➢ Vendor: Microsoft

➢ Exam Code: 98-367

➢ Exam Name: Security Fundamentals

➢ Question 121 -- Question 150

QUESTION 121
Which of the following tools traces all or specific activities of a user on a computer?

A. Task Manager
B. Event Viewer
C. Network Monitor
D. Keylogger

Answer: D

QUESTION 122
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 123
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:
http://4sysops.com/archives/seven-reasons-why-you-need-bitlocker-hard-drive-encryption-for-your-whole-organization/

QUESTION 124
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 125
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 126
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 127
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 128
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.
http://office.microsoft.com/en-us/outlook-help/secure-messages-with-a-digital-signature-HP001230539.aspx

QUESTION 129
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.
http://searchsecurity.techtarget.com/definition/dictionary-attack

QUESTION 130
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 131
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:
http://blogs.technet.com/b/askds/archive/2008/08/25/removable-storage-group-policy-and-windows-server-2008-and-windows-vista.aspx

QUESTION 132
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 133
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:
http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing

QUESTION 134
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 135
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 136
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 137
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 138
Your Web server crashes at exactly the point where it reaches 1 million total visits. You discover the cause of the server crash is malicious code. Which description best fits this code?

A. Virus
B. Worm
C. Polymorphic Virus
D. Logic Bomb

Answer: D

QUESTION 139
Which of the following is the process of keeping track of a user's activity while accessing network resources?

A. Authentication
B. Auditing
C. Spoofing

D. Biometrics

Answer: B

QUESTION 140
The default password length for a Windows Server domain controller is:

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

Answer: C

QUESTION 141
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 142
Which is a special folder permission?

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

Answer: D
Explanation:
http://support.microsoft.com/kb/308419

QUESTION 143
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 144
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:
http://technet.microsoft.com/en-us/library/dd277400.aspx

QUESTION 145
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 146
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 147
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 148
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:
http://en.wikipedia.org/wiki/Self-service_password_reset

QUESTION 149
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 150
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