audit validator for after-actions related to a security assessment. The analyst must make sure the PI I data is protected with the following minimum requirements;
* Ensure confidentiality at rest
* Ensure the integrity of the original email message.
Which of the following controls would ensure these data security requirements are earned out?
A. Encrypt and sign the email using S/MIME.
B. Sign the email using MD5
C. Encrypt the email and send it using TLS.
D. Hash the email using SHA-1
Answer: (SHOW ANSWER)

NEW QUESTION: 495
Which of the following would a security specialist be able to determine upon examination of a server's certificate?
A. Server private key
B. CSR
C. OID
D. CA public key
Answer: A (LEAVE A REPLY)

NEW QUESTION: 496
When configuring settings in a mandatory access control environment, which of the following specifies the subjects that can access specific data objects?

A. Owner
B. System
C. Administrator
D. User
Answer: C (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 497
Select the appropriate attack and remediation from each drop-down list to label the corresponding attack with its remediation.
INSTRUCTIONS
Not all attacks and remediation actions will be used. If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Answer:
check the answer below.
Explanation
Use the following settings for answer this simulation question.

NEW QUESTION: 498
An auditor wants to test the security posture of an organization by running a tool that will display the following:
Which of the following commands should be used?
A. ipconfig
B. arp
C. nbtstat
D. nc
Answer: C (LEAVE A REPLY)

NEW QUESTION: 499
A system uses an application server and database server Employing the principle of least privilege, only database administrators are given administrative privileges on the database server, and only application team members are given administrative privileges on the application server.

Audit and log file reviews are performed by the business unit (a separate group from the database and application teams).
The organization wants to optimize operational efficiency when application or database changes are needed, but it also wants to enforce least privilege, prevent modification of log files, and facilitate the audit and log review performed by the business unit. Which of the following approaches would BEST meet the organization's goals?
A. Switch administrative privileges for the database and application servers. Give the application team administrative privileges on the database servers and the database team administrative privileges on the application
servers.
B. Restrict privileges on the log file directory to "read only" and use a service account to send a copy of these files to the business unit.
C. Give the business unit administrative privileges on both the database and application servers so they can Independently monitor server activity.
D. Remove administrative privileges from both the database and application servers, and give the business unit "read only" privileges on the directories where the log files are kept.
Answer: (SHOW ANSWER)

NEW QUESTION: 500
A manager wants to distribute a report to several other managers within the company. Some of them reside in remote locations that are not connected to the domain but have a local server. Because there is sensitive data within the report and the size of the report is beyond the limit of the email attachment size, emailing the report is not an option. Which of the following protocols should be implemented to distribute the report securely?
(Select three.)
A. LDAPS
B. HTTPS
C. S/MIME
D. SRTP
E. SNMPv3
F. SSH
G. FTPS
Answer: B,F,G (LEAVE A REPLY)

NEW QUESTION: 501
An attack has occurred against a company.
INSTRUCTIONS
You have been tasked to do the following:
Identify the type of attack that is occurring on the network by clicking on the attacker's tablet and reviewing the output. (Answer Area 1) Identify which compensating controls should be implemented on the assets, in order to reduce the effectiveness of future attacks by dragging

them to the correct server. (Answer area 2) All objects will be used, but not all placeholders may be filled. Objects may only be used once.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Answer:

Explanation

NEW QUESTION: 502

A security administrator receives an alert from a third-party vendor that indicates a certificate that was installed in the browser has been hijacked at the root of a small public CA. The security administrator knows there are at least four different browsers in use on more than a thousand computers in the domain worldwide. Which of the following solutions would be BEST for the security administrator to implement to most efficiently assist with this issue?

A. ACL

B. SSL

C. CRL

D. PKI

Answer: (SHOW ANSWER)

NEW QUESTION: 503

An accountant is attempting to log in to the internal accounting system and receives a message that the website's certificate is fraudulent. The accountant finds instructions for manually installing the new trusted root onto the local machine. Which of the following would be the company's BEST option for this situation in the future?

A. Utilize a central CRL.

B. Implement certificate management.

C. Ensure access to KMS.

D. Use a stronger cipher suite.

Answer: (SHOW ANSWER)

Explanation

The Certificate Management System for generation, distribution, storage and verification of certificates for use in a variety of security enhanced applications. The structure of a certificate is defined in the X.509 standard.

NEW QUESTION: 504

A company wants to ensure that the validity of publicly trusted certificates used by its web server can be determined even during an extended internet outage.
Which of the following should be implemented?

A. Ocsp

B. Crl

C. Key escrow
D. Recovery agent
Answer: (SHOW ANSWER)

NEW QUESTION: 505
A security administrator wants to implement strong security on the company smart phones and terminal servers located in the data center. Drag and drop the applicable controls to each asset types?
Instructions: Controls can be used multiple times and not all placeholders need to be filled. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
Company Manages Smart Phone
Screen Lock
Strong Password
Device Encryption
Remote Wipe
GPS Tracking
Pop-up blocker
Data Center Terminal Server
Cable Locks
Antivirus
Host Based Firewall
Proximity Reader
Sniffer
Mantrap

NEW QUESTION: 506
A user receives an email from ISP indicating malicious traffic coming from the user's home network is
detected. The traffic appears to be Linux-based, and it is targeting a website that was recently featured on
the news as being taken offline by an Internet attack. The only Linux device on the network is a home
surveillance camera system.
Which of the following BEST describes what is happening?
A. The camera system is infected with a Trojan.
B. The camera system is infected with a backdoor.
C. The camera system is infected with a bot.
D. The camera system is infected with a RAT.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 507
A system administrator wants to provide balance between the security of a wireless network and usability. The administrator is concerned with wireless encryption compatibility of older devices used by some employees.
Which of the following would provide strong security and backward compatibility when accessing the wireless network?
A. WPA using a preshared key
B. WPA2 using a RADIUS back-end for 802.1x authentication
C. Open wireless network and SSL VPN
D. WEP with a 40-bit key
Answer: B (LEAVE A REPLY)

NEW QUESTION: 508
A security administrator in a bank is required to enforce an access control policy so no single individual is allowed to both initiate and approve financial transactions. Which of the following BEST represents the impact the administrator is deterring?
A. Principle of least privilege
B. External intruder
C. Conflict of interest
D. Fraud
Answer: D (LEAVE A REPLY)

NEW QUESTION: 509
Which of the following would enhance the security of accessing data stored in the cloud? (Select TWO)
A. Block level encryption
B. Predefined challenge question
C. SAML authentication
D. Multifactor authentication
E. Hashing
F. Transport encryption
Answer: C,D (LEAVE A REPLY)

NEW QUESTION: 510
An auditor is reviewing the following output from a password-cracking tool:
Which of the following methods did the author MOST likely use?
A. Rainbow table
B. Dictionary
C. Brute force
D. Hybrid

Answer: D (LEAVE A REPLY)

NEW QUESTION: 511
Management wants to ensure any sensitive data on company provided cell phones is isolated in a single location that can be remotely wiped if the phone is lost. Which of the following technologies BEST meets this need?
A. containerization
B. Sandboxing
C. Geofencing
D. device encryption
Answer: B (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 512
Select the appropriate attack from each drop down list to label the corresponding illustrated attack.
Instructions: Attacks may only be used once, and will disappear from drop down list if selected. When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation:
1: Spear phishing is an e-mail spoofing fraud attempt that targets a specific organization, seeking unauthorized access to confidential data. As with the e-mail messages used in regular phishing expeditions, spear phishing messages appear to come from a trusted source. Phishing messages usually appear to come from a large and well-known company or Web site with a broad membership base, such as eBay or PayPal. In the case of spear phishing, however, the apparent source of the e-mail is likely to be an individual within the recipient's own company and generally someone in a position of authority.
2: The Hoax in this question is designed to make people believe that the fake AV (anti- virus) software is genuine.
3: Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

4: Phishing is the act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.
Phishing email will direct the user to visit a website where they are asked to update personal information, such as a password, credit card, social security, or bank account numbers, that the legitimate organization already has. The website, however, is bogus and set up only to steal the information the user enters on the page.
5: Similar in nature to e-mail phishing, pharming seeks to obtain personal or private (usually financial related) information through domain spoofing. Rather than being spammed with malicious and mischievous e-mail requests for you to visit spoof Web sites which appear legitimate, pharming 'poisons' a DNS server by infusing false information into the DNS server, resulting in a user's request being redirected elsewhere. Your browser, however will show you are at the correct Web site, which makes pharming a bit more serious and more difficult to detect. Phishing attempts to scam people one at a time with an e-mail while pharming allows the scammers to target large groups of people at one time through domain spoofing.
References: http://searchsecurity.techtarget.com/definition/spear-phishing
http://www.webopedia.com/TERM/V/vishing.html
http://www.webopedia.com/TERM/P/phishing.html
http://www.webopedia.com/TERM/P/pharming.html

NEW QUESTION: 513
A technician wants to perform network enumeration against a subnet in preparation for an upcoming assessment. During the first phase, the technician performs a ping sweep. Which of the following scan types did the technicians use?
A. Non-intrusive
B. Credentialed
C. Intrusive
D. Passive
Answer: (SHOW ANSWER)

NEW QUESTION: 514
A company has forbidden the use of external media within its headquarters location. A security analyst is working on adding additional repositories to a server in the environment when the analyst notices some odd processes running on the system. The analyst runs a command and sees the following:
Given this output, which of the following security issues has been discovered?
A. A policy violation
B. A misconfigured HIDS
C. A malware Installation
D. The activation of a Trojan
Answer: A (LEAVE A REPLY)

NEW QUESTION: 515
Company A has acquired Company
B. Company A has different domains spread globally, and typically migrates its acquisitions infrastructure under its own domain infrastructure. Company B, however, cannot be merged into Company A's domain infrastructure.
Which of the following methods would allow the two companies to access one another's resources?
A. Federation
B. Kerberos
C. Single sign-on
D. Attestation
Answer: A (LEAVE A REPLY)

NEW QUESTION: 516
A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.
Answer:

NEW QUESTION: 517
A security administrator has been tasked with implementing controls that meet management goals. Drag and drop the appropriate control used to accomplish the account management goal. Options may be used once or not at all.
Answer:

NEW QUESTION: 518
The chief security officer (CS0) has issued a new policy that requires that all internal websites be configured for HTTPS traffic only. The network administrator has been tasked to update all internal sites without incurring additional costs.
Which of the following is the best solution for the network administrator to secure each internal website?
A. Use certificates signed by the company CA
B. Use a signing certificate as a wild card certificate
C. Use certificates signed by a public ca
D. Use a self-signed certificate on each internal server
Answer: A (LEAVE A REPLY)
This is a way to update all internal sites without incurring additional costs?
To be a CA (Certificate Authority), you need an infrastructure that consists of considerable operational elements, hardware, software, policy frameworks and practice statements, auditing, security infrastructure and personnel.

NEW QUESTION: 519
An organization's policy requires users to create passwords with an uppercase letter, lowercase letter, number, and symbol. This policy is enforced with technical controls, which also prevents users from using any of their previous 12 passwords. The quantization does not use single sign-on, nor does it centralize storage of passwords.
The incident response team recently discovered that passwords for one system were compromised. Passwords for a completely separate system have NOT been compromised, but unusual login activity has been detected for that separate system. Account login has been detected for users who are on vacation.
Which of the following BEST describes what is happening?
A. The compromised password file has been brute-force hacked, and the complexity requirements are not adequate to mitigate this risk.
B. The password history enforcement is insufficient, and old passwords are still valid across many different systems.
C. Some users are meeting password complexity requirements but not password length requirements.
D. Some users are reusing passwords, and some of the compromised passwords are valid on multiple systems.
Answer: (SHOW ANSWER)

NEW QUESTION: 520
Ann, a user, reports she is unable to access an application from her desktop. A security analyst verifies Ann's access and checks the SIEM for any errors. The security analyst reviews the log file from Ann's system and notices the following output:
Which of the following is MOST likely preventing Ann from accessing the application from the desktop?
A. DLP
B. Host-based firewall
C. Network-based firewall
D. Web application firewall
E. UTM
Answer: B (LEAVE A REPLY)

NEW QUESTION: 521
User from two organizations, each with its own PKI, need to begin working together on a joint project. Which of the following would allow the users of the separate PKIs to work together without connection errors?
A. Stapling
B. Trust model
C. Key escrow

D. Intermediate CA
Answer: B (LEAVE A REPLY)

NEW QUESTION: 522
Upon entering an incorrect password, the logon screen displays a message informing the user that the password does not match the username provided and is not the required length of 12 characters.
Which of the following secure coding techniques should a security analyst address with the application developers to follow security best practices?
A. Input validation
B. Error handling
C. Obfuscation
D. Data exposure
Answer: (SHOW ANSWER)

NEW QUESTION: 523
A security administrator is given the security and availability profiles for servers that are being deployed.
Match each RAID type with the correct configuration and MINIMUM number of drives.
Review the server profiles and match them with the appropriate RAID type based on integrity, availability, I/O, storage requirements. Instructions:
All drive definitions can be dragged as many times as necessary
Not all placeholders may be filled in the RAID configuration boxes
If parity is required, please select the appropriate number of parity checkboxes Server profiles may be dragged only once If at any time you would like to bring back the initial state of the simulation, please select the Reset button. When you have completed the simulation, please select the Done button to submit. Once the simulation is submitted, please select the Next button to continue.
Answer:

NEW QUESTION: 524
Due to regulatory requirements, server in a global organization must use time synchronization.
Which of the following represents the MOST secure method of time synchronization?
A. The server should connect to external Stratum 0 NTP servers for synchronization
B. The server should connect to internal Stratum 0 NTP servers for synchronization
C. The server should connect to external Stratum 1 NTP servers for synchronization
D. The server should connect to external Stratum 1 NTP servers for synchronization
Answer: B (LEAVE A REPLY)
Configure your own Internal NTP hierarchical service for your network. It is possible to purchase Stratum 1 or Stratum 0 NTP appliances to use internally for less than the cost of a typical server.

It is also possible to set up a private NTP server at a very low cost. The feasibility of setting up a commercial off the shelf (COTS) NTP server is evidenced in a recent effort to configure a Raspberry Pi computer as a Stratum-1 server. If you do decide to configure you own, please consider the following best practices:
Standardize to UTC time. Within an enterprise, standardize all systems to coordinated universal time (UTC).
Standardizing to UTC simplifies log correlation within the organization and with external parties no matter what time zone the device being synchronized is located in.
Securing the network time service. Restrict the commands that can be used on the stratum servers. Do not allow public queries of the stratum servers. Only allow known networks/hosts to communicate with their respective stratum servers.
Consider the business need for cryptography. Many administrators try to secure their networks with encrypted communications and encrypted authentication. I would introduce a note of caution here because although there are cryptographic services associated with NTP for securing NTP communications, the use of encryption introduces more sources for problems, such as requiring key management, and it also requires a higher computational overhead.
Remember Segal's Law. Ideally, it would work to have three or more Stratum 0 or Stratum 1 servers and use those servers as primary masters. Remember Segal's Law: having two NTP servers makes it hard to know which one is accurate. Two Stratum 0 servers would provide a more accurate timestamp because they are using a time source that is considered definitive.

NEW QUESTION: 525
An organization wishes to provide better security for its name resolution services. Which of the following technologies BEST supports the deployment of DNSSEC at the organization?
A. TPM
B. SSL
C. PKI
D. LDAP
E. TLS
Answer: (SHOW ANSWER)

NEW QUESTION: 526
An audit reported has identifies a weakness that could allow unauthorized personnel access to the facility at its main entrance and from there gain access to the network. Which of the following would BEST resolve the vulnerability?
A. Bollards
B. Faraday cage
C. Air gap
D. Mantrap
Answer: D (LEAVE A REPLY)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 527
In a corporation where compute utilization spikes several times a year, the Chief Information Officer (CIO) has requested a cost-effective architecture to handle the variable capacity demand. Which of the following characteristics BEST describes what the CIO has requested?
A. Elasticity
B. Scalability
C. High availability
D. Redundancy
:
Elasticity is defined as "the degree to which a system is able to adapt to workload changes by provisioning and de-provisioning resources in an autonomic manner, such that at each point in time the available resources match the current demand as closely as possible".
Answer: (SHOW ANSWER)

NEW QUESTION: 528
A security engineer wants to add SSL to the public web server. Which of the following would be the FIRST step to implement the SSL certificate?
A. Encrypt the private key
B. Download the web certificate
C. Install the intermediate certificate
D. Generate a CSR
Answer: D (LEAVE A REPLY)

NEW QUESTION: 529
A network administrator at a small office wants to simplify the configuration of mobile clients connecting to an encrypted wireless network. Which of the following should be implemented if the administrator does not want to provide the wireless password or certificate to the employees?
A. WPA2-PSK
B. TKIP
C. 802.1x
Answer: B (LEAVE A REPLY)

NEW QUESTION: 530
An organization needs to implement more stringent controls over administrator/root credentials and service accounts Requirements for the project include:
Check-in/checkout of credentials
* The ability to use but not know the password
* Automated password changes
* Logging of access to credentials
Which of the following solutions would meet the requirements?
A. A privileged access management system
B. An OpenID Connect authentication system
C. GAuth 2.0
D. Secure Enclave
E. A password vault system
Answer: (SHOW ANSWER)

NEW QUESTION: 531
Which of the following incident response steps involves actions to protect critical systems while maintaining business operations?
A. Recovery
B. Containment
C. Lessons learned
D. Investigation
Answer: B (LEAVE A REPLY)

NEW QUESTION: 532
A security analyst is implementing PKI-based functionality to a web application that has the following requirements:
- File contains certificate information
- Certificate chains
- Root authority certificates
- Private key
All of these components will be part of one file and cryptographically protected with a password.
Given this scenario, which of the following certificate types should the analyst implement to BEST meet these requirements?
A. .der certificate
B. .crt certificate
C. .cer certificate
D. .pfx certificate
Answer: D (LEAVE A REPLY)

NEW QUESTION: 533

The help desk received a call after hours from an employee who was attempting to log into the payroll server remotely. When the help desk returned the call the next morning, the employee was able to log into the server remotely without incident. However, the incident occurred again the next evening. Which of the following BEST describes the cause of the issue?

A. The password expired on the account and needed to be reset

B. Time-of-day restrictions prevented the account from logging in

C. The employee's account was locked out and needed to be unlocked

D. The employee does not have the rights needed to access the database remotely

Answer: B (LEAVE A REPLY)

NEW QUESTION: 534

Which of the following is an important step to take BEFORE moving any installation packages from a test environment to production?

A. Archive and compress the files

B. Update the secure baseline

C. Verify the hashes of files

D. Roll back changes in the test environment

Answer: D (LEAVE A REPLY)

NEW QUESTION: 535

During a third-party audit, it is determined that a member of the firewall team can request, approve, and implement a new rule-set on the firewall. Which of the following will the audit team most l likely recommend during the audit out brief?

A. Least privilege for the firewall team

B. Mandatory access control for the firewall team

C. Discretionary access control for the firewall team

D. Separation of duties policy for the firewall team

Answer: (SHOW ANSWER)

NEW QUESTION: 536

For each of the given items, select the appropriate authentication category from the dropdown choices.

Instructions: When you have completed the simulation, please select the Done button to submit.

Answer:

Explanation

Something you are includes fingerprints, retina scans, or voice recognition.

Something you have includes smart cards, token devices, or keys.

Something you know includes a password, codes, PINs, combinations, or secret phrases.

Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.

Something

you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

NEW QUESTION: 537
A technician suspects that a desktop was compromised with a rootkit. After removing lhe hard drive from the desktop and running an offline le integrity check, the technician reviews the following output:
Based on the above output, which of the following is the malicious file?
A. kernel.dll
B. lsass.exe
C. httpd.axe
D. notepad.exe
Answer: A (LEAVE A REPLY)

NEW QUESTION: 538
A system's administrator has finished configuring firewall ACL to allow access to a new web server.
The security administrator confirms form the following packet capture that there is network traffic from the internet to the web server:
The company's internal auditor issues a security finding and requests that immediate action be taken. With which of the following is the auditor MOST concerned?
A. Clear text credentials
B. Default configuration
C. Misconfigured firewall
D. Implicit deny
Answer: A (LEAVE A REPLY)

NEW QUESTION: 539
Multiple organizations operating in the same vertical want to provide seamless wireless access for their employees as they visit the other organizations. Which of the following should be implemented if all the organizations use the native 802.1x client on their mobile devices?
A. Shibboleth
B. RADIUS federation
C. SAML
D. OAuth
E. OpenID connect
Answer: (SHOW ANSWER)
Explanation/Reference:
Explanation: http://archive.oreilly.com/pub/a/wireless/2005/01/01/authentication.html

NEW QUESTION: 540
Which of the following BEST describes an important security advantage yielded by implementing vendor diversity?
A. Homogeneity
B. Sustainability
C. Configurability
D. Resiliency
Answer: B (LEAVE A REPLY)

NEW QUESTION: 541
For each of the given items, select the appropriate authentication category from the dropdown choices.
Instructions: When you have completed the simulation, please select the Done button to submit.
Answer:
Explanation
Something you are includes fingerprints, retina scans, or voice recognition.
Something you have includes smart cards, token devices, or keys.
Something you know includes a password, codes, PINs, combinations, or secret phrases.
Somewhere you are including a physical location s or logical addresses, such as domain name, an IP address, or a MAC address.
Something
you do includes your typing rhythm, a secret handshake, or a private knock
http://en.wikipedia.org/wiki/Password_authentication_protocol#Working_cycle
http://en.wikipedia.org/wiki/Smart_card#Security

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 542
Drag and drop the correct protocol to its default port.
Answer:
Explanation:
FTP uses TCP port 21. Telnet uses port 23.
SSH uses TCP port 22.

All protocols encrypted by SSH, including SFTP, SHTTP, SCP, SExec, and slogin, also use TCP port 22. Secure Copy Protocol (SCP) is a secure file-transfer facility based on SSH and Remote Copy Protocol (RCP).
Secure FTP (SFTP) is a secured alternative to standard File Transfer Protocol (FTP). SMTP uses TCP port 25.
Port 69 is used by TFTP.
SNMP makes use of UDP ports 161 and 162.
http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NEW QUESTION: 543
After discovering the /etc/shadow file had been rewritten, a security administrator noticed an application insecurely creating files in / tmp.
Which of the following vulnerabilities has MOST likely been exploited?
A. Privilege escalation
B. Resource exhaustion
C. Memory leak
D. Pointer dereference
Answer: (SHOW ANSWER)

Valid SY0-501 Dumps shared by Actual4test.com for Helping Passing SY0-501 Exam! Actual4test.com now offer the **newest SY0-501 exam dumps**, the Actual4test.com SY0-501 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com SY0-501 dumps with Test Engine here: https://www.actual4test.com/SY0-501_examcollection.html (**715** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)