Microsoft

98-367

MTA Security Fundamentals

QUESTION & ANSWERS

Microsoft

98-367 Exam

Microsoft MTA Security Fundamentals Exam

Questions & Answers Demo

Question: 1

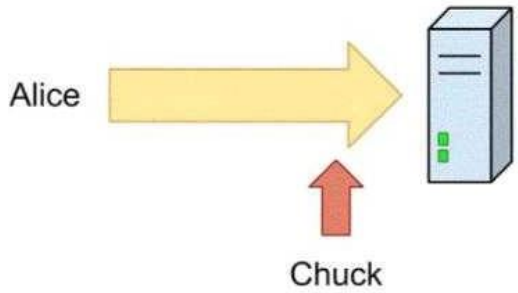
Windows Firewall is a built-in. host-based, stateless firewall.
Select the correct answer if the underlined text does not make the statement correct. Select "No change is needed" if the underlined text makes the statement correct.

A. Stateful
B. Network layer
C. Packet filter
D. No change is needed

Answer: A

Question: 2

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 Area

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

- man in the middle
- eavesdropping
- denial of service

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

- never send a plaintext password
- only send passwords in plaintext to well-known companies
- only send passwords in plaintext over the local network

Answer:

First answer – Eavesdropping
Second Answer – never send a plaintext password

Question: 3

HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

Answer Area

	Yes	No
IPsec requires network applications to be IPsec aware.	○	○
IPsec encrypts data.	○	○
IPsec adds overhead for all network communications for which it is used.	○	○

Answer:

Answer Area

	Yes	No
IPsec requires network applications to be IPsec aware.	○	◉
IPsec encrypts data.	◉	○
IPsec adds overhead for all network communications for which it is used.	◉	○

Question: 4

HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.
Answer Area

	Yes	No
Honey pots are primarily used to attract potential attackers or hackers.	○	○
By setting up a honey pot, an administrator can get insightful information about the attacker, such as the IP address.	○	○
A honey pot is an appliance or piece of software that allows or denies network access based on a preconfigured set of rules.	○	○

Answer:

Answer Area

	Yes	No
Honey pots are primarily used to attract potential attackers or hackers.	○	○
By setting up a honey pot, an administrator can get insightful information about the attacker, such as the IP address.	○	○
A honey pot is an appliance or piece of software that allows or denies network access based on a preconfigured set of rules.	○	○

Question: 5

Bridging is a process of sending packets from source to destination on OSI layer 3.
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. Routing
B.Switchin
g
C.Repeati
ng
D.No change is needed.

Answer: A

Question: 6

The primary purpose of Network Access Protection (NAP) is to prevent:

A. Loss of data from client computers on a network.
B.Non-compliant systems from connecting to a network. C.Users on a network from installing software. D.Unauthorized users from accessing a network.

Answer: B

Explanation:
NAP enforces health policies by inspecting and assessing the health of client computers, restricting network access when client computers are noncompliant with health policy, and remediating noncompliant client computers to bring them into compliance with health policy before they are granted full network access. NAP enforces health policies on client computers that are attempting to connect to a network; NAP also provides ongoing health compliance enforcement while a client computer is connected to a network.
Explanation:
Reference:
http://technet.microsoft.com/en-us/library/cc754378(v=ws.10).aspx

Question: 7

You want to make your computer resistant to online hackers and malicious software. What should you do?

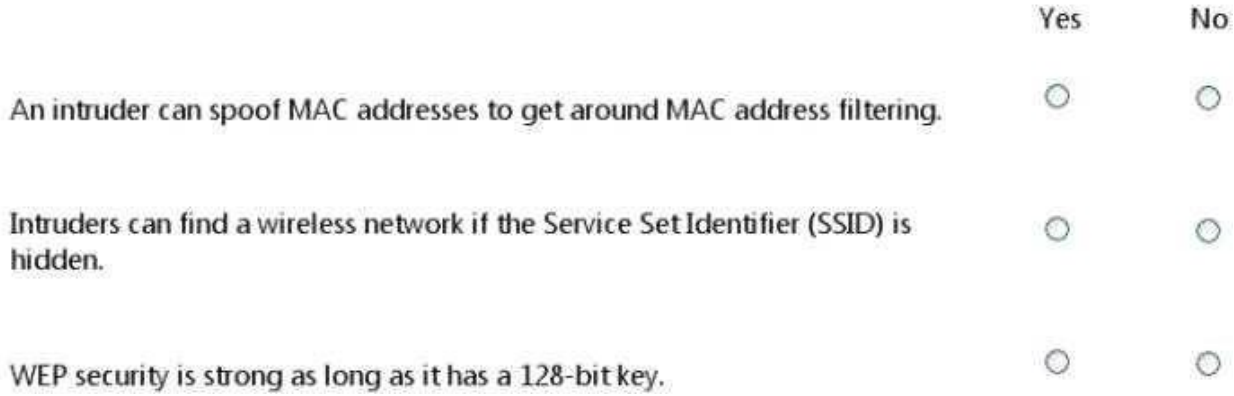
A. Configure a forward proxy.
B. Install anti-virus software.
C. Enable spam filtering.
D. Turn on Windows Firewall.

Answer: B

Question: 8

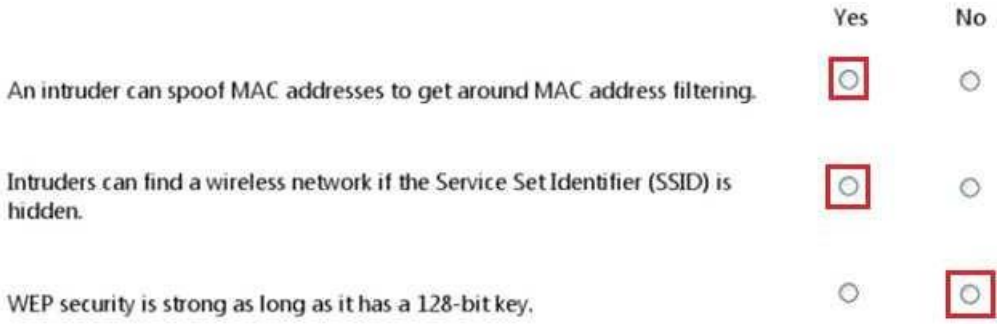
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

Answer Area



Answer:

Answer Area



Question: 9

Your company requires that users type a series of characters to access the wireless network. The series of characters must meet the following requirements:
Contains more than 15
characters Contains at least one
letter Contains at least one
number Contains at least one
symbol
Which security technology meets these requirements?

A. WEP
B.WPA2 PSK
C.WPA2 Enterprise
D.MAC filtering

Answer: B

Explanation: Pre-shared key mode (PSK, also known as Personal mode) is designed for home and small office networks that don't require the complexity of an 802.1X authentication server.[9] Each wireless network device encrypts the network traffic using a 256 bit key. This key may be entered

either as a string of 64 hexadecimal digits, or as a passphrase of 8 to 63 printable ASCII characters

Question: 10

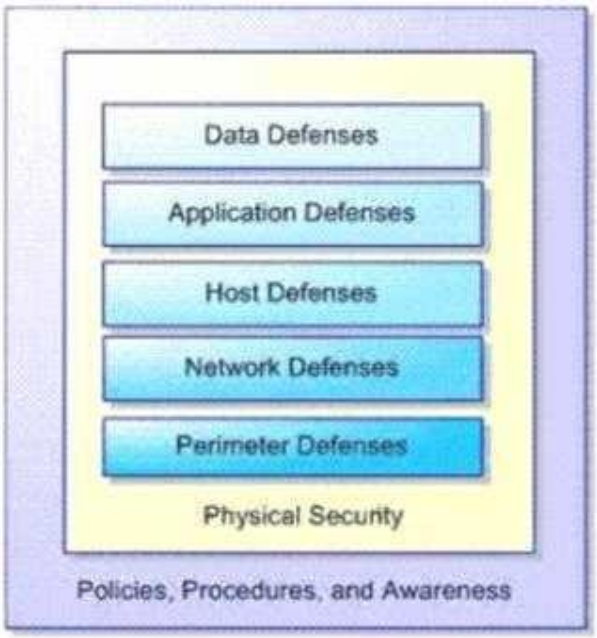
Many Internet sites that you visit require a user name and password. How should you secure these passwords?

A. Save them to a text file
B. Enable session caching
C. Configure the browser to save passwords D.Save them to an encrypted file
E.Reuse the same password

Answer: D

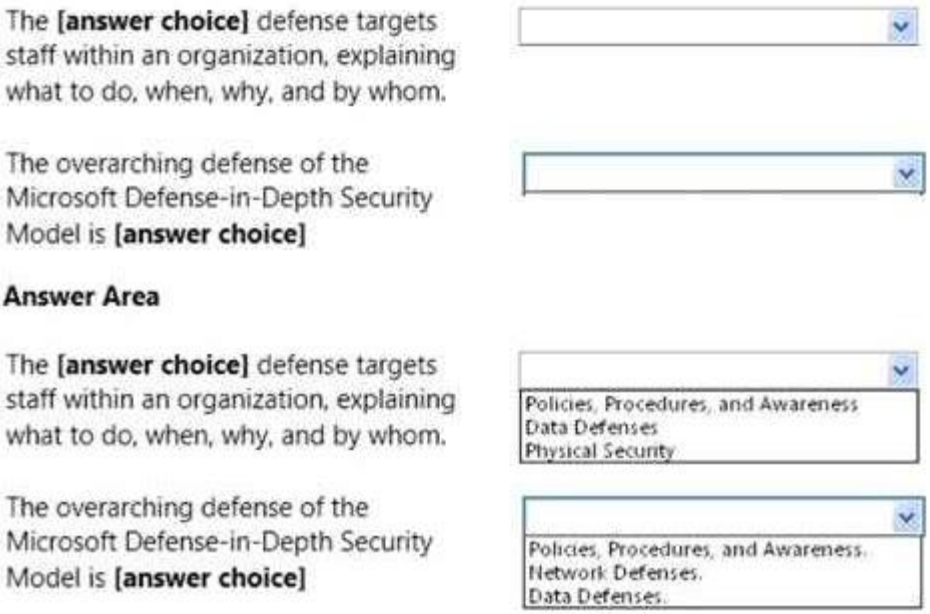
Question: 11

HOTSPOT
You are an intern for a company where your manager wants to be sure you understand the social engineering threats that may occur. Your manager emphasizes the principles of the Microsoft Defense-in-Depth Security Model 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



Answer Area

Answer:

First Answer – Policies, Procedures, and Awareness Second Answers – Data Defenses

Question: 12

Physically securing servers prevents:

A. Theft
B. Compromise of the certificate chain C.Man-in-the middle attacks
D.Denial of Service attacks

Answer: A