JK0-022$^{Q\&As}$

CompTIA Security+ Certification

Pass CompTIA JK0-022 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/jk0-022.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A company has several conference rooms with wired network jacks that are used by both employees and guests. Employees need access to internal resources and guests only need access to the Internet. Which of the following combinations is BEST to meet the requirements?

A. NAT and DMZ

B. VPN and IPSec

C. Switches and a firewall

D. 802.1x and VLANs

Correct Answer: D

802.1x is a port-based authentication mechanism. It\\'s based on Extensible Authentication Protocol (EAP) and is commonly used in closed-environment wireless networks. 802.1x was initially used to compensate for the weaknesses of Wired Equivalent Privacy (WEP), but today it\\'s often used as a component in more complex authentication and connection-management systems, including Remote Authentication Dial-In User Service (RADIUS), Diameter, Cisco System\\'s Terminal Access Controller Access-Control System Plus (TACACS+), and Network Access Control (NAC).

A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. By default, all ports on a switch are part of VLAN 1. But as the switch administrator changes the VLAN assignment on a port-by-port basis, various ports can be grouped together and be distinct from other VLAN port designations. VLANs are used for traffic management. Communications between ports within the same VLAN occur without hindrance, but communications between VLANs require a routing function.

Incorrect Answers:

A: NAT converts the IP addresses of internal systems found in the header of network packets into public IP addresses. A demilitarized zone (DMZ) is an area of a network that is designed specifically for public users to access.

B: A virtual private network (VPN) is a communication tunnel between two entities across an intermediary network. In most cases, the intermediary network is an untrusted network, such as the Internet, and therefore the communication tunnel is also encrypted. Internet Protocol Security (IPSec) is both a stand-alone VPN protocol and a module that can be used with L2TP.

C: A switch is a networking device used to connect other devices together and potentially implement traffic management on their communications. Firewalls manage traffic using filters.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 6, 11, 21, 23, 27, 39, 53.

QUESTION 2

After a recent breach, the security administrator performs a wireless survey of the corporate network. The security administrator notices a problem with the following output: MAC SSID ENCRYPTION POWER BEACONS 00:10:A1:36:12:CC MYCORP WPA2 CCMP 60 1202 00:10:A1:49:FC:37 MYCORP WPA2 CCMP 70 9102 FB:90:11:42:FA:99 MYCORP WPA2 CCMP 40 3031 00:10:A1:AA:BB:CC MYCORP WPA2 CCMP 55 2021 00:10:A1:FA:B1:07 MYCORP WPA2 CCMP 30 6044

Given that the corporate wireless network has been standardized, which of the following attacks is underway?

A. Evil twin

B. IV attack

C. Rogue AP

D. DDoS

Correct Answer: A

The question states that the corporate wireless network has been standardized. By `standardized\\' it means the wireless network access points are running on hardware from the same vendor. We can see this from the MAC addresses used.

The first half of a MAC address is vendor specific. The second half is network adapter specific. We have four devices with MAC addresses that start with 00:10:A1.

The "odd one out" is the device with a MAC address starting FB:90:11. This device is from a different vendor. The SSID of the wireless network on this access point is the same as the other legitimate access points. Therefore, the access

point with a MAC address starting FB:90:11 is impersonating the corporate access points. This is known as an Evil Twin.

An evil twin, in the context of network security, is a rogue or fake wireless access point (WAP) that appears as a genuine hotspot offered by a legitimate provider. In an evil twin attack, an eavesdropper or hacker fraudulently creates this rogue

hotspot to collect the personal data of unsuspecting users. Sensitive data can be stolen by spying on a connection or using a phishing technique.

For example, a hacker using an evil twin exploit may be positioned near an authentic Wi-Fi access point and discover the service set identifier (SSID) and frequency. The hacker may then send a radio signal using the exact same frequency

and SSID. To end users, the rogue evil twin appears as their legitimate hotspot with the same name.

In wireless transmissions, evil twins are not a new phenomenon. Historically, they were known as honeypots or base station clones. With the advancement of wireless technology and the use of wireless devices in public areas, it is very easy

for novice users to set up evil twin exploits.

Incorrect Answers:

B: An initialization vector is a random number used in combination with a secret key as a means to encrypt data. This number is sometimes referred to as a nonce, or "number occurring once," as an encryption program uses it only once per

session.

An initialization vector is used to avoid repetition during the data encryption process, making it impossible for hackers who use dictionary attack to decrypt the exchanged encrypted message by discovering a pattern. This is known as an IV

attack. This is not what is described in this question. Therefore, this answer is incorrect.

C: A rogue access point is a wireless access point that has either been installed on a secure company network without explicit authorization from a local network administrator, or has been created to allow a hacker to conduct a man-in-themiddle attack. Rogue access points of the first kind can pose a security threat to large organizations with many employees, because anyone with access to the premises can install (maliciously or non-maliciously) an inexpensive wireless

router that can potentially allow access to a secure network to unauthorized parties. Rogue access points of the second kind target networks that do not employ mutual authentication (client-server server-client) and may be used in

conjunction with a rogue RADIUS server, depending on security configuration of the target network. The Evil Twin in this question is a type of rogue access point. However, as the access point is impersonating the corporate network, it is

classed as an Evil Twin.

Therefore, this answer is incorrect.

D: A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems (for

example a botnet) flooding the targeted system with traffic. When a server is overloaded with connections, new connections can no longer be accepted. The major advantages to an attacker of using a distributed denial-of-service attack are

that multiple machines can generate more attack traffic than one machine, multiple attack machines are harder to turn off than one attack machine, and that the behavior of each attack machine can be stealthier, making it harder to track and

shut down. These attacker advantages cause challenges for defense mechanisms. For example, merely purchasing more incoming bandwidth than the current volume of the attack might not help, because the attacker might be able to simply

add more attack machines. This after all will end up completely crashing a website for periods of time. This is not what is described in this question.

Therefore, this answer is incorrect.

References: http://www.techopedia.com/definition/5057/evil-twin http://www.techopedia.com/definition/26858/initialization-vector http://en.wikipedia.org/wiki/Denial-of-service_attack

QUESTION 3

A system administrator has noticed that users change their password many times to cycle back to the original password when their passwords expire. Which of the following would BEST prevent this behavior?

A. Assign users passwords based upon job role.

B. Enforce a minimum password age policy.

C. Prevent users from choosing their own passwords.

D. Increase the password expiration time frame.

Correct Answer: B

A minimum password age policy defines the period that a password must be used for before it can be changed.

Incorrect Answers:

A: Assigning users passwords based upon job role is not a secure password solution.

C: Preventing users from choosing their own passwords could make remembering passwords difficult. This could lead to a user having to record a generated password somewhere that is not secure.

D: This will cause a password to be retained for a longer period.

References:

https://technet.microsoft.com/en-us/library/cc779758(v=ws.10).aspx Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 291- 293.

QUESTION 4

Which of the following is a common coding error in which boundary checking is not performed?

A. Input validation

B. Fuzzing

C. Secure coding

D. Cross-site scripting

Correct Answer: A

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

B: Fuzzing is a software testing technique that involves providing invalid, unexpected, or random data to as inputs to a computer program. The program is then monitored for exceptions such as crashes, or failed validation, or memory leaks.

C: Proper and secure coding can prevent many attacks, including cross-site scripting, SQL injection and buffer overflows.

D: Cross-site scripting (XSS) is a form of malicious code-injection attack on a web server in which an attacker injects code into the content sent to website visitors. XSS can be mitigated by implementing patch management on the web server, using firewalls, and auditing for suspicious activity

References: http://en.wikipedia.org/wiki/Fuzz_testing Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 218, 257 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 192, 229, 319

QUESTION 5

Which of the following solutions provides the most flexibility when testing new security controls prior to implementation?

A. Trusted OS

B. Host software baselining

C. OS hardening

D. Virtualization

Correct Answer: D

Virtualization is used to host one or more operating systems in the memory of a single host computer and allows multiple operating systems to run simultaneously on the same hardware. Virtualization offers the flexibility of quickly and easily making backups of entire virtual systems, and quickly recovering the virtual system when errors occur. Furthermore, malicious code compromises of virtual systems rarely affect the host system, which allows for safer testing and experimentation.

Incorrect Answers:

A: Trusted OS is an access-control feature that limits resource access to client systems that run operating system that are known to implement specific security features.

B: Application baseline defines the level or standard of security that will be implemented and maintained for the application. It may include requirements of hardware components, operating system versions, patch levels, installed applications and their configurations, and available ports and services. Systems can be compared to the baseline to ensure that the required level of security is being maintained.

C: Hardening is the process of securing a system by reducing its surface of vulnerability. Reducing the surface of vulnerability typically includes removing or disabling unnecessary functions and features, removing or disabling unnecessary user accounts, disabling unnecessary protocols and ports, and disabling unnecessary services.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 215-217 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 37, 208, 246

QUESTION 6

To protect corporate data on removable media, a security policy should mandate that all removable devices use which of the following?

A. Full disk encryption

B. Application isolation

C. Digital rights management

D. Data execution prevention

Correct Answer: A

Full-disk encryption encrypts the data on the hard drive of the device or on a removable drive. This feature ensures that the data on the device or removable drive cannot be accessed in a useable form should it be stolen.

Incorrect Answers:

B: Application Isolation is the process of ensuring that the application always uses the version of shared files with which it was installed, preventing component versioning conflicts. This is performed by the developer of the application.

C: Digital rights management (DRM) is a set of technologies used by publishers, copyright holders, and individuals to control the after-sale use of digital content, most prominently, to curb piracy of digital content.

D: Data Execution Prevention (DEP) is a security feature built into the operating system. It defines areas of memory as executable and nonexecutable. This protects against program errors, and some malicious exploits, such as buffer overflows.

References: Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 251-
http://www.symantec.com/connect/articles/application-isolation- basics-and-directions
http://en.wikipedia.org/wiki/Digital_rights_management http://en.wikipedia.org/wiki/Data_Execution_Prevention

QUESTION 7

Sara, a security manager, has decided to force expiration of all company passwords by the close of business day. Which of the following BEST supports this reasoning?

A. A recent security breach in which passwords were cracked.

B. Implementation of configuration management processes.

C. Enforcement of password complexity requirements.

D. Implementation of account lockout procedures.

Correct Answer: A

A password only needs to be changed if it doesn\\'t meet the compliance requirements of the company\\'s password policy, or is evidently insecure. It will also need to be changed if it has been reused, or due to possible compromise as a result of a system intrusion.

Incorrect Answers:

B: Configuration management provides visibility and control of a system\\'s performance, as well as its functional and physical attributes.

C: Password complexity normally requires a minimum of three out of four standard character types to be represented in the password. It would not require forcing expiration of all company passwords by the close of business day.

D: Account lockout automatically disables an account due to repeated failed log on attempts. It would not require forcing expiration of all company passwords by the close of business day.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 292, 293.

http://en.wikipedia.org/wiki/Configuration_management

QUESTION 8

In which of the following steps of incident response does a team analyse the incident and determine steps to prevent a future occurrence?

A. Mitigation

B. Identification

C. Preparation

D. Lessons learned

Correct Answer: D

Incident response procedures involves in chronological order: Preparation; Incident identification; Escalation and notification; Mitigation steps; Lessons learned; Reporting; Recover/reconstitution procedures; First responder; Incident isolation (Quarantine; Device removal); Data breach; Damage and loss control. Thus lessons are only learned after the mitigation occurred. For only then can you `step back\\' and analyze the incident to prevent the same occurrence in future.

Incorrect Answers:

A: Mitigation is accomplished anytime that any steps has been taken to reduce risk.

B: When responding to an incident the identification of the incident is essential to know how to handle the incident and then take steps. This happens way before an incident is analyzed to determine which steps to take to prevent the same occurrence in future.

C: Preparation involves all the preventative measures that are taken to prevent any risk incident. This does not means that an incident already occurred as is alluded to in the question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 429

QUESTION 9

A new virtual server was created for the marketing department. The server was installed on an existing host machine. Users in the marketing department report that they are unable to connect to the server. Technicians verify that the server has an IP address in the same VLAN as the marketing department users. Which of the following is the MOST likely reason the users are unable to connect to the server?

A. The new virtual server\\'s MAC address was not added to the ACL on the switch

B. The new virtual server\\'s MAC address triggered a port security violation on the switch

C. The new virtual server\\'s MAC address triggered an implicit deny in the switch

D. The new virtual server\\'s MAC address was not added to the firewall rules on the switch

Correct Answer: A

Configuring the switch to allow only traffic from computers based upon their physical address is known as MAC filtering. The physical address is known as the MAC address. Every network adapter has a unique MAC address hardcoded into the adapter. You can configure the ports of a switch to allow connections from computers with specific MAC addresses only and block all other MAC addresses.

In computer networking, MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network.

MAC addresses are uniquely assigned to each card, so using MAC filtering on a network permits and denies network access to specific devices through the use of blacklists and whitelists. While the restriction of network access through the

use of lists is straightforward, an individual person is not identified by a MAC address, rather a device only, so an authorized person will need to have a whitelist entry for each device that he or she would use to access the network.

Incorrect Answers:

B: The new virtual server\\'s MAC address triggering a port security violation on the switch may happen if the MAC address was not added to the ACL on the switch. However, the port security violation is not the actual cause of the users being

unable to connect to the server. The MAC address not being added to the ACL on the switch is what would prevent the users connecting to the server. Therefore this answer is incorrect.

C: The new virtual server\\'s MAC address triggering an implicit deny in the switch would happen if the MAC address met a condition that caused the deny. This is unlikely. The MAC address not being added to the ACL on the switch to allow

access if more likely. Therefore this answer is incorrect.

D: Dedicated network switches don\\'t tend to have firewalls. A typical home wireless router may function as a switch and a firewall. However, even in this case, the firewall typically wouldn\\'t prevent communications between devices connected

to the switch. This answer is very unlikely and is therefore incorrect.

References:

http://en.wikipedia.org/wiki/MAC_filtering

QUESTION 10

RC4 is a strong encryption protocol that is generally used with which of the following?

A. WPA2 CCMP

B. PEAP

C. WEP

D. EAP-TLS

Correct Answer: C

QUESTION 11

Without validating user input, an application becomes vulnerable to all of the following EXCEPT: A. Buffer overflow.

B. Command injection.

C. Spear phishing.

D. SQL injection.

Correct Answer: C

Input validation is a defensive technique intended to mitigate against possible user input attacks, such as buffer overflows and fuzzing. Input validation checks every user input submitted to the application before processing that input. The check could be a length, a character type, a language type, or a domain.

Incorrect Answers:

A: Buffer overflow is an exploit at programming error, bugs and flaws. It occurs when an application is fed more input data than it is programmed to handle. This may cause the application to terminate or to write data beyond the end of the allocated space in memory. The termination of the application may cause the system to send the data with temporary access to privileged levels in the system, while overwriting can cause important data to be lost. Proper error and exception handling and input validation will help prevent Buffer overflow exploits.

B: Command injection is often used to gain access to restricted directories on a web server. Proper input validation will help prevent command injection attacks.

D: SQL injection attacks use unexpected input to a web application to gain access to the database used by web application. You can protect a web application against SQL injection by implementing input validation and by limiting database account privileges for the account used by the web server and the web application.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 257, 337, 338 Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 195- 196, 197, 319

QUESTION 12

During an audit, the security administrator discovers that there are several users that are no longer employed with the company but still have active user accounts. Which of the following should be performed?

A. Account recovery

B. Account disablement

C. Account lockouts

D. Account expiration

Correct Answer: B

Account Disablement should be implemented when a user will be gone from a company whether they leave temporary or permanently. In the case of permanently leaving the company the account should be disabled. Disablement means that the account will no longer be an active account.

Incorrect Answers:

A: Account recovery is usually done in cases where users have forgotten their password which they use to access their accounts. In this case the users have left the employment of the company.

C: The need to lock an account occurs when a user is attempting to log in but giving incorrect values; locking this account is necessary to prevent a would-be attacker from repeatedly guessing at password values until they find a match.

D: Account expiration is implemented when you want to force users to change their password to access their accounts on a regular basis. References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 140, 141.

QUESTION 13

While opening an email attachment, Pete, a customer, receives an error that the application has encountered an unexpected issue and must be shut down. This could be an example of which of the following attacks?

A. Cross-site scripting

B. Buffer overflow

C. Header manipulation

D. Directory traversal

Correct Answer: B

When the user opens an attachment, the attachment is loaded into memory. The error is caused by a memory issue due to a buffer overflow attack.

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user\\'s files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: 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. As XSS is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

C: A header manipulation attack uses other methods (hijacking, cross-site forgery, and so forth) to change values in HTTP headers and falsify access. When used with XSRF, the attacker can even change a user\\'s cookie. Internet Explorer 8 and above include InPrivate Filtering to help prevent some of this. By default, your browser sends information to sites as they need it--think of requesting a map from a site; it needs to know your location in order to give directions. With InPrivate Filtering, you can configure the browser not to share information that can be captured and manipulated. As header manipulation is a web based attack, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

D: Directory traversal is a form of HTTP exploit in which a hacker uses the software on a Web server to access data in a directory other than the server\\'s root directory. If the attempt is successful, the hacker can view restricted files or even execute commands on the server. Although some educated guesswork is involved in finding paths to restricted files on a Web server, a skilled hacker can easily carry out this type of attack on an inadequately protected server by searching through the directory tree. The risk of such attacks can be minimized by careful Web server programming, the installation of software updates and patches, filtering of input from browsers, and the use of vulnerability scanners. As directory traversal is a form of HTTP exploit, it would require the user to open a web page, not an email attachment. Therefore, this answer is incorrect.

References:

http://searchsecurity.techtarget.com/definition/buffer-overflow http://en.wikipedia.org/wiki/Cross-site_scripting Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 340 http://

searchsecurity.techtarget.com/definition/directory-traversal

QUESTION 14

A malicious individual is attempting to write too much data to an application\\'s memory. Which of the following describes this type of attack?

A. Zero-day

B. SQL injection

C. Buffer overflow

D. XSRF

Correct Answer: C

A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information - which has to go somewhere - can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Although it may occur accidentally through programming error, buffer overflow is an increasingly common type of security attack on data integrity. In buffer overflow attacks, the extra data may contain codes designed to trigger specific actions, in effect sending new instructions to the attacked computer that could, for example, damage the user\\'s files, change data, or disclose confidential information. Buffer overflow attacks are said to have arisen because the C programming language supplied the framework, and poor programming practices supplied the vulnerability.

Incorrect Answers:

A: 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. This type of attack does not attempt to write too much data to an application\\'s memory.

Therefore, this answer is incorrect.

B: SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must

exploit a security vulnerability in an application\\'s software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly

executed. SQL injection is mostly known as an attack vector for websites but can be used to attack any type of SQL database. This type of attack does not attempt to write too much data to an application\\'s memory. Therefore, this answer is

incorrect.

D: Cross-Site Request Forgery--also known as XSRF, session riding, and one-click attack-- involves unauthorized commands coming from a trusted user to the website. This is often done without the user\\'s knowledge, and it employs some

type of social networking to pull it off. For example, assume that Evan and Spencer are chatting through Facebook. Spencer sends Evan a link to what he purports is a funny video that will crack him up. Evan clicks the link, but it actually

brings up Evan\\'s bank account information in another browser tab, takes a screenshot of it, closes the tab, and sends the information to Spencer. The reason the attack is possible is because Evan is a trusted user with his own bank. In order

for it to work, Evan would need to have recently accessed that bank\\'s website and have a cookie that had yet to expire. The best protection against cross-site scripting is to disable the running of scripts (and browser profi les). This type of

attack does not attempt to write too much data to an application\\'s memory.

Therefore, this answer is incorrect.

References: http://searchsecurity.techtarget.com/definition/buffer-overflow http://www.pctools.com/security-news/zero-day-vulnerability/ http://en.wikipedia.org/wiki/ SQL_injection Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 335

QUESTION 15

LDAP and Kerberos are commonly used for which of the following?

A. To perform queries on a directory service

B. To store usernames and passwords for Federated Identity

C. To sign SSL wildcard certificates for subdomains

D. To utilize single sign-on capabilities

Correct Answer: D

Single sign-on is usually achieved via the Lightweight Directory Access Protocol (LDAP), although Kerberos can also be used.

Incorrect Answers:

A: This refers to LDAP only.

B: Federated Identity links a subject\\'s accounts from several sites, services, or entities in a single account. It does not make use of LDAP and Kerberos.

C: SSL wildcard certificates are public key certificates, which can be used with multiple subdomains of a domain, for securing web sites with HTTPS.

References: http://en.wikipedia.org/wiki/Single_sign-on
http://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol http://en.wikipedia.org/wiki/Federated_identity
http://en.wikipedia.org/wiki/Wildcard_certificate