ITCertTest

ITCERTTEST
IT Exam study guide / simulations

http://www.itcerttest.com

IT exam study guide / simulations

Exam : **SY0-401**

Title : CompTIA Security+ Certification

Vendor : CompTIA

Version : DEMO

NO.1 Users are utilizing thumb drives to connect to USB ports on company workstations. A technician is concerned that sensitive files can be copied to the USB drives. Which of the following mitigation techniques would address this concern? (Select TWO).

A. Disable the USB root hub within the OS.

B. Install anti-virus software on the USB drives.

C. Disable USB within the workstations BIOS.

D. Apply the concept of least privilege to USB devices.

E. Run spyware detection against all workstations.

Answer: A,C

Explanation:

A: The USB root hub can be disabled from within the operating system.

C: USB can also be configured and disabled in the system BIOS.

NO.2 Recently clients are stating they can no longer access a secure banking site's webpage. In reviewing the clients' web browser settings, the certificate chain is showing the following:

Certificate Chain:

X Digi Cert

Digi Cert High assurance C3

* banksite.com

Certificate Store:

Digi Cert - Others Certificate Store

Digi Cert High assurance C3 - Others Certificate Store

Based on the information provided, which of the following is the problem when connecting to the website?

A. The certificate signature request was invalid

B. Key escrow is failing for the certificate authority

C. The certificate authority has revoked the certificate

D. The clients do not trust the certificate authority

Answer: C

NO.3 Joe, the Chief Technical Officer (CTO), is concerned about new malware being introduced into the corporate network. He has tasked the security engineers to implement a technology that is capable of alerting the team when unusual traffic is on the network.

Which of the following types of technologies will BEST address this scenario?

A. Application Firewall

B. Anomaly Based IDS

C. Proxy Firewall

D. Signature IDS

Answer: B

Explanation:

Anomaly-based detection watches the ongoing activity in the environment and looks for abnormal occurrences. An anomaly-based monitoring or detection method relies on definitions of all valid forms of activity. This database of known valid activity allows the tool to detect any and all anomalies. Anomaly-based detection is commonly used for protocols.

Because all the valid and legal forms of a protocol are known and can be defined, any variations from those known valid constructions are seen as anomalies.

NO.4 After a merger between two companies a security analyst has been asked to ensure that the organization's systems are secured against infiltration by any former employees that were terminated during the transition. Which of the following actions are MOST appropriate to harden applications against infiltration by former employees? (Select TWO)

A. Monitor VPN client access

B. Reduce failed login out settings

C. Develop and implement updated access control policies

D. Review and address invalid login attempts

E. Increase password complexity requirements

F. Assess and eliminate inactive accounts

Answer: E,F

NO.5 A company has recently allowed employees to take advantage of BYOD by installing WAPs throughout the corporate office. An employee, Joe, has recently begun to view inappropriate material at work using his personal laptop. When confronted, Joe indicated that he was never told that he could not view that type of material on his personal laptop.
Which of the following should the company have employees acknowledge before allowing them to access the corporate WLAN with their personal devices?

A. Privacy Policy

B. Security Policy

C. Consent to Monitoring Policy

D. Acceptable Use Policy

Answer: D

Explanation:
Acceptable use policies (AUPs) describe how the employees in an organization can use company systems and resources, both software and hardware.

NO.6 Which of the following is a directional antenna that can be used in point-to-point or point-to-multi-point WiFi communication systems? (Select TWO).

A. Backfire

B. Dipole

C. Omni

D. PTZ

E. Dish

Answer: A,E

Explanation:
Both the Backfire and the Dish antennae are high gain antenna types that transmit a narrow beam of signal. It can therefore be used as a point-to-point antenna over short distances, but as point-to-multi-point antenna over longer distances.

NO.7 A security administrator develops a web page and limits input into the fields on the web page

as well as filters special characters in output. The administrator is trying to prevent which of the following attacks?

A. Spoofing

B. XSS

C. Fuzzing

D. Pharming

Answer: B

Explanation:

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. Cross-site scripting uses known vulnerabilities in web-based applications, their servers, or plug-in systems on which they rely. Exploiting one of these, attackers fold malicious content into the content being delivered from the compromised site. When the resulting combined content arrives at the client-side web browser, it has all been delivered from the trusted source, and thus operates under the permissions granted to that system. By finding ways of injecting malicious scripts into web pages, an attacker can gain elevated access- privileges to sensitive page content, session cookies, and a variety of other information maintained by the browser on behalf of the user.

By validating user input and preventing special characters, we can prevent the injection of client-side scripting code.

NO.8 Which of the following types of cloud computing would be MOST appropriate if an organization required complete control of the environment?

A. Hybrid Cloud

B. Private cloud

C. Community cloud

D. Community cloud

E. Public cloud

Answer: B

NO.9 Which of the following best practices makes a wireless network more difficult to find?

A. Implement MAC filtering

B. UseWPA2-PSK

C. Disable SSID broadcast

D. Power down unused WAPs

Answer: C

Explanation:

Network administrators may choose to disable SSID broadcast to hide their network from unauthorized personnel. However, the SSID is still needed to direct packets to and from the base station, so it's a discoverable value using a wireless packet sniffer. Thus, the SSID should be disabled if the network isn't for public use.

NO.10 Which of the following are Data Loss Prevention (DLP) strategies that address data in transit issues? (Select TWO).

A. Scanning printing of documents.

B. Scanning of outbound IM (Instance Messaging).
C. Scanning copying of documents to USB.
D. Scanning of SharePoint document library.
E. Scanning of shared drives.
F. Scanning of HTTP user traffic.
Answer: B,F
Explanation:
DLP systems monitor the contents of systems (workstations, servers, networks) to make sure key content is not deleted or removed. They also monitor who is using the data (looking for unauthorized access) and transmitting the data. Outbound IM and HTTP user traffic refers to data over a network which falls within the DLP strategy.

NO.11 Key cards at a bank are not tied to individuals, but rather to organizational roles. After a break in, it becomes apparent that extra efforts must be taken to successfully pinpoint who exactly enters secure areas. Which of the following security measures can be put in place to mitigate the issue until a new key card system can be installed?
A. Bollards
B. Video surveillance
C. Proximity readers
D. Fencing
Answer: B
Explanation:
Video surveillance is making use of a camera, or CCTV that is able to record everything it sees and is always running. This way you will be able to check exactly who enters secure areas.

NO.12 A security technician is concerned there4 is not enough security staff available the web servers and database server located in the DMZ around the clock. Which of the following technologies, when deployed, would provide the BEST round the clock automated protection?
A. HIPS & SIEM
B. NIPS & HIDS
C. HIDS& SIEM
D. NIPS&HIPS
Answer: B

NO.13 Several users' computers are no longer responding normally and sending out spam email to the users' entire contact list. This is an example of which of the following?
A. Trojan virus
B. Botnet
C. Worm outbreak
D. Logic bomb
Answer: C
Explanation:
A worm is similar to a virus but is typically less malicious. A virus will usually cause damage to the system or files whereas a worm will usually just spread itself either using the network or by sending

emails.
A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

NO.14 Ann, a security administrator is hardening the user password policies. She currently has the following in place.
Passwords expire every 60 days
Password length is at least eight characters
Passwords must contain at least one capital letter and one numeric character Passwords cannot be reused until the password has been changed eight times She learns that several employees are still using their original password after the 60-day forced change. Which of the following can she implement to BEST mitigate this?
A. Lower the password expiry time to every 30days instead of every 60 days
B. Require that the password contains at least one capital, one numeric, and one special character
C. Change the re-usage time from eight to 16 changes before a password can be repeated
D. Create a rule that users can only change their passwords once every two weeks
Answer: D

NO.15 A system security analyst wants to capture data flowing in and out of the enterprise. Which of the following would MOST likely help in achieving this goal?
A. Taking screenshots
B. Analyzing Big Data metadata
C. Analyzing network traffic and logs
D. Capturing system image
Answer: C

NO.16 Which of the following is used by the recipient of a digitally signed email to verify the identity of the sender?
A. Recipient's private key
B. Sender's public key
C. Recipient's public key
D. Sender's private key
Answer: B
Explanation:
When the sender wants to send a message to the receiver. It's important that this message not be altered. The sender uses the private key to create a digital signature. The message is, in effect, signed with the private key. The sender then sends the message to the receiver. The recipient uses the public key attached to the message to validate the digital signature. If the values match, the receiver knows the message is authentic. Thus the recipient uses the sender's public key to verify the sender's identity.

NO.17 Users at a company report that a popular news website keeps taking them to a web page with derogatory content. This is an example of which of the following?

A. Evil twin

B. DNS poisoning

C. Vishing

D. Session hijacking

Answer: B

Explanation:

DNS spoofing (or DNS cache poisoning) is a computer hacking attack, whereby data is introduced into a Domain Name System (DNS) resolver's cache, causing the name server to return an incorrect IP address, diverting traffic to the attacker's computer (or any other computer).

A domain name system server translates a human-readable domain name (such as example.com) into a numerical IP address that is used to route communications between nodes. Normally if the server doesn't know a requested translation it will ask another server, and the process continues recursively. To increase performance, a server will typically remember (cache) these translations for a certain amount of time, so that, if it receives another request for the same translation, it can reply without having to ask the other server again.

When a DNS server has received a false translation and caches it for performance optimization, it is considered poisoned, and it supplies the false data to clients. If a DNS server is poisoned, it may return an incorrect IP address, diverting traffic to another computer (in this case, the server hosting the web page with derogatory content).

NO.18 Which of the following statements is MOST likely to be included in the security awareness training about P2P?

A. P2P is always used to download copyrighted material.

B. P2P can be used to improve computer system response.

C. P2P may prevent viruses from entering the network.

D. P2P may cause excessive network bandwidth.

Answer: D

Explanation:

P2P networking by definition involves networking which will reduce available bandwidth for the rest of the users on the network.

NO.19 A security analyst needs to ensure all external traffic is able to access the company's front-end servers but protect all access to internal resources. Which of the following network design elements would MOST likely be recommended?

A. DMZ

B. Cloud computing

C. VLAN

D. Virtualization

Answer: A

Explanation:

A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access. The DMZ is a buffer network between the public untrusted Internet and the private trusted

LAN. Often a DMZ is deployed through the use of a multihomed firewall.

NO.20 The Chief Technology Officer (CTO) wants to improve security surrounding storage of customer passwords.
The company currently stores passwords as SHA hashes. Which of the following can the CTO implement requiring the LEAST change to existing systems?

A. Smart cards

B. TOTP

C. Key stretching

D. Asymmetric keys

Answer: A

Explanation:
Smart cards usually come in two forms. The most common takes the form of a rectangular piece of plastic with an embedded microchip. The second is as a USB token. It contains a built in processor and has the ability to securely store and process information. A "contact" smart card communicates with a PC using a smart card reader whereas a "contactless" card sends encrypted information via radio waves to the PC.
Typical scenarios in which smart cards are used include interactive logon, e-mail signing, e-mail decryption and remote access authentication. However, smart cards are programmable and can contain programs and data for many different applications. For example smart cards may be used to store medical histories for use in emergencies, to make electronic cash payments or to verify the identity of a customer to an e-retailer.
Microsoft provides two device independent APIs to insulate application developers from differences between current and future implementations: CryptoAPI and Microsoft Win32 SCard APIs.
The Cryptography API contains functions that allow applications to encrypt or digitally sign data in a flexible manner, while providing protection for the user's sensitive private key data. All cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs).
There are many different cryptographic algorithms and even when implementing the same algorithm there are many choices to make about key sizes and padding for example. For this reason, CSPs are grouped into types, in which each supported CryptoAPI function, by default, performs in a way particular to that type. For example, CSPs in the PROV_DSS provider type support DSS Signatures and MD5 and SHA hashing.

NO.21 Ann, a security technician, is reviewing the IDS log files. She notices a large number of alerts for multicast packets from the switches on the network. After investigation, she discovers that this is normal activity for her network. Which of the following BEST describes these results?

A. True negatives

B. True positives

C. False positives

D. False negatives

Answer: C

Explanation:
False positives are essentially events that are mistakenly flagged and are not really events to be concerned about.

NO.22 Which of the following is an attack vector that can cause extensive physical damage to a datacenter without physical access?

A. CCTV system access

B. Dial-up access

C. Changing environmental controls

D. Ping of death

Answer: C

Explanation:

Environmental systems include heating, air conditioning, humidity control, fire suppression, and power systems. All of these functions are critical to a well-designed physical plant. A computer room will typically require full-time environmental control. Changing any of these controls (when it was set to its optimum values) will result in damage.

NO.23 Which of the following protocols operates at the HIGHEST level of the OSI model?

A. ICMP

B. IPSec

C. SCP

D. TCP

Answer: C

Explanation:

SCP (Secure Copy) uses SSH (Secure Shell). SSH runs in the application layer (layer 7) of the OSI model.

NO.24 A security administrator is responsible for performing periodic reviews of user permission settings due to high turnover and internal transfers at a corporation. Which of the following BEST describes the procedure and security rationale for performing such reviews?

A. Review all user permissions and group memberships to ensure only the minimum set of permissions required to perform a job is assigned.

B. Review the permissions of all transferred users to ensure new permissions are granted so the employee can work effectively.

C. Ensure all users have adequate permissions and appropriate group memberships, so the volume of help desk calls is reduced.

D. Ensure former employee accounts have no permissions so that they cannot access any network file stores and resources.

Answer: A

Explanation:

Reviewing user permissions and group memberships form part of a privilege audit is used to determine that all groups, users, and other accounts have the appropriate privileges assigned according to the policies of the corporation.

NO.25 A developer needs to utilize AES encryption in an application but requires the speed of encryption and decryption to be as fast as possible. The data that will be secured is not sensitive so speed is valued over encryption complexity. Which of the following would BEST satisfy these requirements?

A. AES with output feedback
B. AES with cipher feedback
C. AES with cipher block chaining
D. AES with counter mode
Answer: B

NO.26 Which of the following would a security administrator implement in order to identify change from the standard configuration on a server?
A. Penetration test
B. Code review
C. Baseline review
D. Design review
Answer: C
Explanation:
The standard configuration on a server is known as the baseline.
The IT baseline protection approach is a methodology to identify and implement computer security measures in an organization. The aim is the achievement of an adequate and appropriate level of security for IT systems. This is known as a baseline.
A baseline report compares the current status of network systems in terms of security updates, performance or other metrics to a predefined set of standards (the baseline).

NO.27 Which of the following can hide confidential or malicious data in the whitespace of other files (e.g. JPEGs)?
A. Hashing
B. Transport encryption
C. Digital signatures
D. Steganography
Answer: D
Explanation:
Steganography is the process of concealing a file, message, image, or video within another file, message, image, or video.
Note: The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages, no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message.

NO.28 Which of the following types of application attacks would be used to identify malware causing security breaches that have NOT yet been identified by any trusted sources?
A. Zero-day
B. LDAP injection
C. XML injection
D. Directory traversal

Answer: A
Explanation:
The security breaches have NOT yet been identified. This is zero day vulnerability.
A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it-this exploit is called a zero day attack. Uses of zero day attacks can include infiltrating malware, spyware or allowing unwanted access to user information. The term
"zero day" refers to the unknown nature of the hole to those outside of the hackers, specifically, the developers. Once the vulnerability becomes known, a race begins for the developer, who must protect users.

NO.29 An administrator is configuring a new Linux web server where each user account is confined to a cheroot jail. Which of the following describes this type of control?
A. SysV
B. Sandbox
C. Zone
D. Segmentation
Answer: B

NO.30 Jo an employee reports to the security manager that several files in a research and development folder that only JOE has access to have been improperly modified. The modified data on the files in recent and the modified by account is Joe's. The permissions on the folder have not been changed, and there is no evidence of malware on the server hosting the folder or on Joe's workstation. Several failed login attempts to Joe's account were discovered in the security log of the LDAP server. Given this scenario, which of the following should the security manager implement to prevent this in the future?
A. Generic account prohibition
B. Account lockout
C. Password complexity
D. User access reviews
Answer: B

NO.31 A software company sends their offsite backup tapes to a third party storage facility. TO meet confidentiality the tapes should be:
A. Labeled
B. Hashed
C. Encrypted
D. Duplicated
Answer: A

NO.32 Which of the following BEST explains the use of an HSM within the company servers?
A. Thumb drives present a significant threat which is mitigated by HSM.
B. Software encryption can perform multiple functions required by HSM.
C. Data loss by removable media can be prevented with DLP.

D. Hardware encryption is faster than software encryption.

Answer: D

Explanation:

Hardware Security Module (HSM) is a cryptoprocessor that can be used to enhance security. It provides a fast solution for the for large asymmetrical encryption calculations and is much faster than software-based cryptographic solutions.

NO.33 Which of the following types of encryption will help in protecting files on a PED?

A. Mobile device encryption

B. Transport layer encryption

C. Encrypted hidden container

D. Database encryption

Answer: A

Explanation:

Device encryption encrypts the data on a Personal Electronic Device (PED). This feature ensures that the data on the device cannot be accessed in a useable form should the device be stolen.

NO.34 Company employees are required to have workstation client certificates to access a bank website. These certificates were backed up as a precautionary step before the new computer upgrade. After the upgrade and restoration, users state they can access the bank's website, but not login. Which is the following is MOST likely the issue?

A. The IP addresses of the clients have change

B. The client certificate passwords have expired on the server

C. The certificates have not been installed on the workstations

D. The certificates have been installed on the CA

Answer: C

Explanation:

The computer certificates must be installed on the upgraded client computers.

NO.35 A recent audit of a company's identity management system shows that 30% of active accounts belong to people no longer with the firm. Which of the following should be performed to help avoid this scenario? (Select TWO).

A. Automatically disable accounts that have not been utilized for at least 10 days.

B. Utilize automated provisioning and de-provisioning processes where possible.

C. Request that employees provide a list of systems that they have access to prior to leaving the firm.

D. Perform regular user account review / revalidation process.

E. Implement a process where new account creations require management approval.

Answer: B,D

Explanation:

Provisioning and de-provisioning processes can occur manually or automatically. Since the manual processes are so time consuming, the automated option should be used as it is more efficient. Revalidating user accounts would determine which users are no longer active.

NO.36 A Windows-based computer is infected with malware and is running too slowly to boot and

run a malware scanner. Which of the following is the BEST way to run the malware scanner?

A. Kill all system processes

B. Enable the firewall

C. Boot from CD/USB

D. Disable the network connection

Answer: C

Explanation:

Antivirus companies frequently create boot discs you can use to scan and repair your computer. These tools can be burned to a CD or DVD or installed onto a USB drive. You can then restart your computer and boot from the removable media. A special antivirus environment will load where your computer can be scanned and repaired.

Incorrect Options:

A: Kill all system processes will stop system processes, and could have a negative effect on the system. It is not the BEST way to run the malware scanner B: The basic purpose of a firewall is to isolate one network from another. It is not the BEST way to run the malware scanner.

D: Disabling the network connection will not allow for the BEST way to run the malware scanner.

Reference:

http://www.howtogeek.com/187037/how-to-scan-and-repair-a-badly-infected-computer- from -outside-windows/ Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, 6th Edition, Sybex, Indianapolis, 2014, p. 342

NO.37 It is MOST difficult to harden against which of the following?

A. XSS

B. Zero-day

C. Buffer overflow

D. DoS

Answer: C

NO.38 Which of the following is considered the MOST effective practice when securing printers or scanners in an enterprise environment?

A. Routine vulnerability scanning of peripherals

B. Install in a hardened network segment

C. Turn off the power to the peripherals at night

D. Enable print sharing only from workstations

Answer: A

NO.39 A user attempts to install new and relatively unknown software recommended by a colleague. The user is unable to install the program, despite having successfully installed other programs previously. Which of the following is MOST likely the cause for the user's inability to complete the installation?

A. Application black listing

B. Network Intrusion Prevention System

C. Group policy

D. Application white listing

Answer: A

NO.40 Which of the following attacks initiates a connection by sending specially crafted packets in which multiple TCP flags are set to 1?

A. Replay

B. Smurf

C. Xmas

D. Fraggle

Answer: C