

PASS4SURES.COM

A Composite Solution With Just One Click

Microsoft

98-367 PRACTICE EXAM

MTA Security Fundamentals

Product Questions: 123

Version: 10.0

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.

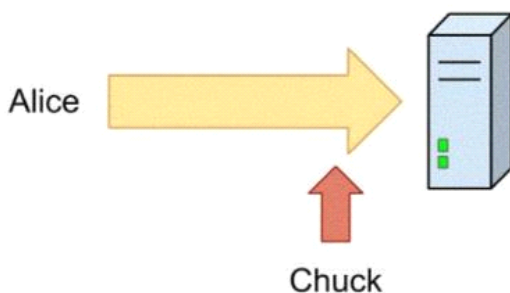
- A. Stateful
- B. Network layer
- C. Packet filter
- D. No change is needed

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.	<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"/>

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.	<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"/>

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. Switching
- C. Repeating
- 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](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

	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"/>

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?

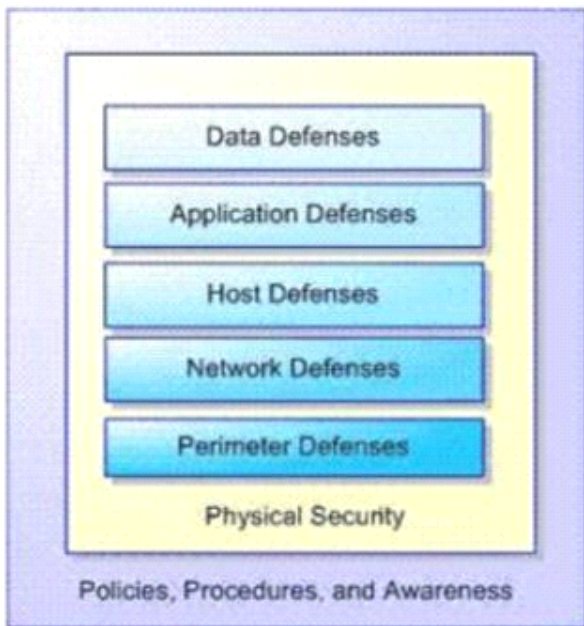
- A. Save them to a text file
- B. Enable session caching
- C. Configure the browser to save passwords
- D. Save them to an encrypted file
- E. Reuse the same password

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

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:

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

Question: 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>

Question: 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"/>

Question: 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**Question: 16**

In Internet Explorer 8, the InPrivate 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>

Question: 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.

Question: 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

Question: 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

Question: 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

Question: 21

The Windows Firewall protects computers from unauthorized network connections.

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. Email viruses
- B. Phishing scams
- C. Unencrypted network access
- D. No change is needed

Answer: D

Question: 22

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
Tools like Microsoft Security Compliance Manager and Microsoft Baseline Security Analyzer can assist with server hardening.	<input type="radio"/>	<input type="radio"/>
Administrator passwords may contain ASCII characters generated by a combination of the ALT key and three digits on the numeric keypad.	<input type="radio"/>	<input type="radio"/>
The removal of unused registry entries and executables increases the surface vulnerability of the server.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
Tools like Microsoft Security Compliance Manager and Microsoft Baseline Security Analyzer can assist with server hardening.	<input checked="" type="radio"/>	<input type="radio"/>
Administrator passwords may contain ASCII characters generated by a combination of the ALT key and three digits on the numeric keypad.	<input checked="" type="radio"/>	<input type="radio"/>
The removal of unused registry entries and executables increases the surface vulnerability of the server.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 23

Coho Winery wants to increase their web presence and hires you to set up a new web server. Coho already has servers for their business and would like to avoid purchasing a new one.

Which server is best to use as a web server, considering the security and performance concerns?

- A. SQL Server
- B. File Server
- C. Domain Controller
- D. Application Server

Answer: C

Question: 24

A user who receives a large number of emails selling prescription medicine is probably receiving pharming mail. 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. Malware
- B. Spoofed mail
- C. Spam
- D. No change is needed.

Answer: C

Question: 25

The client computers on your network are stable and do not need any new features. Which is a benefit of applying operating system updates to these clients?

- A. Keep the software licensed
- B. Keep the server ports available
- C. Update the hardware firewall
- D. Close existing vulnerabilities

Answer: D

Question: 26

Which password attack uses all possible alpha numeric combinations?

- A. Social engineering
- B. Brute force attack
- C. Dictionary attack
- D. Rainbow table attack

Answer: C

Question: 27

A digitally signed e-mail message:

- A. Validates the recipient
- B. Validates the sender
- C. Is encrypted
- D. Is virus-free

Answer: B

Explanation:

By digitally signing a message, you apply your unique digital mark to the message. The digital signature includes your certificate and public key. This information proves to the recipient that you signed the contents of the message and not an imposter, and that the contents have not been altered in transit.

Explanation:

Reference:

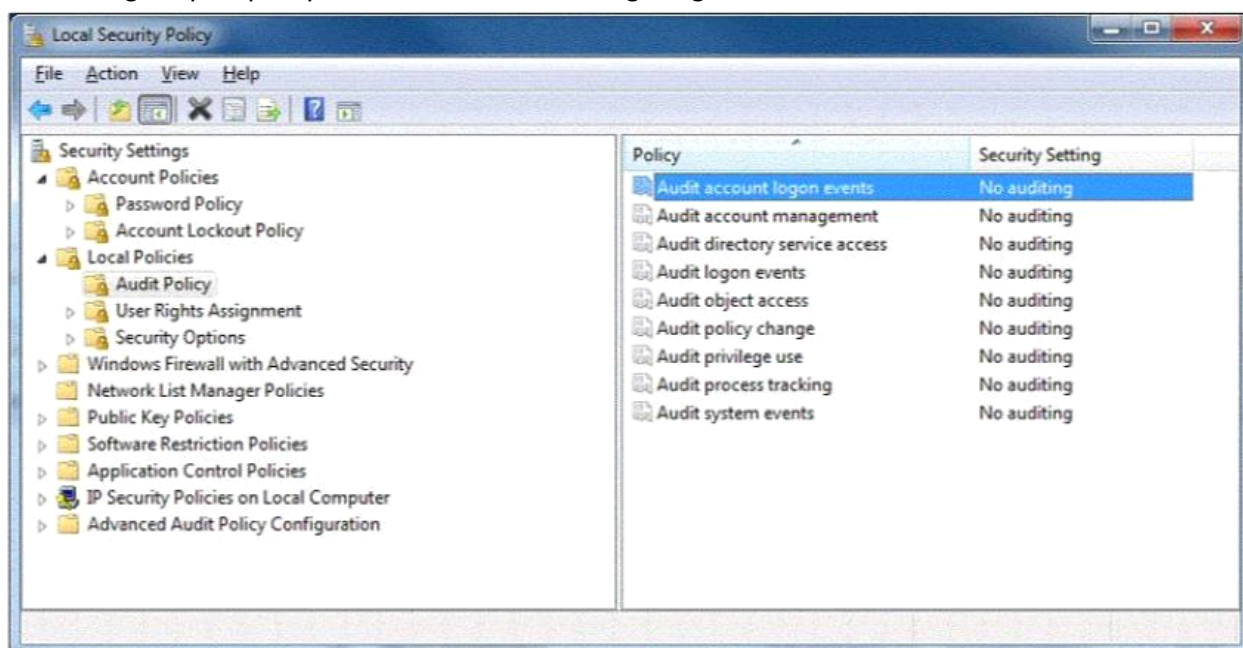
<http://office.microsoft.com/en-us/outlook-help/secure-messages-with-a-digital-signature-HP001230539.aspx>

Question: 28

HOTSPOT

You are preparing a local audit policy for your workstation. No auditing is enabled.

The settings of your policy are 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.

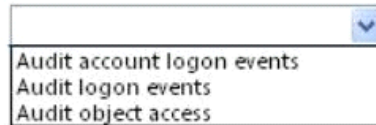
Answer Area

In order to log each time the computer validates account credentials, the **[answer choice]** policy needs to be enabled.

You need to log each time someone reboots the workstation. The **[answer choice]** policy will log a reboot of the computer.

Answer Area

In order to log each time the computer validates account credentials, the **[answer choice]** policy needs to be enabled.



You need to log each time someone reboots the workstation. The **[answer choice]** policy will log a reboot of the computer.



Answer:

First answer – Audit account logon events

Second answers – audit system events

Explanation:

Dozens of events can be audited in Windows. The events fall into several categories:

Audit account logon events - audit each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account. This event category is applicable to domain controllers only since DC's are used to validate accounts in domains.

Audit account management - audit each event of account management on a computer. Examples of account maintenance include password changes, user account and group modifications.

Audit directory service access - audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.

Audit logon events - audit each instance of a user logging on to or logging off from a computer. Note that this is different than the 'Audit account login events' category. This tracks the logon event to a specific server. The former tracks which domain controller authenticated the user.

Audit object access - audit the event of a user accessing an object that has its own system access control list (SACL) specified. Examples of objects are files, folders, registry keys, printers, etc.

Audit policy change - audit every incident of a change to user rights assignment policies, audit policies, or trust policies.

Audit privilege use - audit each instance of a user exercising a user right.

Audit process tracking - audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.

Audit system events - audit when a user restarts or shuts down the computer or when an event occurs that affects either the system security or the security log.

Reference:

http://www.petri.co.il/windows_auditing.htm

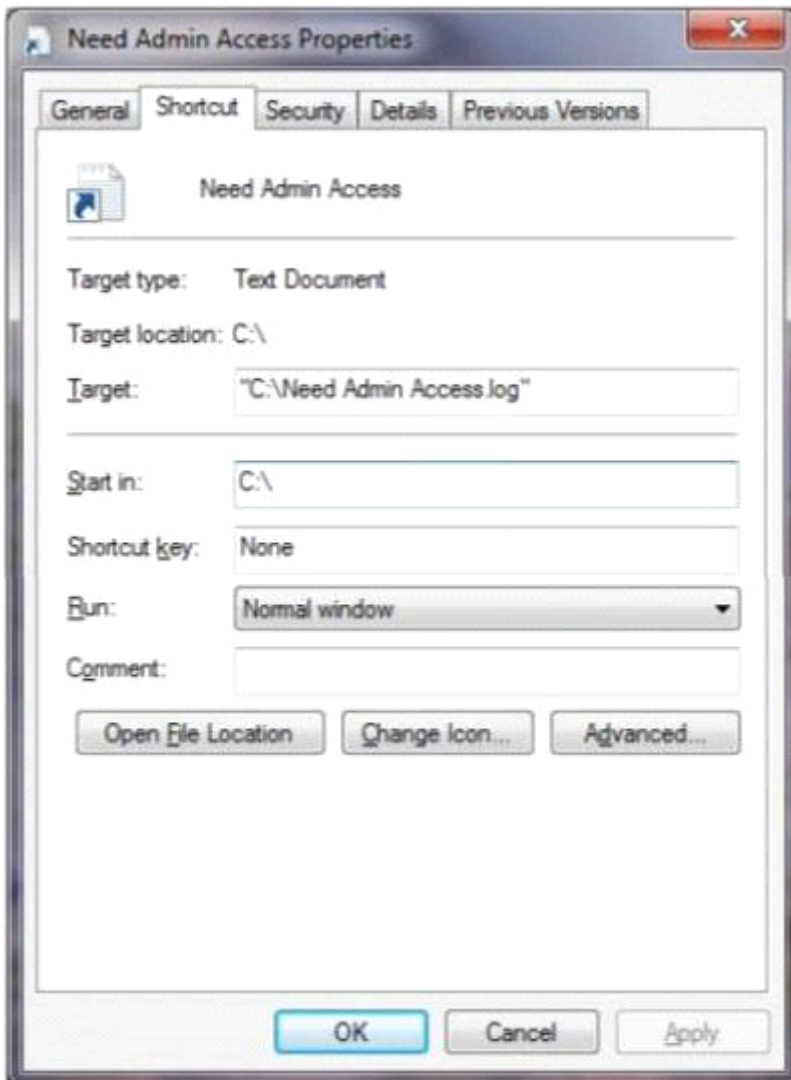
Question: 29

HOTSPOT

You are at school and logged in to a Windows 7 computer using a standard user account.

You need to change some of the properties of a desktop icon for an assignment. Your instructor provides you with an administrator username and password and asks you to do two tasks.

When you open the Need Admin Access Properties window, you see 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

To allow this log file to be opened as an administrator, you should [answer choice]

To allow this log file to be opened in a maximized window, you should [answer choice]

Answer Area

To allow this log file to be opened as an administrator, you should [answer choice]

click Advanced and choose "run as administrator."
click Run and choose "run as administrator."
click the Security tab and give admin rights to your standard account.

To allow this log file to be opened in a maximized window, you should [answer choice]

click Run and choose "maximized window."
click the General tab and click "change to open the document as a maximized window."
click Change Icon to choose "run as a maximized window."

Answer:

Answer Area

To allow this log file to be opened as an administrator, you should [answer choice]

click Advanced and choose "run as administrator."
 click Run and choose "run as administrator."
 click the Security tab and give admin rights to your standard account.

To allow this log file to be opened in a maximized window, you should [answer choice]

click Run and choose "maximized window."
 click the General tab and click "change to open the document as a maximized window."
 click Change Icon to choose "run as a maximized window."

Question: 30

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: 31

Account lockout policies are used to prevent which type of security attack?

- A. Brute force attacks
- B.Users sharing passwords
- C.Social engineering
- D.Passwords being reused immediately

Answer: A**Question: 32**

What is the standard or basic collection of NTFS permissions?

- A. Read and execute, read, write, full control, modify, list folder contents
- B.Change permissions, read permissions, write permissions
- C.Read attributes, list folder/read data, traverse folder/execute file
- D.Create files/write data, create folders/append data, take ownership

Answer: A

Explanation:

Reference:

<http://technet.microsoft.com/en-us/library/bb727008.aspx>

Question: 33

Which is the minimum requirement to create BitLocker-To-Go media on a client computer?

- A. Windows XP Professional Service Pack 3
- B. Windows Vista Enterprise Edition
- C. Windows 7 Enterprise Edition
- D. Windows 2000 Professional Service Pack 4

Answer: A

Question: 34

Which enables you to change the permissions on a folder?

- A. Take ownership
- B. Extended attributes
- C. Auditing
- D. Modify

Answer: D

Question: 35

A group of users has access to Folder A and all of its contents. You need to prevent some of the users from accessing a subfolder inside Folder A.

What should you do first?

- A. Disable folder sharing
- B. Hide the folder
- C. Change the owner
- D. Block inheritance

Answer: A

Question: 36

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
Biometrics are used to authenticate users.	<input type="radio"/>	<input type="radio"/>
Biometric data is usually encrypted when it is gathered.	<input type="radio"/>	<input type="radio"/>
An example of a biometric device is a fingerprint scanner.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

	Yes	No
Biometrics are used to authenticate users.	<input checked="" type="radio"/>	<input type="radio"/>
Biometric data is usually encrypted when it is gathered.	<input checked="" type="radio"/>	<input type="radio"/>
An example of a biometric device is a fingerprint scanner.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Biometric devices, such as finger scanners consist of a reader or scanning device, Software that converts the scanned information into digital form and compares match points, and a database that stores the biometric data for comparison. To prevent identity theft, biometric data is usually encrypted when it is gathered.

Question: 37

What are three examples of two-factor authentication? (Choose three.)

- A. A fingerprint and a pattern
- B. A password and a smart card
- C. A username and a password
- D. A password and a pin number
- E. A pin number and a debit card

Answer: A, B, E

Explanation:

At minimum two-factor authentication requires two out of three regulatory-approved authentication variables such as:

Something you know (like the PIN on your bank card or email password).

Something you have (the physical bank card or a authenticator token).

Something you are (biometrics like your finger print or iris pattern).

Question: 38

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
You can view audit logs in the Event Viewer.	<input type="radio"/>	<input type="radio"/>
Audit logs have a set size limit and cannot be adjusted.	<input type="radio"/>	<input type="radio"/>
You can configure an email event notification for an audited activity.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
You can view audit logs in the Event Viewer.	<input checked="" type="radio"/>	<input type="radio"/>
Audit logs have a set size limit and cannot be adjusted.	<input type="radio"/>	<input checked="" type="radio"/>
You can configure an email event notification for an audited activity.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 39

You need to limit the programs that can run on client computers to a specific list. Which technology should you implement?

- A. Windows Security Center
- B. Security Accounts Manager
- C. System Configuration Utility
- D. AppLocker group policies

Answer: A

Question: 40

The purpose of User Account Control (UAC) is to:

- A. Encrypt the user's account
- B. Limit the privileges of software
- C. Secure your data from corruption
- D. Facilitate Internet filtering

Answer: B

Explanation:

User Account Control (UAC) is a technology and security infrastructure introduced with Microsoft's Windows machines. It aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the user may receive administrative privileges, and malware should be kept from compromising the operating system.

Question: 41

What does implementing Windows Server Update Services (WSUS) allow a company to manage?

- A. Shared private encryption key updates
- B. Updates to Group Policy Objects
- C. Active Directory server replication
- D. Windows updates for workstations and servers

Answer: D

Question: 42

The purpose of Microsoft Baseline Security Analyzer is to:

- A. List system vulnerabilities.
- B. Apply all current patches to a server.
- C. Set permissions to a default level.
- D. Correct a company's security state.

Answer: A

Question: 43

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
UAC reduces your permissions to that of a standard user unless higher permissions are necessary.	<input type="radio"/>	<input type="radio"/>
UAC notifies you when additional permissions are required and asks if you wish to continue.	<input type="radio"/>	<input type="radio"/>
UAC cannot be disabled.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
UAC reduces your permissions to that of a standard user unless higher permissions are necessary.	<input checked="" type="radio"/>	<input type="radio"/>
UAC notifies you when additional permissions are required and asks if you wish to continue.	<input checked="" type="radio"/>	<input type="radio"/>
UAC cannot be disabled.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 44

The Graphic Design Institute hires you to help them set up a server for their 20-person team. As a general practice of hardening the server, you start by performing which two tasks? (Choose two.)

- A. Disable the guest account.
- B. Rename the admin account.
- C. Remove the account lockout policy.
- D. Format partitions with FAT32.

Answer: A, B**Question: 45**

What are two attributes that an email message may contain that should cause a user to question whether the message is a phishing attempt? (Choose two.)

- A. An image contained in the message
- B. Spelling and grammar errors
- C. Threats of losing service
- D. Use of bold and italics

Answer: B, C

Explanation:

Reference:

<http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>

Question: 46

Keeping a server updated:

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

Answer: B

Question: 47

Before you deploy Network Access Protection (NAP), you must install:

- A. Internet Information Server (IIS)
- B. Network Policy Server (NPS)
- C. Active Directory Federation Services
- D. Windows Update Service

Answer: B

Explanation:

Reference:

<http://technet.microsoft.com/en-us/library/bb681008.aspx>

Question: 48

What is a common method for password collection?

- A. Email attachments
- B. Back door intrusions
- C. SQL Injection
- D. Network sniffers

Answer: D

Question: 49

Which provides the highest level of security in a firewall?

- A. Stateful inspection
- B. Outbound packet filters
- C. Stateless inspection
- D. Inbound packet filters

Answer: A

Question: 50

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

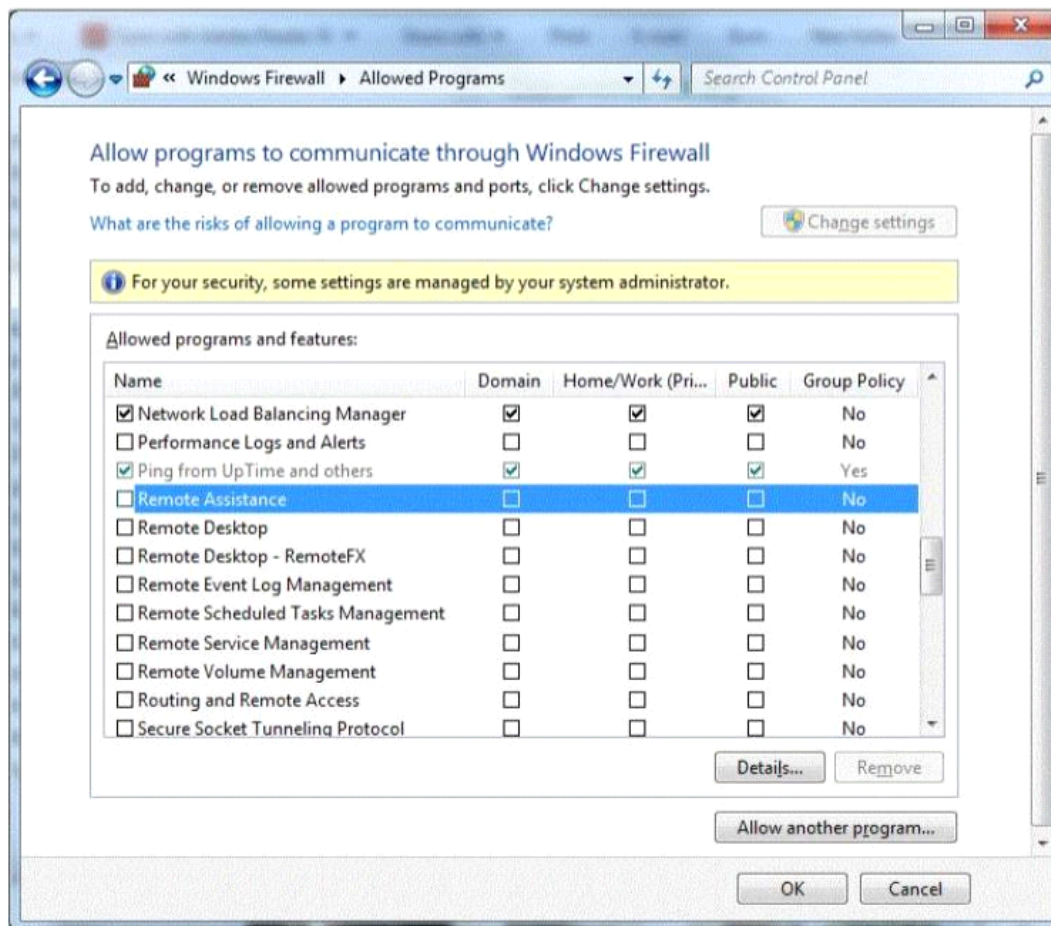
Explanation:

Reference:

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

Question: 51

You are setting up Remote Desktop on your computer. Your computer is a member of a domain. Your firewall configuration is shown in the following image:



You need to allow Remote Desktop to be able to get through your firewall for users on your company's network. Which settings should you enable?

- A. Remote Assistance: Home/Work (Private)
- B. Remote Desktop: Public
- C. Remote Desktop: Home/Work (Private)
- D. Remote Assistance: Domain

Answer: A

Question: 52

You are trying to connect to an FTP server on the Internet from a computer in a school lab. You cannot get a

connection. You try on another computer with the same results. The computers in the lab are able to browse the Internet.

You are able to connect to this FTP server from home.

What could be blocking the connection to the server?

- A. A layer-2 switch
- B. A wireless access point
- C. A firewall
- D. A layer-2 hub

Answer: C

Question: 53

What does NAT do?

- A. It encrypts and authenticates IP packets.
- B. It provides caching and reduces network traffic.
- C. It translates public IP addresses to private addresses and vice versa.
- D. It analyzes incoming and outgoing traffic packets.

Answer: C

Explanation:

Reference:

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

Question: 54

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
Smart cards can be used in biometrics-based systems.	<input type="radio"/>	<input type="radio"/>
Smart cards can be read from distances of several inches to many yards.	<input type="radio"/>	<input type="radio"/>
Smart cards provide a means of securely storing data on the card.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
Smart cards can be used in biometrics-based systems.	<input checked="" type="radio"/>	<input type="radio"/>
Smart cards can be read from distances of several inches to many yards.	<input type="radio"/>	<input checked="" type="radio"/>
Smart cards provide a means of securely storing data on the card.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 55

The default password length for a Windows Server domain controller is:

- A. 0
- B.5
- C.7
- D.14

Answer: C

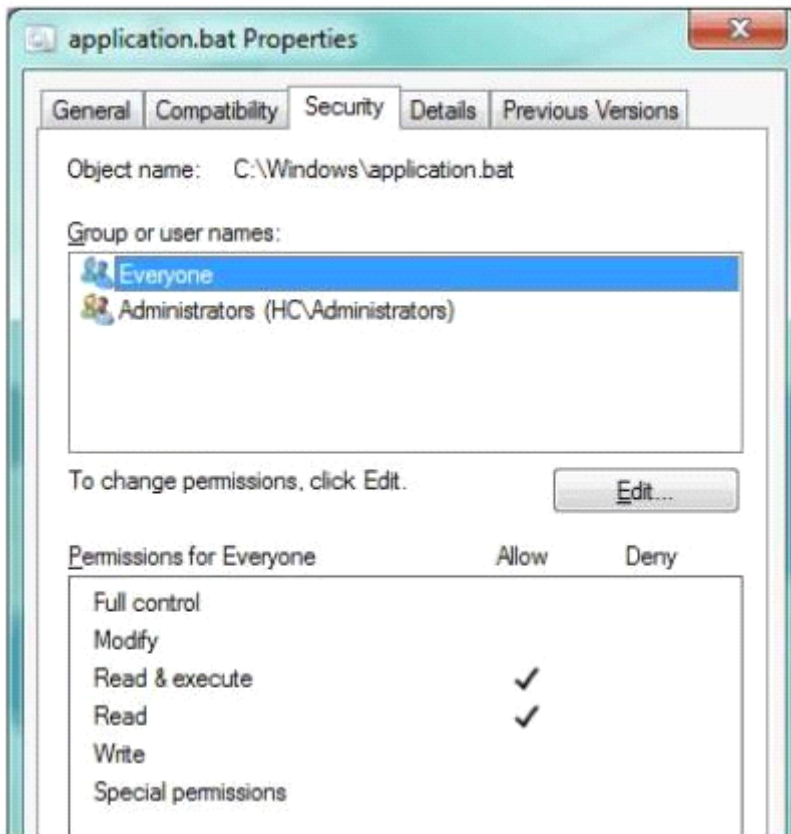
Question: 56

HOTSPOT

Your supervisor asks you to review file permission settings on the application.bat file.

You need to report which file system the file is on and the type of permission the file has.

You review the application Properties dialog box 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 "cygwin.bat" file in the image is currently on the [answer choice] file system.

[answer choice] permissions are currently being displayed for the "cygwin.bat" file.

Answer Area

The "cygwin.bat" file in the image is currently on the [answer choice] file system.

- FAT16
- FAT32
- NTFS

[answer choice] permissions are currently being displayed for the "cygwin.bat" file.

- Basic
- Advanced
- Full Control

Answer:

Answer Area

The "cygwin.bat" file in the image is currently on the [answer choice] file system.

[answer choice] permissions are currently being displayed for the "cygwin.bat" file.

Question: 57**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
There are several built-in basic audit policies and advanced audit policies in Windows.	<input type="radio"/>	<input type="radio"/>
Advanced audit policies applied by a Group Policy are compatible with a basic audit policy.	<input type="radio"/>	<input type="radio"/>
A system access control list (SACL) enables administrators to log attempts to access a secured object.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
There are several built-in basic audit policies and advanced audit policies in Windows.	<input checked="" type="radio"/>	<input type="radio"/>
Advanced audit policies applied by a Group Policy are compatible with a basic audit policy.	<input type="radio"/>	<input checked="" type="radio"/>
A system access control list (SACL) enables administrators to log attempts to access a secured object.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 58

You create a web server for your school. When users visit your site, they get a certificate error that says your site is not trusted.

What should you do to fix this problem?

A. Install a certificate from a trusted Certificate Authority (CA).

- B. Use a digital signature.
- C. Generate a certificate request.
- D. Enable Public Keys on your website.

Answer: A

Question: 59

What is an example of non-propagating malicious code?

- A. A back door
- B. A hoax
- C. A Trojan horse
- D. A worm

Answer: A

Question: 60

A brute force attack:

- A. Uses response filtering
- B. Tries all possible password variations
- C. Uses the strongest possible algorithms
- D. Targets all the ports

Answer: B

Question: 61

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
FAT32 has built-in security features that control user access.	<input type="radio"/>	<input type="radio"/>
NTFS has built-in security features that control file access.	<input type="radio"/>	<input type="radio"/>
All users on the same FAT32 file system have access rights to all files.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
FAT32 has built-in security features that control user access.	<input type="radio"/>	<input checked="" type="radio"/>
NFTS has built-in security features that control file access.	<input checked="" type="radio"/>	<input type="radio"/>
All users on the same FAT32 file system have access rights to all files.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 62

Humongous Insurance is an online healthcare insurance company. During an annual security audit a security firm tests the strength of the company's password policy and suggests that Humongous Insurance implement password history policy.

What is the likely reason that the security firm suggests this?

- A. Past passwords were easily cracked by the brute force method.
- B. Past passwords of users contained dictionary words.
- C. Previous password breaches involved use of past passwords.
- D. Past passwords lacked complexity and special characters.

Answer: B

Question: 63

The WPA2 PreShared Key (PSK) is created by using a passphrase (password) and salting it with the WPS PIN. 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. Service Set Identifier (SSID)
- B. Admin password
- C. WEP key
- D. No change is needed

Answer: A

Question: 64

What are three major attack vectors that a social engineering hacker may use? (Choose three.)

- A. Telephone
- B. Reverse social engineering
- C. Waste management
- D. Honey pot systems
- E. Firewall interface

Answer: A, B, C

Question: 65

Which two security settings can be controlled by using group policy? (Choose two.)

- A. Password complexity
- B. Access to the Run... command
- C. Automatic file locking
- D. Encrypted access from a smart phone

Answer: A, B

Explanation:

Reference:

<http://technet.microsoft.com/en-us/library/cc875814.aspx>

Question: 66

Cookies impact security by enabling: (Choose two.)

- A. Storage of Web site passwords.
- B. Higher security Web site protections.
- C. Secure Sockets Layer (SSL).
- D. Web sites to track browsing habits.

Answer: A, D

Explanation:

Reference:

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

Question: 67

To keep third-party content providers from tracking your movements on the web, enable InPrivate Browsing. 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. InPrivate Filtering
- B. SmartScreen Filter
- C. Compatibility Mode
- D. No change is needed

Answer: A

Question: 68

Which enables access to all of the logged-in user's capabilities on a computer?

- A. Java applets
- B. ActiveX controls
- C. Active Server Pages (ASP)
- D. Microsoft Silverlight

Answer: B

Question: 69

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
BitLocker to Go Reader allows you to encrypt drives.	<input type="radio"/>	<input type="radio"/>
BitLocker to Go Reader requires drives that are encrypted using a password.	<input type="radio"/>	<input type="radio"/>
BitLocker to Go works on Windows Vista and Windows XP.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
BitLocker to Go Reader allows you to encrypt drives.	<input type="radio"/>	<input checked="" type="radio"/>
BitLocker to Go Reader requires drives that are encrypted using a password.	<input checked="" type="radio"/>	<input type="radio"/>
BitLocker to Go works on Windows Vista and Windows XP.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 70

You need to install a domain controller in a branch office. You also need to secure the information on the domain controller. You will be unable to physically secure the server.
Which should you implement?

- A. Read-Only Domain Controller
- B. Point-to-Point Tunneling Protocol (PPTP)
- C. Layer 2 Tunneling Protocol (L2TP)

D.Server Core Domain Controller

Answer: A

Explanation:

A read-only domain controller (RODC) is a new type of domain controller in the Windows Server® 2008 operating system. With an RODC, organizations can easily deploy a domain controller in locations where physical security cannot be guaranteed. An RODC hosts read-only partitions of the Active Directory® Domain Services (AD DS) database.

Explanation: [http://technet.microsoft.com/en-us/library/cc732801\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx)

Question: 71

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

Explanation:

Reference:

<http://www.microsoft.com/mscorp/safety/technologies/senderid/technology.mspx>

Question: 72

What is the primary advantage of using Active Directory Integrated Zones?

- A. Zone encryption
- B. Password protection
- C. Non-repudiation
- D. Secure replication

Answer: D

Explanation:

Reference:

<http://books.google.com/books?id=CY-2LBZCVgC&pg=PA201&dq=%22Active+Directory+Integrated+Zones%22,+Secure+replication&hl=en&sa=X&ei=9s92U-v1KI-zyASjzILIDg&ved=0CE0Q6AEwAQ#v=onepage&q=%22Active%20Directory%20Integrated%20Zones%22%2C%20Secure%20replication&f=false>

Question: 73

Which two are included in an enterprise antivirus program? (Choose two.)

- A. Attack surface scanning
- B. On-demand scanning
- C. Packet scanning
- D. Scheduled scanning

Answer: B, D

Question: 74

Phishing is an attempt to:

- A. Obtain information by posing as a trustworthy entity.
- B. Limit access to e-mail systems by authorized users.
- C. Steal data through the use of network intrusion.
- D. Corrupt e-mail databases through the use of viruses.

Answer: A

Explanation:

Phishing is the act of attempting to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Question: 75

Humongous Insurance needs to set up a domain controller in a branch office. Unfortunately, the server cannot be sufficiently secured from access by employees in that office, so the company is installing a Primary Domain Controller. 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. Read-Only Domain Controller
- B. Backup Domain Controller
- C. Active Directory Server
- D. No change is needed.

Answer: A

Question: 76

Where should you lock up the backup tapes for your servers?

- A. The server room
- B. A filing cabinet
- C. The tape library
- D. An offsite fire safe

Answer: D

Explanation:

Backup tapes should be stored off site, preferably in a fire safe, so that the data is available should a fire, flood, or

other disaster affect the location were the servers are.

Question: 77

Which is a special folder permission?

- A. Read
- B.Modify
- C.Write
- D.Delete

Answer: D

Explanation:

Reference:

<http://support.microsoft.com/kb/308419>

Question: 78

When conducting a security audit the first step is to:

- A. Inventory the company's technology assets
- B.Install auditing software on your servers
- C.Set up the system logs to audit security events
- D.Set up a virus quarantine area

Answer: A

Question: 79

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

Explanation:

Reference:

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

Question: 80

You need to grant a set of users write access to a file on a network share. You should add the users to:

- A. A security group
- B.The Authenticated Users group
- C.The Everyone group
- D.A distribution group

Answer: B

Question: 81

The certificate of a secure public Web server on the Internet should be:

- A. Issued by a public certificate authority (CA)
- B.Signed by using a 4096-bit key
- C.Signed by using a 1024-bit key
- D.Issued by an enterprise certificate authority (CA)

Answer: A

Question: 82

Setting a minimum password age restricts when users can:

- A. Request a password reset
- B.Change their passwords
- C.Log on by using their passwords
- D.Set their own password expiration

Answer: B

Explanation:

Configure the minimum password age to be more than 0 if you want Enforce password history to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite.

Question: 83

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
If your computer is on a domain, your network administrator can reset your password.	<input type="radio"/>	<input type="radio"/>
An administrator account can reset a password for a standard user account.	<input type="radio"/>	<input type="radio"/>
There is a risk of losing access to encrypted files if a password is reset.	<input type="radio"/>	<input type="radio"/>

Answer:**Answer Area**

	Yes	No
If your computer is on a domain, your network administrator can reset your password.	<input checked="" type="radio"/>	<input type="radio"/>
An administrator account can reset a password for a standard user account.	<input checked="" type="radio"/>	<input type="radio"/>
There is a risk of losing access to encrypted files if a password is reset.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 84

Basic security questions used to reset a password are susceptible to:

- A. Hashing
- B. Social engineering
- C. Network sniffing
- D. Trojan horses

Answer: B

Explanation:

Reference:

http://en.wikipedia.org/wiki/Self-service_password_reset

Question: 85

You suspect a user's computer is infected by a virus.
What should you do first?

- A. Restart the computer in safe mode
- B. Replace the computer's hard disk drive
- C. Disconnect the computer from the network
- D. Install antivirus software on the computer

Answer: D

Question: 86

You create a new file in a folder that has inheritance enabled.
By default, the new file:

- A. Takes the permissions of the parent folder
- B. Does not take any permissions
- C. Takes the permissions of other folders in the same directory
- D. Takes the permissions of other files in the same directory

Answer: A

Explanation:

Reference:

https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/acl_inherit_permissions.mspx?mfr=true

Question: 87

Password history policies are used to prevent:

- A. Brute force attacks
- B. Users from sharing passwords
- C. Social engineering
- D. Passwords from being reused immediately

Answer: D

Explanation:

This security setting determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords.

This policy enables administrators to enhance security by ensuring that old passwords are not reused continually.

Explanation:

Reference:

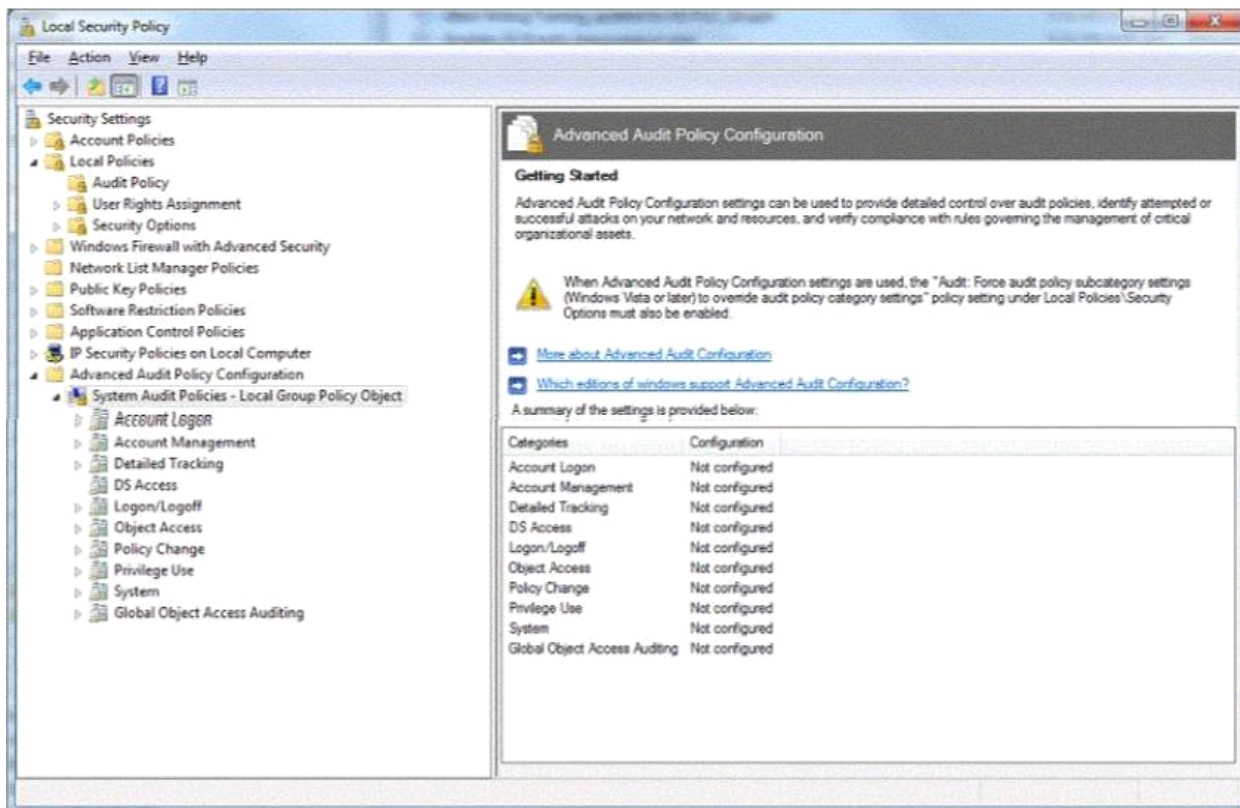
[http://technet.microsoft.com/en-us/library/cc758950\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc758950(v=ws.10).aspx)

Question: 88

HOTSPOT

You are preparing an audit policy for the workstations at Contoso, Ltd. Currently, no advanced auditing is enabled. The workstations are not members of the domain.

The settings of your Advanced Audit Policy Configuration are 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

To enable auditing of all local login events, you need to turn on the **[answer choice]** Advanced Audit Policy.

You need to know when someone accesses files in the c:\temp directory. Auditing is turned on for this directory. You need to enable the **[answer choice]** Advanced Audit Policy to log these events.

Answer Area

To enable auditing of all local login events, you need to turn on the **[answer choice]** Advanced Audit Policy.

Logon/Logoff
Account Logon
System

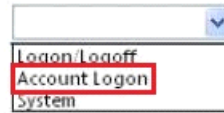
You need to know when someone accesses files in the c:\temp directory. Auditing is turned on for this directory. You need to enable the **[answer choice]** Advanced Audit Policy to log these events.

Object Access
Privilege Use
System

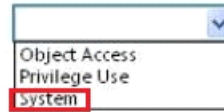
Answer:

Answer Area

To enable auditing of all local login events, you need to turn on the **[answer choice]** Advanced Audit Policy.



You need to know when someone accesses files in the c:\temp directory. Auditing is turned on for this directory. You need to enable the **[answer choice]** Advanced Audit Policy to log these events.

**Question: 89**

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: 90

Creating MD5 hash for files is an example of ensuring what?

- A. Confidentiality
- B. Availability
- C. Least privilege
- D. Integrity

Answer: D

Explanation:

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity.

Question: 91

Which three elements does HTTPS encrypt? (Choose three.)

- A. Browser cookies
- B. Server IP address
- C. Port numbers
- D. Website URL
- E. Login information

Answer: A, D, E

Explanation:

Reference:

<http://stackoverflow.com/questions/499591/are-https-urls-encrypted>

Question: 92

The company that you work for wants to set up a secure network, but they do not have any servers. Which three security methods require the use of a server? (Choose three.)

- A. 802.1x
- B.WPA2 Personal
- C.WPA2 Enterprise
- D.RADIUS
- E.802.11ac

Answer: A, C, D

Question: 93

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

Explanation:

Reference:

<http://technet.microsoft.com/en-us/library/cc875841.aspx>

Question: 94

Dumpster diving refers to a physical threat that a hacker might use to look for information about a computer network. 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. Phishing
- B.Malware
- C.Reverse Social engineering
- D.No change is needed

Answer: D

Question: 95

An attorney hires you to increase the wireless network security for the law firm's office. The office has a very basic network, with just a modem and a router.

Which of these security modes offers the highest security?

- A. WPA-Personal
- B. WEP
- C. WPA2-Personal
- D. WPA-Enterprise

Answer: C

Question: 96

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

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

Internet
Local Intranet
Restricted Sites

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

change the security level on Local Intranet.
change the security level on Internet.
uncheck Enable Protected Mode.

Answer:

First answer – Local Intranet

Second answer – change the security level on Local Intranet

Question: 97**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
By using NAP, administrators can place non-compliant computers onto restricted networks.	<input type="radio"/>	<input type="radio"/>
All computers that are not in compliance with NAP policies require manual intervention to be brought into compliance.	<input type="radio"/>	<input type="radio"/>
NAP can enforce that client computers are running a firewall.	<input type="radio"/>	<input type="radio"/>

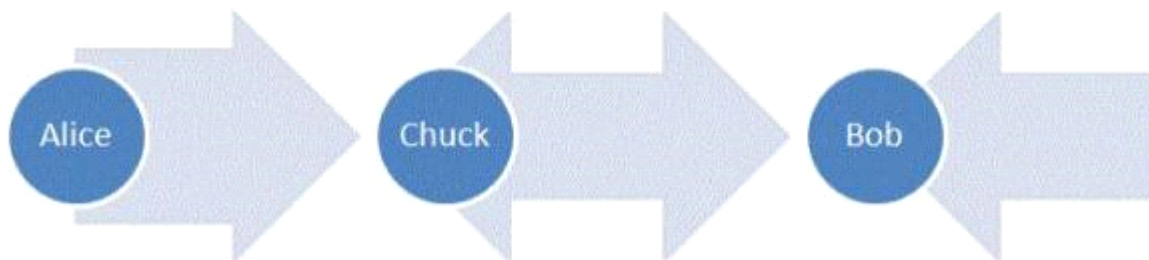
Answer:

Answer Area

	Yes	No
By using NAP, administrators can place non-compliant computers onto restricted networks.	<input checked="" type="radio"/>	<input type="radio"/>
All computers that are not in compliance with NAP policies require manual intervention to be brought into compliance.	<input type="radio"/>	<input checked="" type="radio"/>
NAP can enforce that client computers are running a firewall.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 98**HOTSPOT**

Alice and Bob are exchanging messages with each other. Chuck modifies the messages sent between Alice and Bob 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 [answer choice] attack.

Alice and Bob could add a [answer choice] to avoid this type of attack.

Answer Area

The scenario demonstrated is a [answer choice] attack.

- man in the middle
- phishing
- denial of service

Alice and Bob could add a [answer choice] to avoid this type of attack.

- checksum
- digital signature
- timestamp

Answer:

First answer – man in the middle
 Second answer – digital signature

Explanation:

The usual way to prevent the man-in-the-middle attack is to use a public key cryptosystem capable of providing digital signatures. For set up, the parties must know each others public keys in advance. After the shared secret has been generated, the parties send digital signatures of it to each other. The man-in-the-middle can attempt to forge these signatures, but fails because he cannot fake the signatures.

Question: 99

Which type of firewall allows for inspection of all characteristics of a packet?

- A. NAT
- B.Stateful
- C.Stateless
- D.Windows Defender

Answer: B

Explanation:

Reference:

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

Question: 100

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
DNSSEC prevents spoofing of query responses.	<input type="radio"/>	<input type="radio"/>
Clients can verify that the DNS server that they are communicating with is legitimate.	<input type="radio"/>	<input type="radio"/>
DNSSEC prevents man-in-the-middle attacks for DNS queries.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
DNSSEC prevents spoofing of query responses.	<input checked="" type="radio"/>	<input type="radio"/>
Clients can verify that the DNS server that they are communicating with is legitimate.	<input checked="" type="radio"/>	<input type="radio"/>
DNSSEC prevents man-in-the-middle attacks for DNS queries.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 101

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: 102**

You are an intern and are working remotely.
 You need a solution that meets the following requirements:
 Allows you to access data on the company network securely
 Gives you the same privileges and access as if you were in the office
 What are two connection methods you could use? (Choose two.)

- A. Forward Proxy
- B. Virtual Private Network (VPN)
- C. Remote Access Service (RAS)
- D. Roaming Profiles

Answer: B, D**Question: 103**

Network Access Protection (NAP) enables administrators to control access to network resources based on a computer's:

- A. Encryption level
- B. Warranty
- C. Physical location
- D. Configuration

Answer: D

Explanation:

Network Access Protection (NAP) is a new set of operating system components included with the Windows Server® 2008 and Windows Vista® operating systems that provides a platform to help ensure that client computers on a private network meet administrator-defined requirements for system health. NAP policies define the required configuration and update status for a client computer's operating system and critical software. For example, computers might be required to have antivirus software with the latest signatures installed, current operating system updates installed, and a host-based firewall enabled. By enforcing compliance with health requirements, NAP can help network administrators mitigate some of the risk caused by improperly configured client computers that might be exposed to viruses and other malicious software.

Question: 104

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: 105

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: 106

Which attack listens to network traffic of a computer resource?

- A. Resource gathering
- B. Denial of service
- C. ARP poisoning

- D.Eavesdropping
- E.Logic bomb

Answer: D

Explanation:

Eavesdropping

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Question: 107

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: 108

A network sniffer is software or hardware that:

- A. Records user activity and transmits it to the server
- B.Captures and analyzes network communication
- C.Protects workstations from intrusions
- D.Catalogs network data to create a secure index

Answer: B

Explanation:

A network sniffer is a computer tool that captures network data in the form of low-level packets. Network sniffers can be used for technical troubleshooting and analyzing the communication.

Question: 109

What is a service set identifier (SSID)?

- A. A wireless encryption standard
- B. The wireless LAN transmission type
- C. The broadcast name of an access point
- D. A wireless security protocol

Answer: C

Explanation:

SSID (service set identifier) is a function performed by an Access Point that transmits its name so that wireless stations searching for a network connection can 'discover' it. It's what allows your wireless adapter's client manager program or Windows built-in wireless software to give you a list of the Access Points in range.

Question: 110

To implement WPA2 Enterprise, you would need a/an:

- A. RADIUS server
- B. SSL server
- C. WEP server
- D. VPN server

Answer: A

Question: 111

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
To protect users from untrusted browser pop-ups, you may set a default browser configuration that blocks all pop-ups and automated downloads.	<input type="radio"/>	<input type="radio"/>
Online pop-ups and dialog boxes can display a realistic operating system or application error messages.	<input type="radio"/>	<input type="radio"/>
Protecting users from untrusted pop-up applications is mostly a function of awareness.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

	Yes	No
To protect users from untrusted browser pop-ups, you may set a default browser configuration that blocks all pop-ups and automated downloads.	<input type="radio"/>	<input checked="" type="radio"/>
Online pop-ups and dialog boxes can display a realistic operating system or application error messages.	<input checked="" type="radio"/>	<input type="radio"/>
Protecting users from untrusted pop-up applications is mostly a function of awareness.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 112

You would implement a wireless intrusion prevention system to:

- A. Prevent wireless interference
- B. Detect wireless packet theft
- C. Prevent rogue wireless access points
- D. Enforce SSID broadcasting

Answer: C

Explanation:

Reference:

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

Question: 113

The manager of a coffee shop hires you to securely set up WiFi in the shop.
To keep computer users from seeing each other, what should you use with an access point?

- A. Client bridge mode
- B. Client isolation mode
- C. MAC address filtering
- D. Client mode

Answer: B

Explanation:

Wireless Client Isolation is a unique security feature for wireless networks. When Client Isolation is enabled any and all devices connected to the wireless LAN will be unable to talk to each other.

Question: 114

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: 115

How does the sender policy framework (SPF) aim to reduce spoofed email?

- A. It provides a list of IP address ranges for particular domains so senders can be verified.
- B.It includes an XML policy file with each email that confirms the validity of the message.
- C.It lists servers that may legitimately forward mail for a particular domain.
- D.It provides an encryption key so that authenticity of an email message can be validated

Answer: A

Question: 116

Windows Server Update Services (WSUS) is a tool that:

- A. Updates data stored in Windows servers
- B.Manages the services that run on a server
- C.Updates licensing for Windows servers
- D.Manages updates for Microsoft software

Answer: D

Explanation:

Windows Server Update Services (WSUS) enables information technology administrators to deploy the latest Microsoft product updates to computers that are running the Windows operating system. By using WSUS, administrators can fully manage the distribution of updates that are released through Microsoft Update to computers in their network.

Explanation:

Reference:

<http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx>

Question: 117

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

Explanation:

Reference:

<http://www.usewisdom.com/computer/passwords.html>

Question: 118

To protect systems from buffer overflow errors, you can use:

- A. Antivirus software
- B. Data Execution Prevention
- C. A proxy server
- D. An Intruder Prevention System

Answer: B

Question: 119

You sign up for an online bank account. Every 6 months, the bank requires you to change your password. You have changed your password 5 times in the past. Instead of coming up with a new password, you decide to use one of your past passwords, but the bank's password history prevents you on doing so.

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. Minimum password age
- B. Maximum password duration
- C. Password complexity
- D. No change is needed.

Answer: D

Question: 120

You need to prevent unauthorized users from reading a specific file on a portable computer if the portable computer is stolen.

What should you implement?

- A. File-level permissions
- B. Advanced Encryption Standard (AES)
- C. Folder-level permissions
- D. Distributed File System (DFS)
- E. BitLocker

Answer: E

Explanation:

Reference:

<http://4sysops.com/archives/seven-reasons-why-you-need-bitlocker-hard-drive-encryption-for-your-whole-organization/>

Question: 121

Your password is 1Vu*cl!8sT.

Which attack method is your password vulnerable to?

- A. Rainbow table
- B. Brute force
- C. Spidering
- D. Dictionary

Answer: A

Question: 122

You have a Windows 7 desktop computer, and you create a Standard User account for your roommate so that he can use the desktop from time to time. Your roommate has forgotten his password.

Which two actions can you take to reset the password? (Choose two.)

- A. Use your password reset disk.
- B. Use your administrator account.
- C. Boot into Safe Mode with your roommate's account.
- D. From your roommate's account press CTRL+ALT+DELETE, and then click Change a password.

Answer: A, B

Question: 123

You have two servers that run Windows Server. All drives on both servers are formatted by using NTFS.

You move a file from one server to the other server. The file's permissions in the new location will:

- A. Enable full access to the everyone group
- B. Restrict access to the Administrators group
- C. Inherit the destination folder's permissions
- D. Retain the original folder's permissions

Answer: C

Explanation:

You can modify how Windows Explorer handles permissions when objects are copied or moved to another NTFS volume. When you copy or move an object to another volume, the object inherits the permissions of its new folder.