

CERTPARK



QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



Exam : **98-367**

Title : MTA Security Fundamentals
Practice Test

Version : Demo

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.

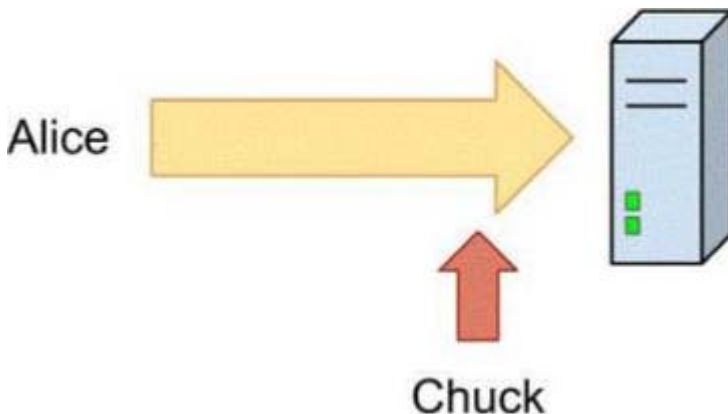
- A. Stateful
- B. Network layer
- C. Packet filter
- D. No change is needed

Answer: A

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:

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

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.	<input type="radio"/>	<input type="radio"/>
IPsec encrypts data.	<input type="radio"/>	<input type="radio"/>
IPsec adds overhead for all network communications for which it is used.	<input type="radio"/>	<input type="radio"/>
Answer:		
Answer Area		
	Yes	No
IPsec requires network applications to be IPsec aware.	<input type="radio"/>	<input checked="" type="radio"/>
IPsec encrypts data.	<input checked="" type="radio"/>	<input type="radio"/>
IPsec adds overhead for all network communications for which it is used.	<input checked="" type="radio"/>	<input type="radio"/>

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.	<input type="radio"/>	<input type="radio"/>
By setting up a honey pot, an administrator can get insightful information about the attacker, such as the IP address.	<input type="radio"/>	<input type="radio"/>
A honey pot is an appliance or piece of software that allows or denies network access based on a preconfigured set of rules.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

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

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. Switching
- C. Repeating
- D. No change is needed.

Answer: A

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.

Reference: [http://technet.microsoft.com/en-us/library/cc754378 \(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc754378 (v=ws.10).aspx)

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

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

	Yes	No
An intruder can spoof MAC addresses to get around MAC address filtering.	<input type="radio"/>	<input type="radio"/>
Intruders can find a wireless network if the Service Set Identifier (SSID) is hidden.	<input type="radio"/>	<input type="radio"/>
WEP security is strong as long as it has a 128-bit key.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
An intruder can spoof MAC addresses to get around MAC address filtering.	<input checked="" type="radio"/>	<input type="radio"/>
Intruders can find a wireless network if the Service Set Identifier (SSID) is hidden.	<input checked="" type="radio"/>	<input type="radio"/>
WEP security is strong as long as it has a 128-bit key.	<input type="radio"/>	<input checked="" type="radio"/>

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

10. Many Internet sites that you visit require a user name and password.

How should you secure these passwords?

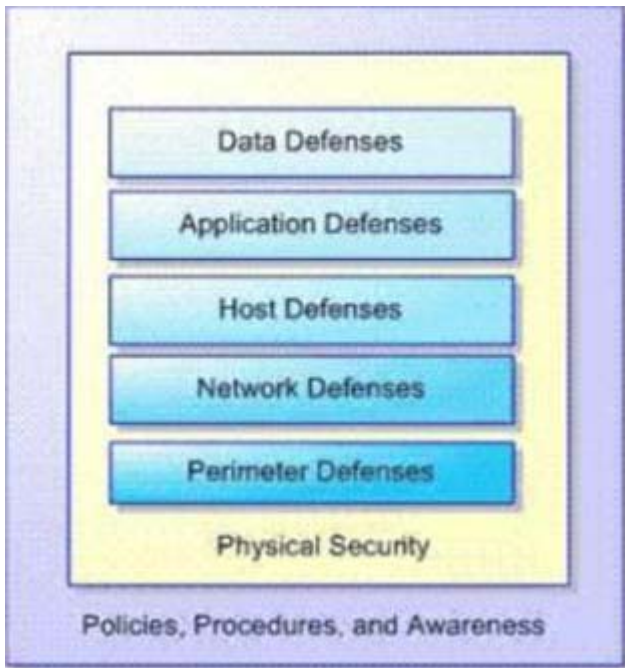
- A. Save them to a text file
- B. Enable session caching
- C. Configure the browser to save passwords
- D. Save them to an encrypted file
- E. Reuse the same password

Answer: D

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

The [answer choice] defense targets staff within an organization, explaining what to do, when, why, and by whom.

The overarching defense of the Microsoft Defense-in-Depth Security Model is [answer choice]

Answer Area

The [answer choice] defense targets staff within an organization, explaining what to do, when, why, and by whom.

- Policies, Procedures, and Awareness
- Data Defenses
- Physical Security

The overarching defense of the Microsoft Defense-in-Depth Security Model is [answer choice]

- Policies, Procedures, and Awareness.
- Network Defenses.
- Data Defenses.

Answer:

Answer Area

The [answer choice] defense targets staff within an organization, explaining what to do, when, why, and by whom.

- Policies, Procedures, and Awareness
- Data Defenses
- Physical Security

The overarching defense of the Microsoft Defense-in-Depth Security Model is [answer choice]

- Policies, Procedures, and Awareness.
- Network Defenses.
- Data Defenses.

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

13. To prevent users from copying data to removable media, you should:

- A. Lock the computer cases
- B. Apply a group policy
- C. Disable copy and paste
- D. Store media in a locked room

Answer: B

Explanation:

Reference:

<http://blogs.technet.com/b/askds/archive/2008/08/25/removable-storage-group-policy-and-windows-server-2008-and-windows-vista.aspx>

14. 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
Because senior executives have rights to access sensitive data, they should use administrator accounts.	<input type="radio"/>	<input type="radio"/>
The User Account Control (UAC) has one overall goal: to grant users the lowest level permissions required to complete their tasks.	<input type="radio"/>	<input type="radio"/>
System administrators should use a standard user account when performing routine functions like reading emails and browsing the Internet.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
Because senior executives have rights to access sensitive data, they should use administrator accounts.	<input type="radio"/>	<input checked="" type="radio"/>
The User Account Control (UAC) has one overall goal: to grant users the lowest level permissions required to complete their tasks.	<input checked="" type="radio"/>	<input type="radio"/>
System administrators should use a standard user account when performing routine functions like reading emails and browsing the Internet.	<input checked="" type="radio"/>	<input type="radio"/>

15.You are an intern at Wide World Importers and help manage 1000 workstations. All the workstations are members of an Active Domain. You need to push out an internal certificate to Internet Explorer on all workstations.

What is the quickest method to do this?

- A. Local policy
- B. Logon script
- C. Windows Update
- D. Group policy

Answer: A

16.In Internet Explorer 8, the In Private Browsing feature prevents:

- A. Unauthorized private data input.
- B. Unencrypted communication between the client computer and the server.
- C. User credentials from being sent over the Internet.
- D. Any session data from being stored on the computer.

Answer: D

Explanation:

Reference: <http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing>

17.The purpose of a digital certificate is to verify that a:

- A. Public key belongs to a sender.
- B. Computer is virus-free.
- C. Private key belongs to a sender.
- D. Digital document is complete.

Answer: A

Explanation:

In cryptography, a public key certificate (also known as a digital certificate or identity certificate) is an electronic document that uses a digital signature to bind a public key with an identity.

18.A mail system administrator scans for viruses in incoming emails to increase the speed of mail

processing. 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. Decrease the chances of a virus getting to a client machine
- B. Verify that the senders of the messages are legitimate
- C. Ensure that all links in the messages are trustworthy
- D. No change is needed.

Answer: A

19. You are volunteering at an organization that gets a brand new web server. To make the server more secure, you should add a second administrator account. 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. Disable unused services
- B. Enable LM authentication
- C. Enable NTLM authentication
- D. No change is needed.

Answer: A

20. Role separation improves server security by:

- A. Enforcing principle of least privilege.
- B. Installing applications on separate hard disks.
- C. Physically separating high security servers from other servers.
- D. Placing servers on separate VLANs.

Answer: A