98-367.exam.71q

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

98-367

Security fundamentals

Exam A

QUESTION 1

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 2

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 3
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 4
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 5
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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 7
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 8
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 9
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 10
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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 12

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 13

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 14

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 15
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: http://technet.microsoft.com/en-us/library/bb727008.aspx

QUESTION 16
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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which enables you to change the permissions on a folder?

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

Correct Answer: D
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.)

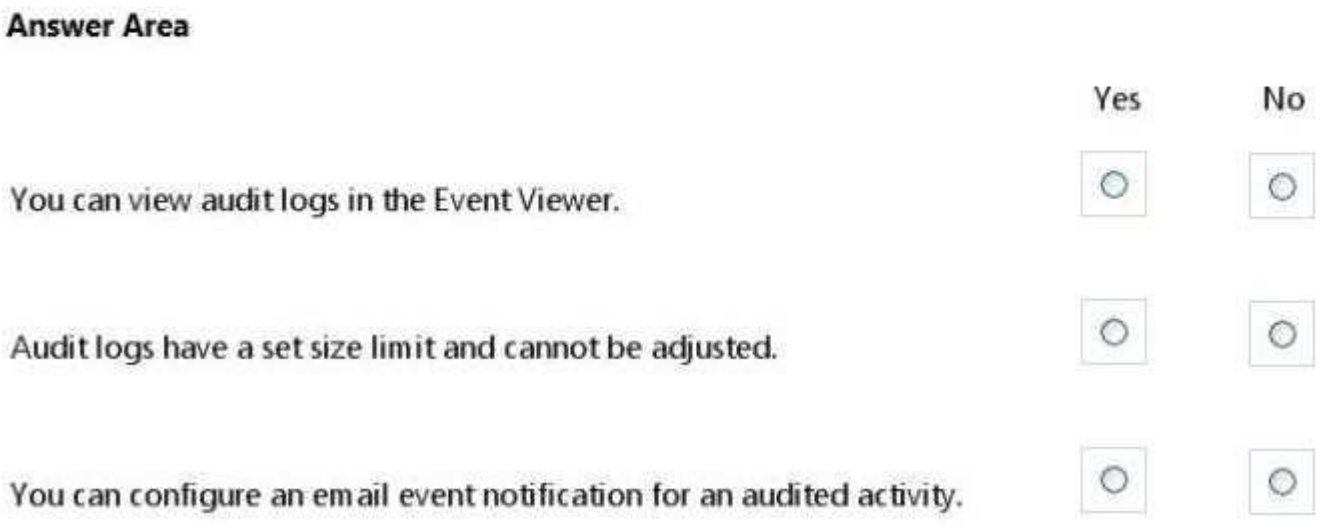
A. A fingerprint and a pattern
B. A password and a smart card
C. A username and a password
D. A password and a pin number
E. A pin number and a debit card

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

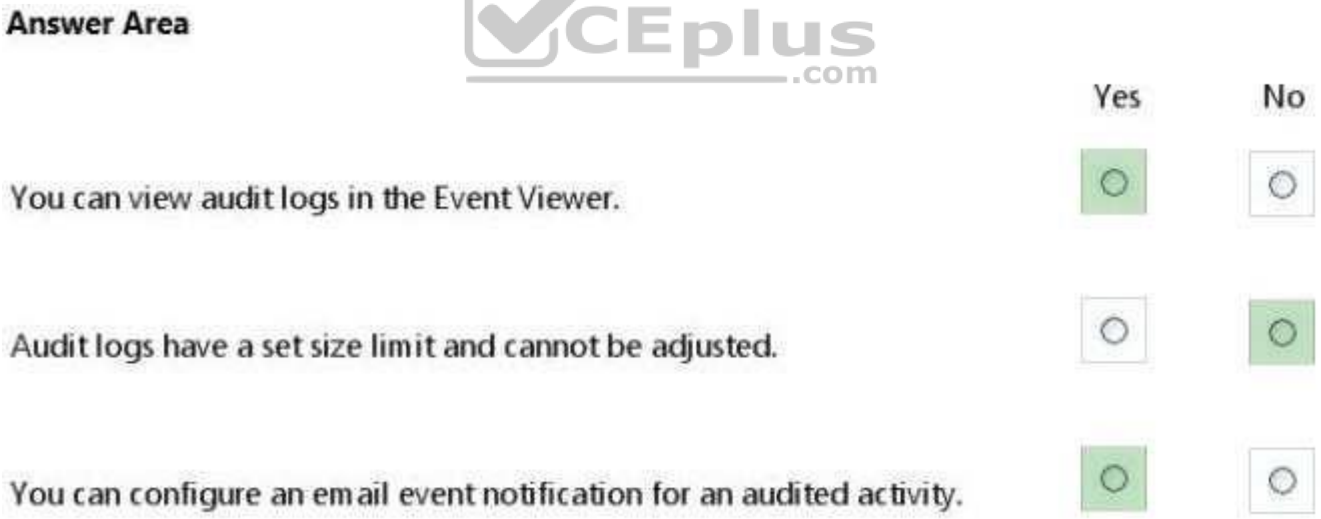
Hot Area:



Answer Area

	Yes	No
You can view audit logs in the Event Viewer.	○	○
Audit logs have a set size limit and cannot be adjusted.	○	○
You can configure an email event notification for an audited activity.	○	○

Correct Answer:



Answer Area

	Yes	No
You can view audit logs in the Event Viewer.	[✓ ○]	○
Audit logs have a set size limit and cannot be adjusted.	○	[✓ ○]
You can configure an email event notification for an audited activity.	[✓ ○]	○

Section: (none)
Explanation
Explanation/Reference:

QUESTION 21
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 22
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 23
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 24
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 25
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 26

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 27

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 28

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 29
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 30
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.

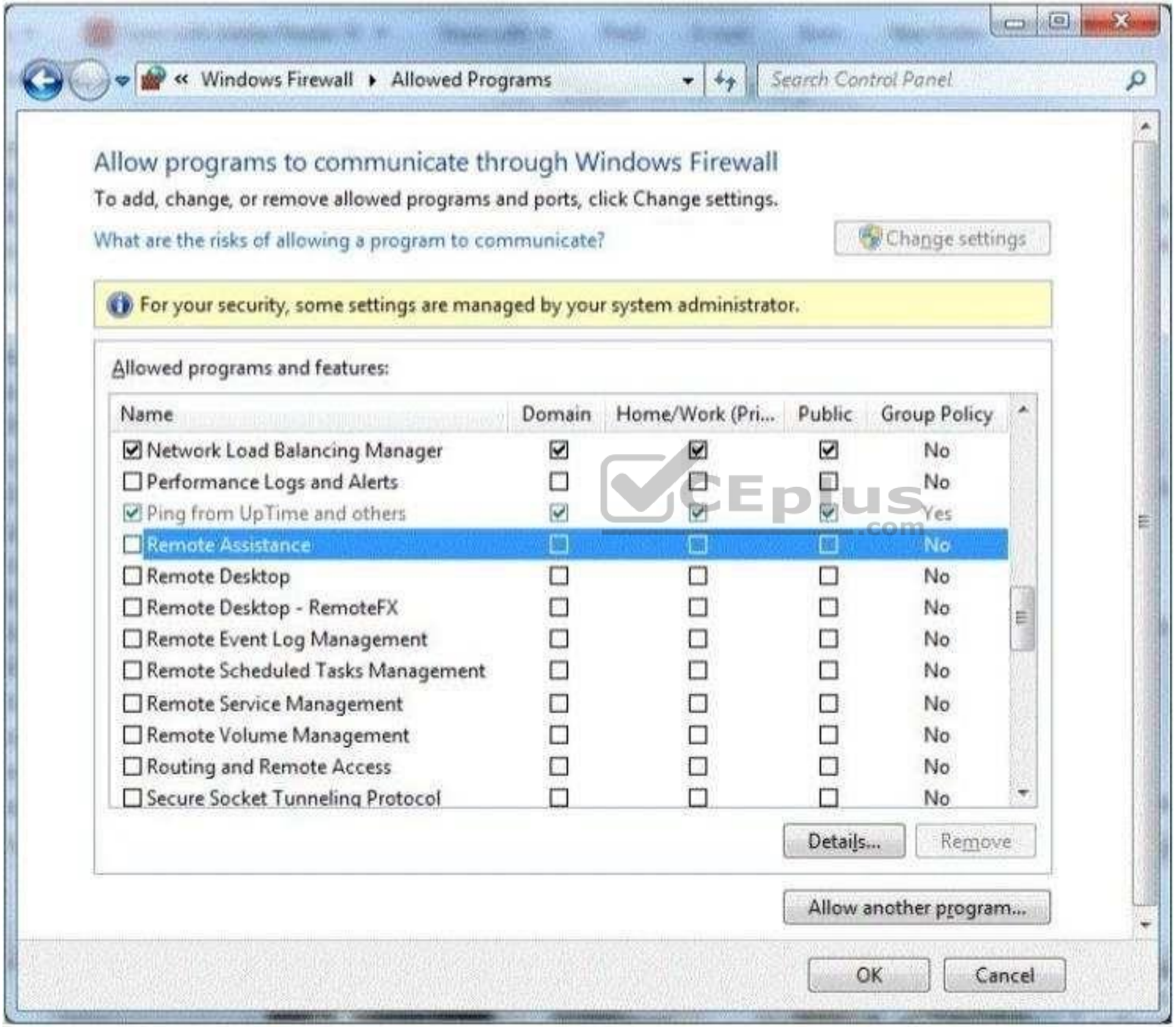
A. No change is needed
B. Certificates
C. IPsec
D. Biometrics

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 31
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:



Allow programs to communicate through Windows Firewall

To add, change, or remove allowed programs and ports, click Change settings.

What are the risks of allowing a program to communicate?

For your security, some settings are managed by your system administrator.

Allowed programs and features:

Name	Domain	Home/Work (Pri...	Public	Group Policy
☑ Network Load Balancing Manager	☑	☑	☑	No
□ Performance Logs and Alerts	□	□	□	No
☑ Ping from UpTime and others	☑	☑	☑	Yes
□ Remote Assistance	□	□	□	No
□ Remote Desktop	□	□	□	No
□ Remote Desktop - RemoteFX	□	□	□	No
□ Remote Event Log Management	□	□	□	No
□ Remote Scheduled Tasks Management	□	□	□	No
□ Remote Service Management	□	□	□	No
□ Remote Volume Management	□	□	□	No
□ Routing and Remote Access	□	□	□	No
□ Secure Socket Tunneling Protocol	□	□	□	No

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
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 34
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 35
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 36

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 37

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 38

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 systemsE. Firewall interface

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
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 40
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 41
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.
Explanation: http://technet.microsoft.com/en-us/library/cc732801(v=ws.10).aspx

QUESTION 42
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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 44
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
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 46
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 47
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 48
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 49
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 50
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 51
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 52
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 53
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 54
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 55
Password history policies are used to prevent:

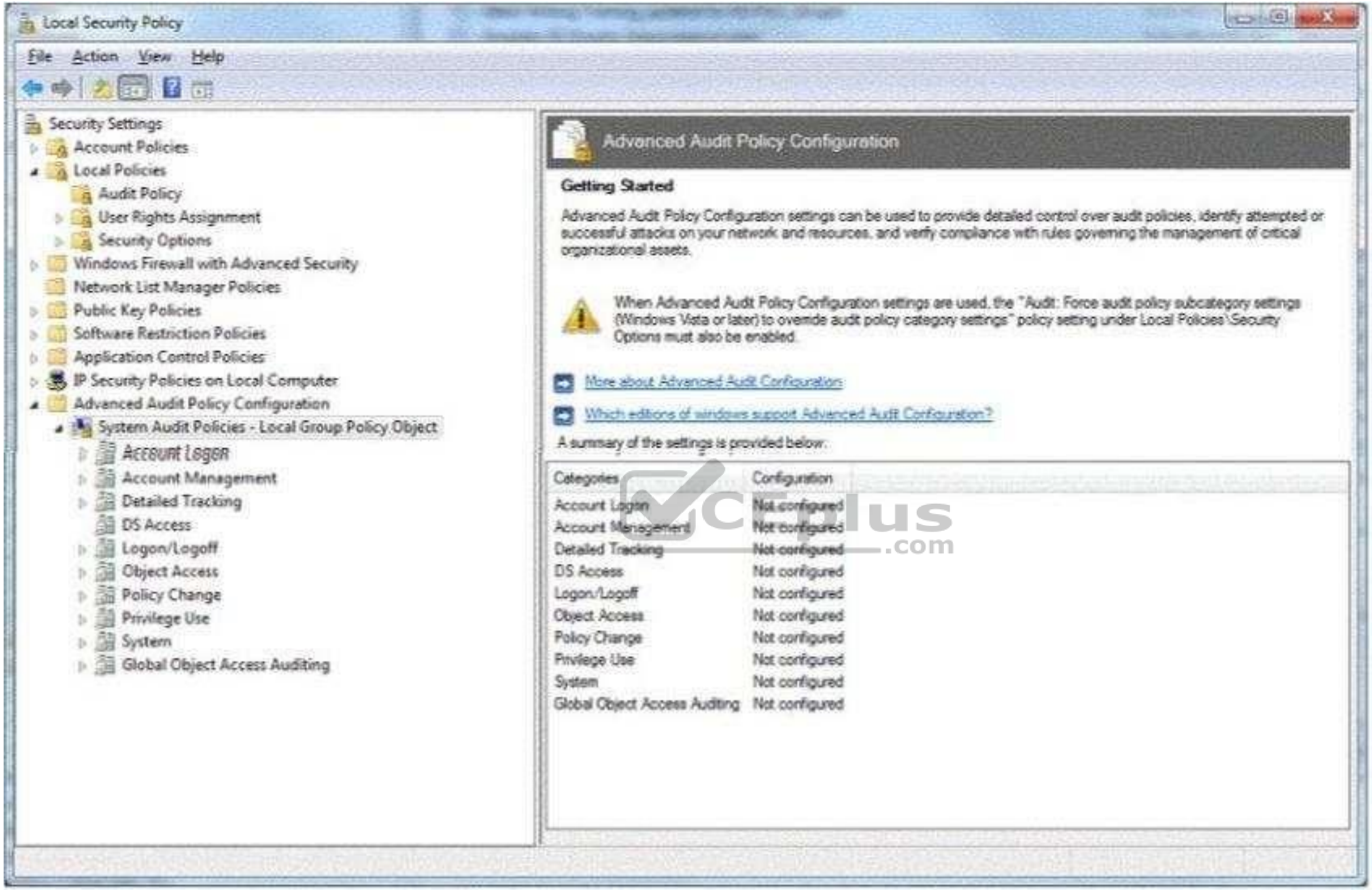
A. Brute force attacks
B. Users from sharing passwords
C. Social engineering
D. Passwords from being reused immediately

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 56
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:


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
System Audit Policies - Local Group Policy Object
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing

Advanced Audit Policy Configuration

Getting Started

Advanced Audit Policy Configuration settings can be used to provide detailed control over audit policies, identify attempted or successful attacks on your network and resources, and verify compliance with rules governing the management of critical organizational assets.

When Advanced Audit Policy Configuration settings are used, the "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" policy setting under Local Policies\Security Options must also be enabled.

More about Advanced Audit Configuration

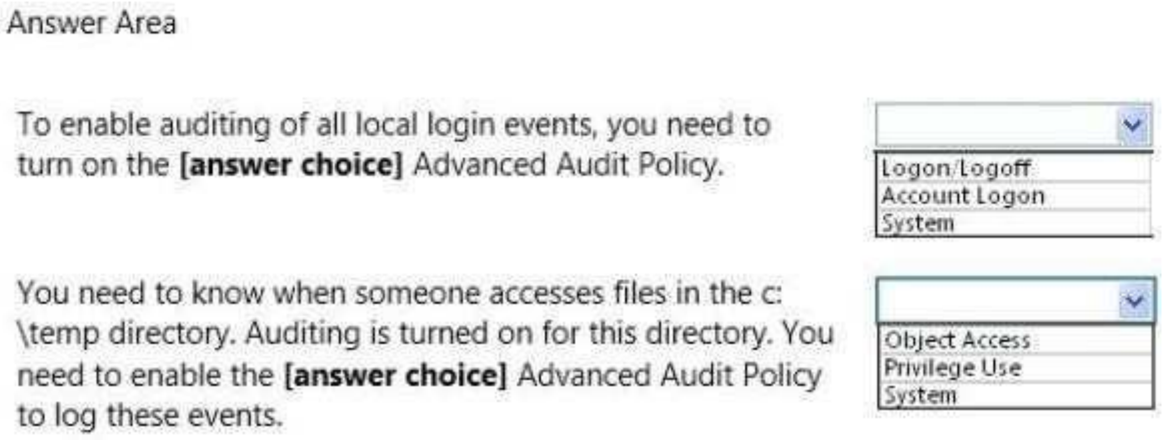
Which editions of windows support Advanced Audit Configuration?

A summary of the settings is provided below:

Categories	Configuration
Account Logon	Not configured
Account Management	Not configured
Detailed Tracking	Not configured
DS Access	Not configured
Logon/Logoff	Not configured
Object Access	Not configured
Policy Change	Not configured
Privilege Use	Not configured
System	Not configured
Global Object Access Auditing	Not configured

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

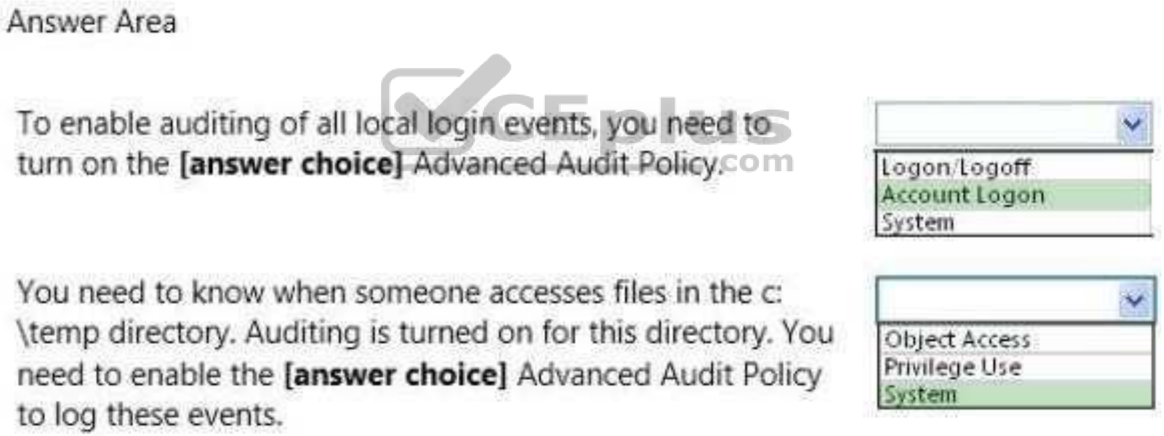
To enable auditing of all local login events, you need to turn on the **[answer choice]** Advanced Audit Policy.

- 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

Correct Answer:



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**

Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

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 58
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 59
Which type of firewall allows for inspection of all characteristics of a packet?

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

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 60
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
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 63
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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
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 64
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
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 66
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 67
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 68
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 69
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 70

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 71
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.