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

CompTIA Security+ Certification

QUESTION 1

Ann, the system administrator, is installing an extremely critical system that can support ZERO downtime. Which of the following BEST describes the type of system Ann is installing?

A. High availability

B. Clustered

C. RAID

D. Load balanced

Correct Answer: A

QUESTION 2

The data security manager is notified that a client will be sending encrypted information on optical discs for import into the company database. Once imported, the information is backed up and the discs are no longer needed. Following the import, which of the following is the BEST action for the manager to take?

A. Wipe the discs and place into inventory for future use

B. Send the discs back to the client

C. Contract with a third party to shred the discs

D. Instruct employees to store the discs in a secure area

Correct Answer: B

QUESTION 3

How often, at a MINIMUM, should Sara, an administrator, review the accesses and rights of the users on her system?

A. Annually

B. Immediately after an employee is terminated

C. Every five years

D. Every time they patch the server

Correct Answer: A

Reviewing the accesses and rights of the users on a system at least annually is acceptable practice. More frequently would be desirable but too frequently would be a waste of administrative time.

Incorrect Answers:

B: You could check that a user hasn\\'t accessed your system after the user has been terminated. However, this question is asking about all users. It is unnecessary to check the accesses and rights of all users every time one user is terminated. Therefore, this answer is incorrect.

C: Every five years is too long. You should check the accesses and rights of the users on a system at least annually. Therefore, this answer is incorrect.

D: It is unnecessary to check the accesses and rights of the users on a system every time the system is patched. This would be a waste of administrative time. Therefore, this answer is incorrect.

QUESTION 4

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 5

A technician has just installed a new firewall onto the network. Users are reporting that they cannot reach any website. Upon further investigation, the technician determines that websites can be reached by entering their IP addresses. Which of the following ports may have been closed to cause this issue?

A. HTTP

B. DHCP

C. DNS

D. NetBIOS

Correct Answer: C

DNS links IP addresses and human-friendly fully qualified domain names (FQDNs), which are made up of the Top-level domain (TLD), the registered domain name, and the Subdomain or hostname.

Therefore, if the DNS ports are blocked websites will not be reachable.

Incorrect Answers:

A: HTTP is responsible for the transmission of HTML documents and embedded multimedia components.

B: Dynamic Host Configuration Protocol (DHCP) allows DHCP servers to assign, or lease, IP addresses to computers and other devices that are enabled as DHCP clients.

D: NetBIOS is a program that allows applications on different computers to communicate within a local area network (LAN).

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 42, 46. https://technet.microsoft.com/en-us/library/cc896553(v=ws.10).aspx http://en.wikipedia.org/wiki/NetBIOS

QUESTION 6

HOTSPOT

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

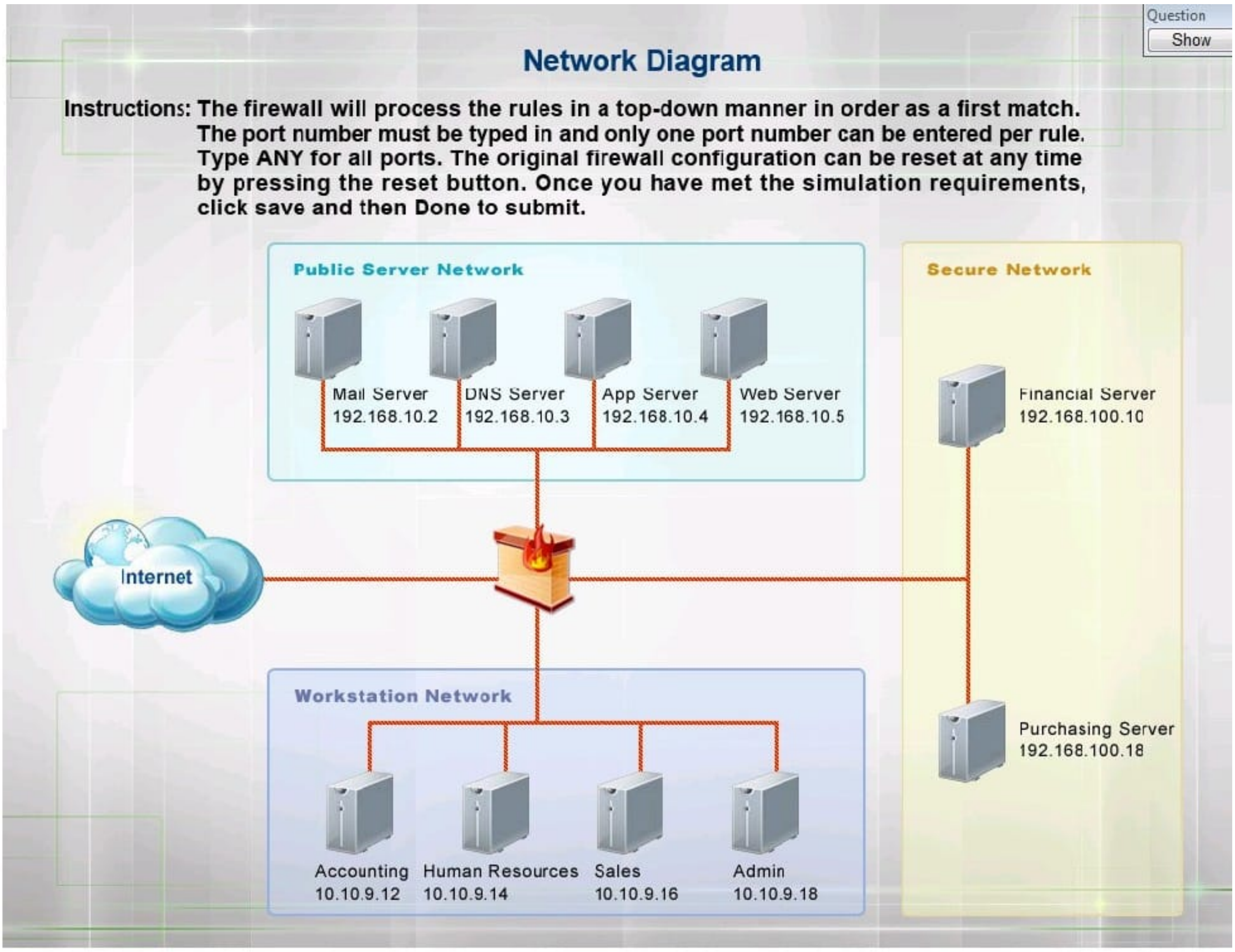
3.

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

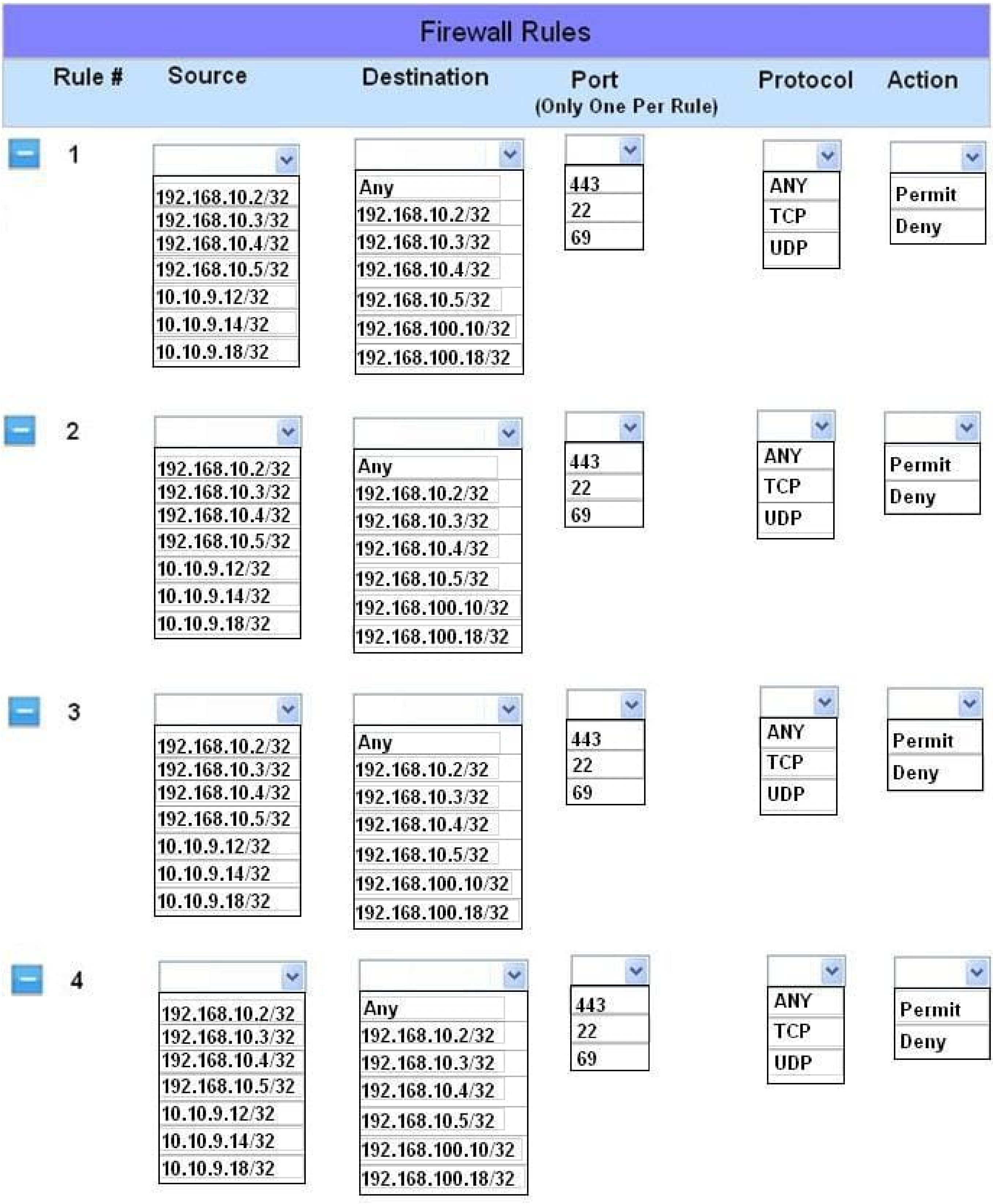
Done to submit.



Network Diagram

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.

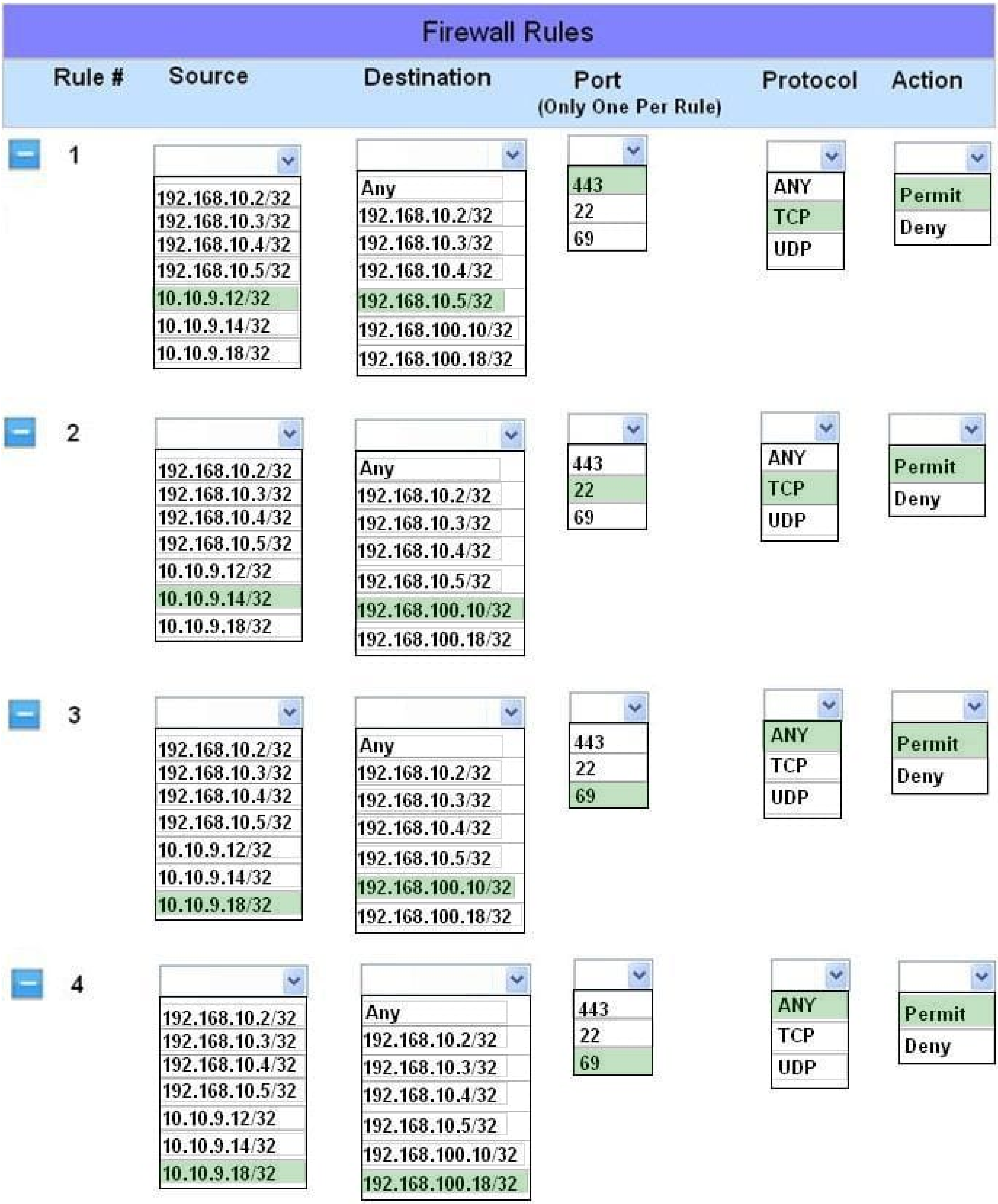
Hot Area:



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 192.168.100.18/32	443 22 69	ANY TCP UDP	Permit Deny

Correct Answer:



Firewall Rules

Rule #	Source	Destination	Port (Only One Per Rule)	Protocol	Action
1	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 **10.10.9.12/32** 10.10.9.14/32 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 **192.168.10.5/32** 192.168.100.10/32 192.168.100.18/32	**443** 22 69	ANY **TCP** UDP	**Permit** Deny
2	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 **10.10.9.14/32** 10.10.9.18/32	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 **192.168.100.10/32** 192.168.100.18/32	443 **22** 69	ANY **TCP** UDP	**Permit** Deny
3	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 **10.10.9.18/32**	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 **192.168.100.10/32** 192.168.100.18/32	443 22 **69**	**ANY** TCP UDP	**Permit** Deny
4	192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 10.10.9.12/32 10.10.9.14/32 **10.10.9.18/32**	Any 192.168.10.2/32 192.168.10.3/32 192.168.10.4/32 192.168.10.5/32 192.168.100.10/32 **192.168.100.18/32**	443 22 **69**	**ANY** TCP UDP	**Permit** Deny

QUESTION 7

One of the system administrators at a company is assigned to maintain a secure computer lab. The administrator has rights to configure machines, install software, and perform user account maintenance. However, the administrator cannot add new computers to the domain, because that requires authorization from the Information Assurance Officer. This is an example of which of the following?

A. Mandatory access

B. Rule-based access control

C. Least privilege

D. Job rotation

Correct Answer: C

A least privilege policy should be used when assigning permissions. Give users only the permissions that they need to do their work and no more.

Incorrect Answers:

A: Mandatory access control is used to control how information access is permitted. In a MAC environment, all access capabilities are predefined. Users can\\'t share information unless their rights to share it are established by administrators. Consequently, administrators must make any changes that need to be made to such rights.

B: Rule-based access control is when the settings used are in the pre-configured security policies.

D: Job rotation is when one person fills in for another and vice versa so that there is redundancy in this regard.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 151, 152

QUESTION 8

A company requires that a user\\'s credentials include providing something they know and something they are in order to gain access to the network. Which of the following types of authentication is being described?

A. Biometrics

B. Kerberos

C. Token

D. Two-factor

Correct Answer: D

Two-factor authentication is when two different authentication factors are provided for authentication purposes. In this case, "something they know and something they are". Incorrect Answers:

A: Biometrics refers to a collection of physical attributes of the human body that can be used for authentication. It is an authentication factor type. Something they are.

B: Kerberos is used for the security and protection of authentication credentials.

C: Tokens is an authentication factor type. Something they have.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 272, 280, 281, 282.

QUESTION 9

Which of the following can be implemented in hardware or software to protect a web server from cross-site scripting attacks?

A. Intrusion Detection System

B. Flood Guard Protection

C. Web Application Firewall

D. URL Content Filter

Correct Answer: C

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.

Incorrect Answers:

A: An Intrusion Detection System (IDS) is used to detect attempts to access a system. It cannot be used to detect cross-site scripting attacks where a malicious user is injecting malicious content into content being downloaded by a user.

B: Flood Guard Protection is used to prevent a network being flooded by data such as DoS, SYN floods, ping floods etc. The flood of data saturates the network and prevents the successful transmission of valid data across the network. Flood Guard Protection is not used to prevent cross-site scripting attacks. D. A URL Content Filter is used to permit access to allowed URLs (Websites) only or to block access to URLs that are not allowed according to company policy. For example, a company might use a URL Content Filter to block access to social networking sites. A URL Content Filter is not used to prevent cross-site scripting attacks.

References: http://en.wikipedia.org/wiki/Cross-site_scripting
https://www.owasp.org/index.php/Web_Application_Firewall

QUESTION 10

Which of the following functions provides an output which cannot be reversed and converts data into a string of characters?

A. Hashing

B. Stream ciphers

C. Steganography

D. Block ciphers

Correct Answer: A

Hashing refers to the hash algorithms used in cryptography. It is used to store data, such as hash tables one of its characteristics is that it must be one-way it is not reversible.

Incorrect Answers:

B: A stream cipher is similar to a block cipher in that they are both symmetric methods of cryptography. The difference is that with a stream cipher the data is encrypted one bit, or byte, at a time whereas with a block cipher the algorithm works on chunks of data.

C: Steganography is 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.

D: A block cipher is a symmetric method in cryptography that encrypts data in chunks; very similar to stream ciphers.

References: Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, p 248, 255, 291 http://en.wikipedia.org/wiki/Hash_function http://www.webopedia.com/TERM/H/hashing.html

QUESTION 11

A computer security officer has investigated a possible data breach and has found it credible. The officer notifies the data center manager and the Chief Information Security Officer (CISO). This is an example of:

A. escalation and notification.

B. first responder.

C. incident identification.

D. incident mitigation.

Correct Answer: A

QUESTION 12

A small company has a website that provides online customer support. The company requires an account recovery process so that customers who forget their passwords can regain access.

Which of the following is the BEST approach to implement this process?

A. Replace passwords with hardware tokens which provide two-factor authentication to the online customer support site.

B. Require the customer to physically come into the company\\'s main office so that the customer can be authenticated prior to their password being reset.

C. Web-based form that identifies customer by another mechanism and then emails the customer their forgotten password.

D. Web-based form that identifies customer by another mechanism, sets a temporary password and forces a password change upon first login.

Correct Answer: D

People tend to forget their passwords, thus you should have a password recovery system for them that will not increase risk exposure. Setting a temporary password will restrict the time that the password is valid and thus decrease risk; and in addition forcing the customer to change it upon first login will make the password more secure for the customer.

Incorrect Answers:

A: Two-factor authentication is a security process in which the user provides two means of identification, one of which is typically a physical token, such as a card, and the other of which is typically something memorized, such as a security

code. But in this case the problem stems from a forgotten password.

B: Requiring customers to physically come in to the company\\'s main office is not a viable option what if the customer is on a different continent?

C: Emailing customers their forgotten password is risky as the email can be intercepted, a forgotten password is best being eliminated from the system as a forgotten password if still active can compromise your business as well as your

customers.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp. 139, 142

QUESTION 13

Human Resources suspect an employee is accessing the employee salary database. The administrator is asked to find out who it is. In order to complete this task, which of the following is a security control that should be in place?

A. Shared accounts should be prohibited.

B. Account lockout should be enabled

C. Privileges should be assigned to groups rather than individuals

D. Time of day restrictions should be in use

Correct Answer: A

Since distinguishing between the actions of one person and another isn\\'t possible if they both use a shared account, shared accounts should not be allowed. If shared accounts are being used, the administrator will find the account, but have more than one suspect. To nullify this occurrence, Shared accounts should be prohibited.

Incorrect Answers:

B: When a user repeatedly enters an incorrect password at logon, Account lockout automatically disables their account someone attempts. Repeated incorrect logon attempts are not the issue in this instance.

C: Group-based privileges assign all members of a group a privilege or access to a resource as a collective. Assigning privileges to groups won\\'t help the administrator find the suspect.

D: Time of day restrictions limits when a specific user account can log on to the network according to the time of day. Time of day restrictions won\\'t help the administrator find the suspect.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 280, 293, 294.

QUESTION 14

Privilege creep among long-term employees can be mitigated by which of the following procedures?

A. User permission reviews

B. Mandatory vacations

C. Separation of duties

D. Job function rotation

Correct Answer: A

Privilege creep is the steady build-up of access rights beyond what a user requires to perform his/her task. Privilege creep can be decreased by conducting sporadic access rights reviews, which will confirm each user\\'s need to access specific roles and rights in an effort to find and rescind excess privileges.

Incorrect Answers:

B: Mandatory vacations require each employee to be on vacation for a minimal amount of time each year. During this time a different employee sits at their desk and performs their work tasks.

C: Separation of duties divides administrator or privileged tasks into separate groupings.

D: Job function rotation allows for employees to be knowledgeable about another employee\\'s job function in the event that an employee is sick or on vacation.

References:

Stewart, James Michael, CompTIA Security+ Review Guide, Sybex, Indianapolis, 2014, pp 81, 82, 294.

QUESTION 15

Which of the following allows a company to maintain access to encrypted resources when employee turnover is high?

A. Recovery agent

B. Certificate authority

C. Trust model

D. Key escrow

Correct Answer: A

If an employee leaves and we need access to data he has encrypted, we can use the key recovery agent to retrieve his decryption key. We can use this recovered key to access the data. A key recovery agent is an entity that has the ability to

recover a key, key components, or plaintext messages as needed. As opposed to escrow, recovery agents are typically used to access information that is encrypted with older keys.

Incorrect Answers:

B: A certificate authority (CA) is an organization. A CA is responsible for issuing, revoking, and distributing certificates. A CA cannot recovery keys.

C: A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. A trust model cannot recover keys.

D: Key escrow is not used to recover old keys.

Key escrow addresses the possibility that a third party may need to access keys. Under the conditions of key escrow, the keys needed to encrypt/decrypt data are held in an escrow account (think of the term as it relates to home mortgages)

and made available if that third party requests them. The third party in question is generally the government, but it could also be an employer if an employee\\'s private messages have been called into question.

References:

Dulaney, Emmett and Chuck Eastton, CompTIA Security+ Study Guide, Sixth Edition, Sybex, Indianapolis, 2014, pp 262, 279-280, 285-289

Latest JK0-022 Dumps JK0-022 VCE Dumps JK0-022 Practice Test