Microsoft

Exam 98-367

Security fundamentals

Version: 9.0

[Total Questions: 123]

Question No : 1

The Active Directory controls, enforces, and assigns security policies and access rights for all users.

Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.

A. NTFS permissions
B. User Account Control
C. Registry
D. No change is needed

Answer: D

Question No : 2

E-mail bombing attacks a specific entity by:

A. Redirecting all e-mail to another entity
B. Sending high volumes of e-mail
C. Tracing e-mail to the destination address
D. Triggering high levels of security alerts

Answer: B

Explanation:

In Internet usage, an email bomb is a form of net abuse consisting of sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted in a denial-of-service attack.

Question No : 3

Which two characteristics should you recommend for a user's domain password? (Choose two.)

A. Hard to guess

B. Includes Unicode characters
C. Easy to remember
D. Easy to increment

Answer: A,C
Reference: http://www.usewisdom.com/computer/passwords.html

Question No : 4

Passwords that contain recognizable words are vulnerable to a:

A. Denial of Service attack
B. Hashing attack
C. Dictionary attack
D. Replay attack

Answer: C
Explanation:
A dictionary attack is a method of breaking into a password-protected computer or server by systematically entering every word in a dictionary as a password. A dictionary attack can also be used in an attempt to find the key necessary to decrypt an encrypted message or document.

Dictionary attacks work because many computer users and businesses insist on using ordinary words as passwords. Dictionary attacks are rarely successful against systems that employ multiple-word phrases, and unsuccessful against systems that employ random combinations of uppercase and lowercase letters mixed up with numerals.
Reference: http://searchsecurity.techtarget.com/definition/dictionary-attack

Question No : 5

This question requires that you evaluate the underlined text to determine if it is correct.

The first line of defense against attacks from the Internet is a software firewall.

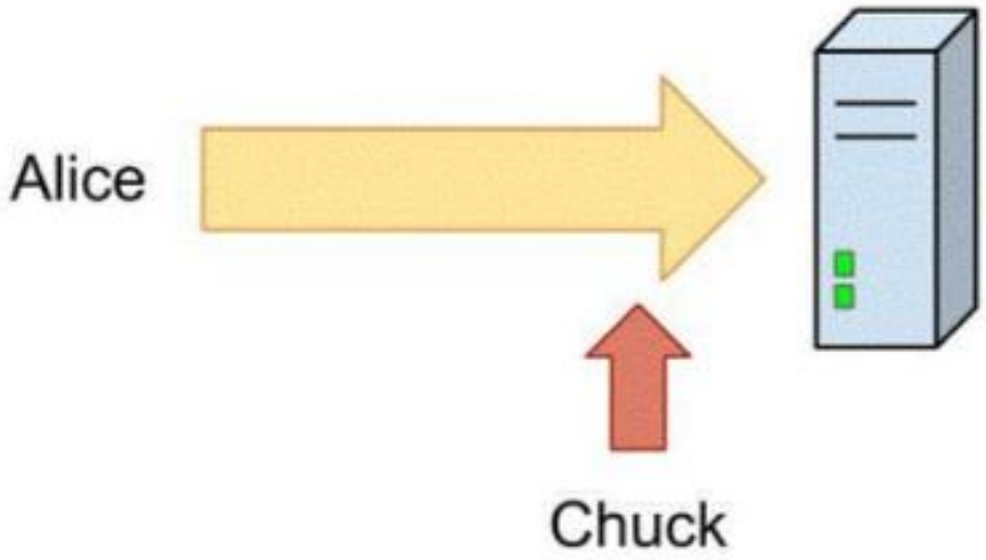
Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.

A. hardware firewall
B. virus software
C. radius server
D. No change is needed

Answer: A

Question No : 6 HOTSPOT

Alice sends her password to the game server in plaintext. Chuck is able to observe her password as shown in the following image:

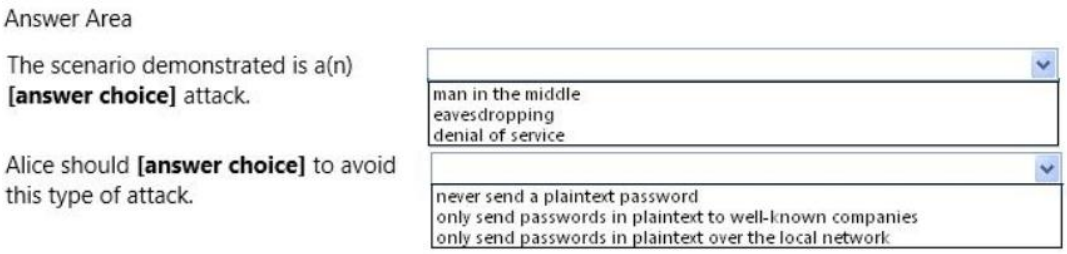


Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

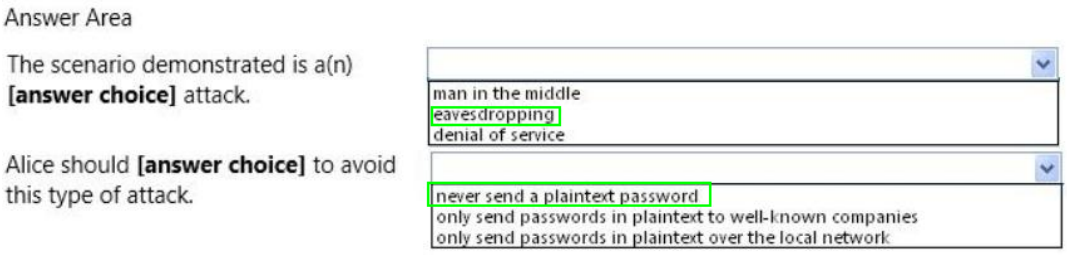
Answer Area

The scenario demonstrated is a(n) **[answer choice]** attack.

Alice should **[answer choice]** to avoid this type of attack.



Answer:



Question No : 7

You are trying to establish communications between a client computer and a server. The server is not responding.

You confirm that both the client and the server have network connectivity.

Which should you check next?

A. Microsoft Update
B. Data Execution Prevention
C. Windows Firewall
D. Active Directory Domains and Trusts

Answer: D

Question No : 8

Which technology enables you to filter communications between a program and the Internet?

A. RADIUS server
B. Antivirus software
C. Software firewall
D. BitLocker To Go

Answer: C

Explanation:

There are two types of firewalls the Hardware Firewall and the Software Firewall. A Software Firewall is a software program and a Hardware Firewall is a piece of hardware. Both have the same objective of filtering communications over a system.

Question No : 9

The primary method of authentication in an SSL connection is passwords.

To answer, choose the option "No change is needed" if the underlined text is correct. If the underlined text is not correct, choose the correct answer.

A. No change is needed
B. Certificates
C. IPsec
D. Biometrics

Answer: B

Reference: https://www.geocerts.com/ssl/understanding_authentication

Question No : 10

Keeping a server updated:

A. Maximizes network efficiency
B. Fixes security holes
C. Speeds up folder access
D. Synchronizes the server

Answer: B

Question No : 11

Which of the following describes a VLAN?

A. It connects multiple networks and routes data packets.
B. It is a logical broadcast domain across physical subnets.
C. It is a subnetwork that reveals a company's externally facing resources to the public network.
D. It allows different network protocols to communicate between different network segments.

Answer: B

Explanation:

VLAN (Virtual Local Network) is a logically separate IP subnetwork which allow multiple IP networks and subnets to exist on the same-switched network.

VLAN is a logical broadcast domain that can span multiple physical LAN segments. It is a modern way administrators configure switches into virtual local-area networks (VLANs) to improve network performance by separating large Layer 2 broadcast domains into smaller ones.

Question No : 12

You are an intern at Litware, Inc. Your manager asks you to make password guess attempts harder by limiting login attempts on company computers.

What should you do?

A. Enforce password sniffing.
B. Enforce password history.
C. Make password complexity requirements higher.
D. Implement account lockout policy.

Answer: D

Reference: http://technet.microsoft.com/en-us/library/dd277400.aspx

Question No : 13

Shredding documents helps prevent:

A. Man-in-the-middle attacks
B. Social engineering
C. File corruption
D. Remote code execution
E. Social networking

Answer: B
Reference: http://technet.microsoft.com/en-us/library/cc875841.aspx

Question No : 14 HOTSPOT

An employee where you work is unable to access the company message board in Internet Explorer.

You review her Internet Options dialog box, as shown in the following image:

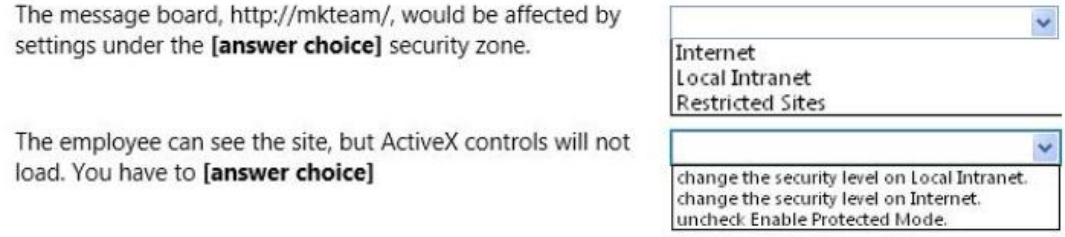
Use the drop-down menus to select the answer choice that completes each statement. Each correct selection is worth one point.

Answer Area

The message board, http://mkteam/, would be affected by settings under the **[answer choice]** security zone.

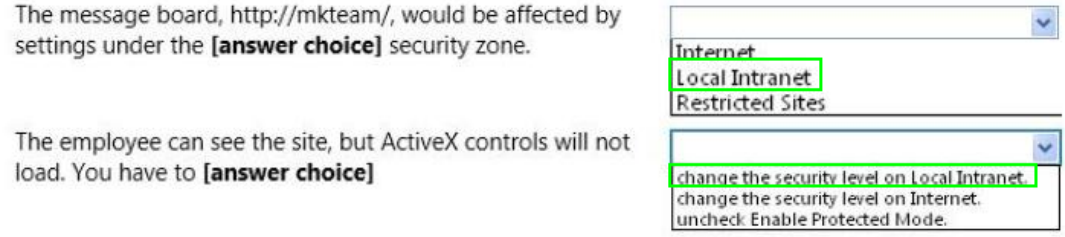
The employee can see the site, but ActiveX controls will not load. You have to **[answer choice]**

Answer Area



Answer:

Answer Area



Question No : 15

E-mail spoofing:

A. Forwards e-mail messages to all contacts
B. Copies e-mail messages sent from a specific user
C. Obscures the true e-mail sender
D. Modifies e-mail routing logs

Answer: C
Reference:
http://www.microsoft.com/mscorp/safety/technologies/senderid/technology.mspx

Question No : 16

Which attack listens to network traffic of a computer resource?