98-367.88q

Number: 98-367
Passing Score: 800
Time Limit: 120 min

98-367

Security fundamentals

Exam A

QUESTION 1

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2

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

Correct Answer: B
Section: (none)

Explanation

Explanation/Reference:
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 3
Physically securing servers prevents:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:
Reference: http://blogs.technet.com/b/askds/archive/2008/08/25/removable-storage-group-policy-and-windows-server-2008-and-windows-vista.aspx

QUESTION 5
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 7
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 authenticationC. Enable NTLM authentication
D. No change is needed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

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 ControllerD. Application Server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

A user who receives a large number of emails selling prescription medicine is probably receiving <u>pharming mail</u>.

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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
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

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 13
Which password attack uses all possible alpha numeric combinations?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

A digitally signed e-mail message:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

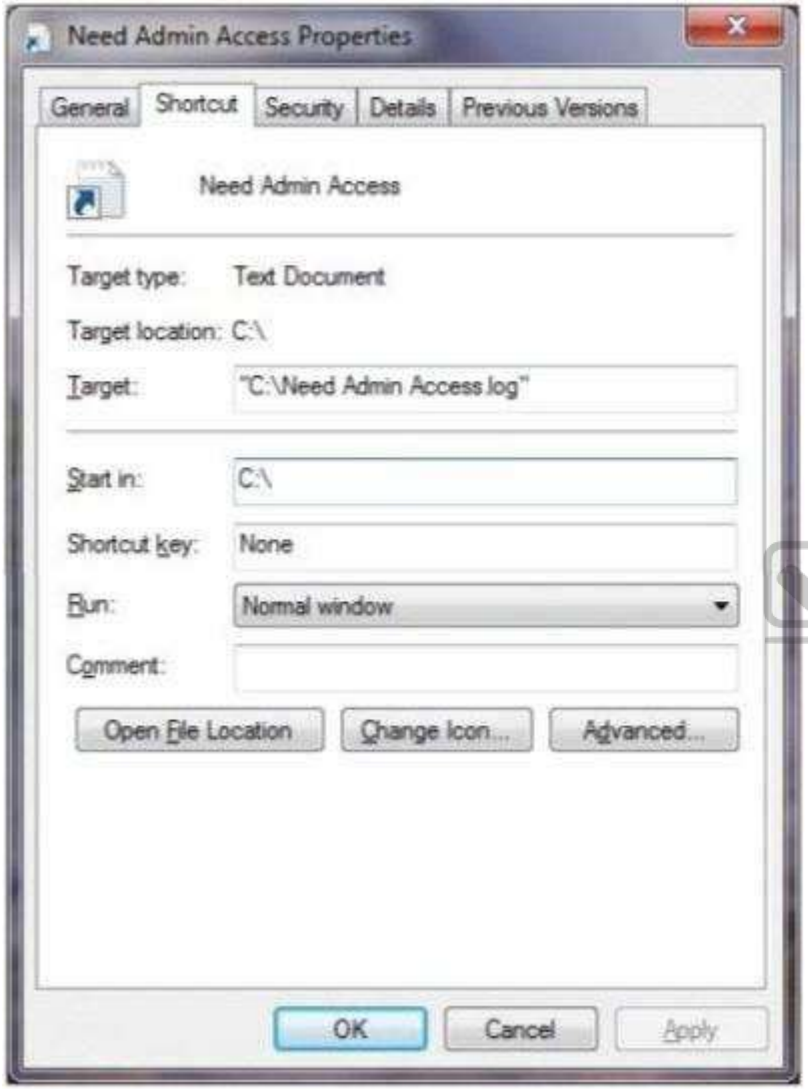
QUESTION 15

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:



Need Admin Access

Target type: Text Document

Target location: C:\

Target: "C:\Need Admin Access.log"

Start in: C:\

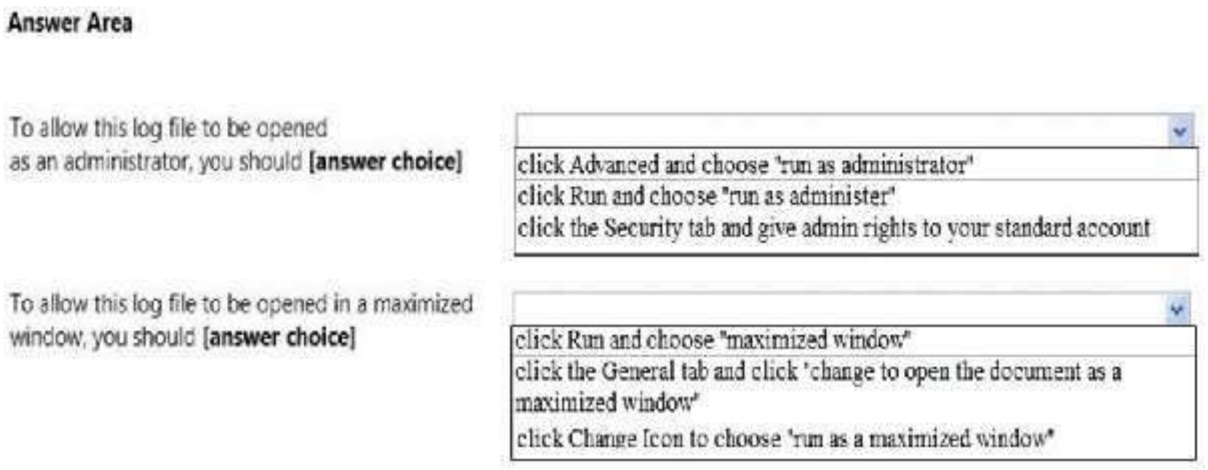
Shortcut key: None

Run: Normal window

Comment:

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

Hot Area:



Answer Area

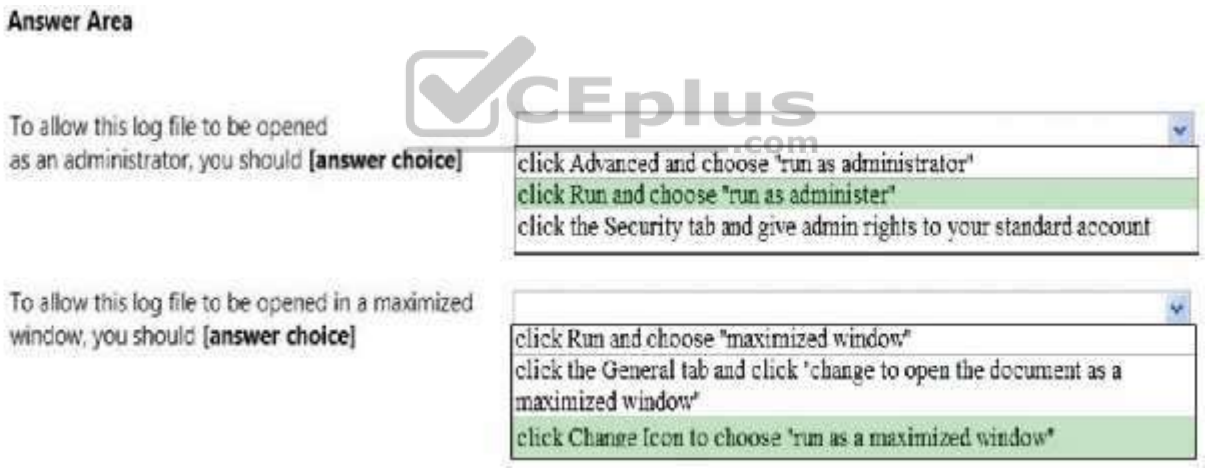
To allow this log file to be opened as an administrator, you should **[answer choice]**

- click Advanced and choose "run as administrator"
- click Run and choose "run as administer"
- 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"

Correct 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 administer"]
- 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"]

Section: (none)
Explanation

Explanation/Reference:

QUESTION 16

Passwords that contain recognizable words are vulnerable to a:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 17
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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

Correct Answer: ABE
Section: (none)
Explanation

Explanation/Reference:
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 20
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 22
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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 23
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

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

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx

QUESTION 26
Keeping a server updated:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: http://technet.microsoft.com/en-us/library/bb681008.aspx

QUESTION 28
What is a common method for password collection?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 30

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

What is an example of non-propagating malicious code?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
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

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:
Reference: http://technet.microsoft.com/en-us/library/cc875814.aspx

QUESTION 38
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.

Correct Answer: AD
Section: (none)
Explanation

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

QUESTION 39
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which enables access to all of the logged-in user's capabilities on a computer?

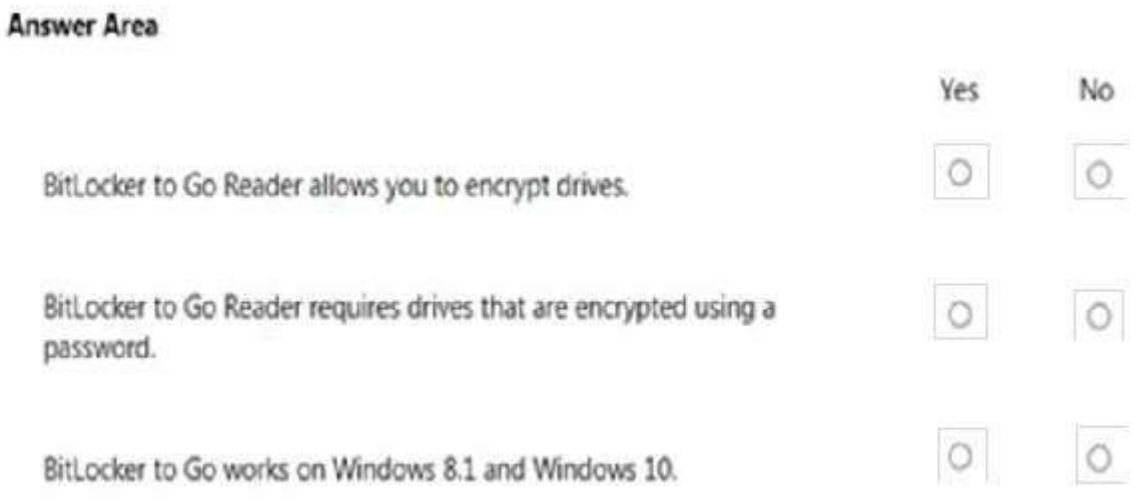
A. Java applets
B. ActiveX controls
C. Active Server Pages (ASP)
D. Microsoft Silverlight

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
HOTSPOT
For each of the following statements, select Yes if the statement is true. Otherwise, select No. Each correct selection is worth one point.

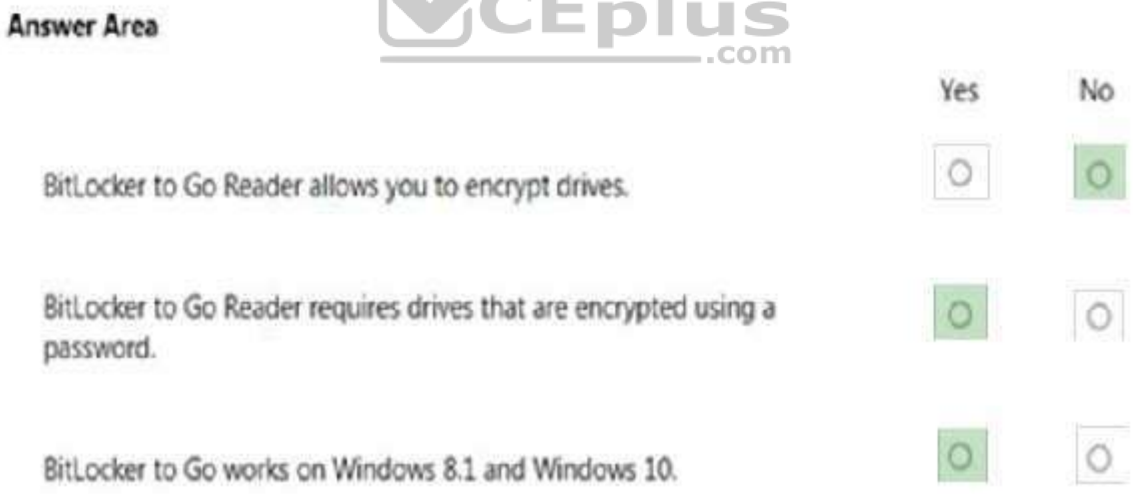
Hot Area:



Answer Area

	Yes	No
BitLocker to Go Reader allows you to encrypt drives.	○	○
BitLocker to Go Reader requires drives that are encrypted using a password.	○	○
BitLocker to Go works on Windows 8.1 and Windows 10.	○	○

Correct Answer:



Answer Area

	Yes	No
BitLocker to Go Reader allows you to encrypt drives.	○	●
BitLocker to Go Reader requires drives that are encrypted using a password.	●	○
BitLocker to Go works on Windows 8.1 and Windows 10.	●	○

Section: (none)

Explanation
Explanation/Reference:

QUESTION 42
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.

References: http://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx

QUESTION 43
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

Correct Answer: C

Section: (none)
Explanation

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

QUESTION 44
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 45
Which is a special folder permission?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: http://support.microsoft.com/kb/308419

QUESTION 46
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 48
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 51

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

A. Hashing
B. Social engineering
C. Network sniffingD. Trojan horses

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 52

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53

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

Correct Answer: A
Section: (none)
Explanation

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

QUESTION 54
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://technet.microsoft.com/en-us/library/cc758950(v=ws.10).aspx

QUESTION 55
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Creating MD5 hash for files is an example of ensuring what?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 57

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

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

Correct Answer: ADE
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 58

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

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59

Shredding documents helps prevent:

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 60
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 62
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 63
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 64
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 65
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 66
To implement WPA2 Enterprise, you would need a/an:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 68
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 69
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
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 70
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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.
Reference: http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx

QUESTION 72
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

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Reference: http://www.usewisdom.com/computer/passwords.html

QUESTION 73
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

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.

QUESTION 75

You need to be able to gather information about a running program.

Which type of auditing should you implement?

A. directory services
B. object access
C. logon events
D. process tracking

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76

The purpose of Windows Server Update Services (WSUS) is to:

A. manage the deployment of patches to company servers
B. provide alerts and reports on system vulnerabilities
C. set permissions to the minimum level necessary for each function
D. update licensing for Windows servers

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77

A process by which DNS zone data is obtained by an attacker is referred to as:

A. spoofing
B. footprinting
C. phishing
D. Denial of Service

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
DRAG DROP

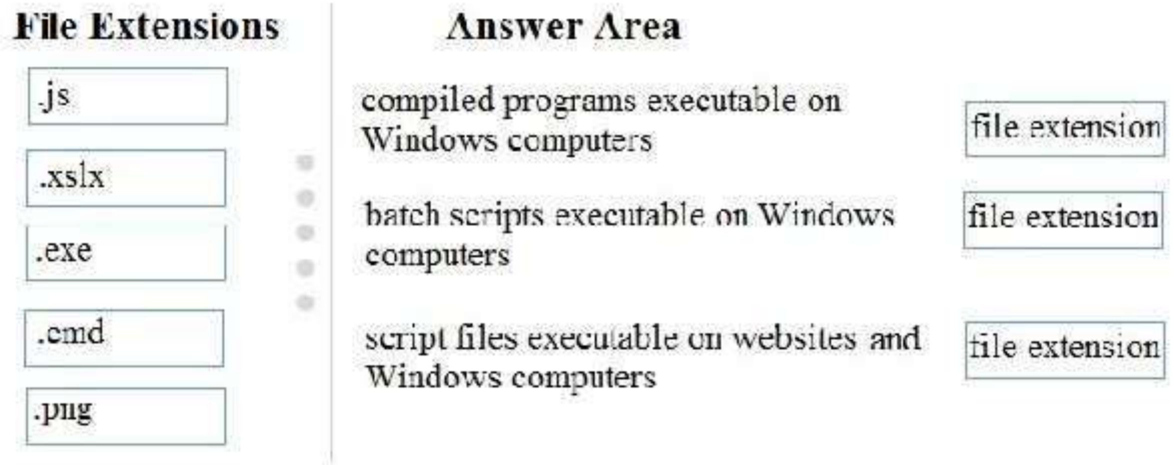
Certain potentially harmful file types should be filtered as attachments of incoming email messages.

Match the file extension that should be filtered with its description.

Instructions: To answer, drag the appropriate file extension from the column on the left to its description on the right. Each file extension may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Note: For each correct selection is worth one point.

Select and Place:



File Extensions

.js

.xslx

.exe

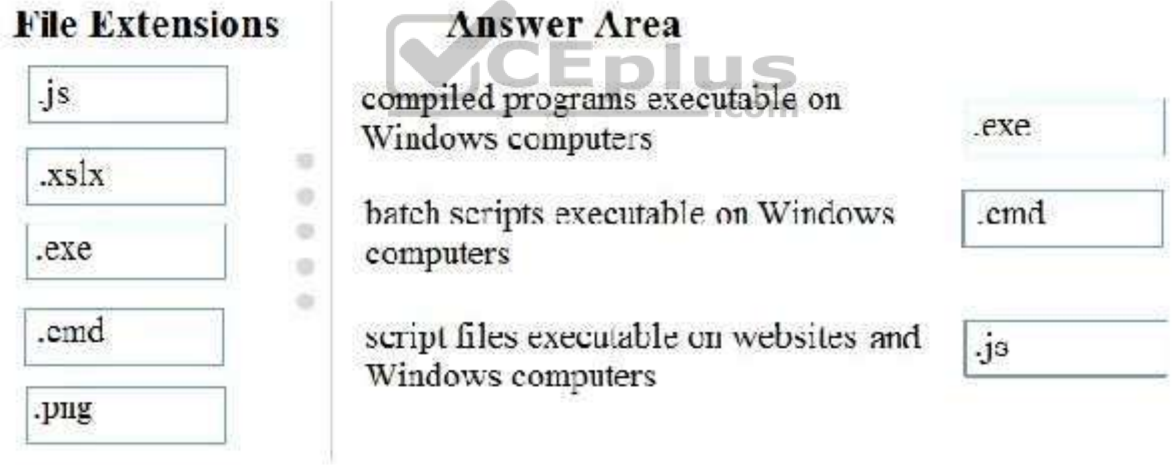
.cmd

.png

Answer Area

compiled programs executable on Windows computers	file extension
batch scripts executable on Windows computers	file extension
script files executable on websites and Windows computers	file extension

Correct Answer:



File Extensions

.js

.xslx

.exe

.cmd

.png

Answer Area

compiled programs executable on Windows computers	.exe
batch scripts executable on Windows computers	.cmd
script files executable on websites and Windows computers	.js

Section: (none)
Explanation

Explanation/Reference:

QUESTION 79

Media Access Control (MAC) filtering enables you to:

A. limit access to a network based on the client computer’s network adapter.
B. set access permissions to a shared folder.
C. prevent communications between specific IP addresses.
D. restrict communications to a specific website.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

What are two examples of physical site security? (Choose two.)

A. keeping machines in locked offices
B. sending backups to a remote location
C. enforcing multi-factor authentication
D. using BitLocker encryption on drives

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81

You need to hide internal IP addresses from the Internet while maintaining client access to the Internet.

What should you implement?

A. Port forwarding
B. Secure Sockets Layer (SSL)
C. Access Control Lists
D. Network Address Translation (NAT)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
A malicious user who intercepts and modifies communications is known as a:

A. red hat hacker
B. white hat hacker
C. network sniffer
D. man-in-the-middle

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
You have an application that uses IPsec to secure communications between an Internet client and a server on the internal network.

To which network security service must the IPsec client connect?

A. SFTP
B. SSH
C. VPN
D. RADIUS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84

You want to prevent external users from acquiring information about your network. You should implement a:

A. router
B. layer-3 switch
C. firewall
D. proxy server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

What are three examples of factors required for multi-factor authentication? (Choose three.)

A. a username
B. a smart card
C. a fingerprint
D. a password challenge question
E. a pin number

Correct Answer: ACE
Section: (none)
Explanation

Explanation/Reference:

References: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods

QUESTION 86

You are trying to enable BitLocker on your father's computer.

What is the purpose of the Trusted Platform Module (TPM) when it is used by BitLocker?

A. to store an encrypted file allocation table for the protected drive

B. to provide a co-processor that encrypts/decrypts data
C. to verify the integrity of the early boot components
D. to store the hashed data produced by BitLocker encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which type of password attack attempts to guess passwords by using a list of common passwords?

A. Keylogger
B. brute force
C. man-in-the-middle
D. dictionary

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Malicious software designed to collect personally identifiable information is referred to as :

A. spyware
B. a cookie
C. a network sniffer
D. freeware

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: