MU2b Authentication, Authorization and Accounting Questions Set 2

1. You enable the audit of successful and failed policy changes. Where can you view entries related to policy change attempts? Lesson 2 p 61 (also https://technet.microsoft.com/en-us/library/cc766468(v=ws.10).aspx) Your choices are:
    (1) Application event log
    (2) Security event log
    (3) System event log
    (4) Directory services event log

Auditing is not enabled by default in Windows. To enable auditing, you must specify what types of system events to audit using group policies or the local security policy (Security Settings\Local Policies\Audit Policy). See Figure 2-20. Table 2-3 shows the basic audit events that are available in Windows Server 2003 and 2008. Windows Server 2008 also has additional options for more granular control. After you enable logging, you then open the Event Viewer security logs to view the logged security events. By default, these logs can only be seen and managed by the Administrators group. The answer is: These entries related to policy change attempts can be found in the Security Event Log.

2. Implementing security auditing allows you to determine what? Your choices are:
    (5) Provide physical security for your network.
    (6) Force users to use strong passwords.
    (7) Implement a key logger.
    (8) Determine if a security breach has occurred.
    (9) Encrypt files to prevent unauthorized access.

This should help you determine the correct answer: http://www.enforcive.com/network-security-audit Think of a tax audit. What do auditors do? They look through tax files to see if any tax regulations have been violated.

It allows you to determine if a security breach has occurred. This is stated nowhere in the book, but this is the basic definition of what security auditing does.

3. Object access auditing is used to monitor what? Lesson 2 p 62. Your choices are:
    (10)Which users log on to the network.
    (11)Which users open specific files.
    (12)The amount of memory usage.
    (13)The amount of CPU usage.

Determines whether the OS audits user attempts to access non-Active Directory objects, including NTFS files, folders, and printers. The answer is object access monitoring is used to monitor which users open specific files.

4. For what purpose would you use security auditing to audit logon events? Lesson 2 p 71. Your choices are:

(14)To determine a user's effective permissions.
(15)to know when to reset a user's password
(16)to ensure that only authenticated users are accessing the network
(17)to detect a possible password attack

Account lockout refers to the number of incorrect logon attempts permitted before a system locks an account. Each bad logon attempt is tracked by the bad logon counter, and when the counter exceeds the account lockout threshold, no further logon attempts are permitted. This setting is critical because one of the most common password attacks (discussed later in the lesson) involves repeatedly attempting to log on with guessed passwords. The answer is you would use security auditing to audit logon events to detect a possible password attack.

5. Which type of certificate authority (CA) issues its own certificates? Lesson 4 p 47. Your choices are:
   (18)Issuing CA
   (19)Root CA
   (20)Subordinate CA
   (21)Policy CA

The Enterprise Root CA is at the top level of the certificate authority hierarchy. Once Enterprise Root CA is configured, it registers automatically within Active Directory, and all computers within the domain trust it. This authority will support auto enrollment and auto-renewal of digital certificates. –Think, if it is the highest in the hierarchy who would issue its certificates? The Root CA.

6. What will happen when you move a file you encrypted through the encrypting files system (EFS) to an unencrypted folder on an NTFS partition? Lesson 2 p 51-52. Your choices are:
   (22)The file remains encrypted.
   (23)An error is generated.
   (24)The file is automatically decrypted.
   (25)You are prompted to decrypt the file.

If someone steals a hard drive that is protected by NTFS permissions, that person could take the hard drive, put it in a system of which he or she is an administrator, and access all files and folders on the hard drive. Therefore, to truly protect a drive that could be stolen or accessed illegally, you can encrypt the files and folders on that drive. Encrypting File System (EFS) can encrypt files on an NTFS volume so that they cannot be used unless the user has access to the keys required to decrypt the information. After a file has been encrypted, you do not have to manually decrypt the encrypted file before you can use it. Rather, once you encrypt a file or folder, you work with the encrypted file or folder just as you would with any other file or folder. EFS is keyed to a specific user account, using the public and private keys that are the basis of the Windows public key infrastructure (PKI). The user who creates a file is the only person who can read it. As the user works, EFS encrypts the files he or she creates using a key generated from the user's public key. Data encrypted with this key can be decrypted only by the user's personal encryption certificate, which is generated using his or her private key. The answer is that the file remains encrypted.

7. A laptop computer running Windows Server 2008 does not have Trusted Platform Module (TPM) installed. You want to protect the data on the computer in case the computer is stolen. Which action should you take?
    (26)Configure Encrypting File System (EFS).
    (27)Install and configure BitLocker.
    (28)Install and configure TPM.
    (29)Manually encrypt all system files.

You can find your answer here: https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx.
BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline. On computers that do not have a TPM version 1.2, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation, and it does not provide the pre-startup system integrity verification offered by BitLocker with a TPM. The answer is to Install and configure BitLocker.

8. In which situation would you typically use a stand-alone certificate authority (CA) in your public key infrastructure (PKI) design? Lesson 2 p 47. Your choices are:
    (30)When deploying multiple root CAs in a single domain.
    (31)When creating a hierarchy with a third party root.
    (32)When issuing certificates to users outside of your domain.
    (33)When creating a trust infrastructure between root and subordinate CAs.

If you need to support outside clients and customers, you would most likely build a standalone CA. Unlike the Enterprise Root CA, a stand-alone CA does not use Active Directory. Because stand-alone CAs do not support auto enrollment, all requests for certificates are pending until an administrator approves them. The answer is that you would use a stand-alone certificate authority in your public key infrastructure design when issuing certificates to users outside of your domain.

9. Using Trusted Platform Module (TPM) ensures what? Lesson 2 p 54. Your choices are:
    (34)A dedicated firewall.
    (35)Data Availability
    (36)Protection from a brute force attack.
    (37)Hardware encryption of data.

BitLocker Drive Encryption is the feature in the Windows 7 Ultimate and Enterprise editions that makes use of a computer's Trusted Platform Module (TPM). A TPM is a microchip built into a computer that is used to store cryptographic information, such as encryption keys. Information stored on the TPM can be more secure from external software attacks and physical theft. For instance, BitLocker Drive Encryption can use a TPM to validate the integrity of a computer's boot manager and boot files at startup, as well as to guarantee that a computer's hard disk has not been tampered with while the operating system was offline. The answer is that TPM ensures hardware encryption of data.

10. A brute force attack is used to do what? Lesson 2 p 21. Your choices are:
    (38)Prevent access to network resources.
    (39)Discover details about network configuration.
    (40)Hijack communication sessions.
    (41)Discover passwords.

When seeking access to a file, computer, or network, hackers will first attempt to crack passwords by trying obvious possibilities, including the names and birthdays of a user's spouse or children, key words used by the user, or the user's hobbies. If these efforts don't work, most hackers will next attempt brute force attacks, which consist of trying as many possible combinations of characters as time and money permit. A subset of the brute force attack is the dictionary attack, which attempts all words in one or more dictionaries. Lists of common passwords are also typically tested. The answer is brute force attacks are used to discover passwords.

11. Which technology is used to provide file encryption for removable storage devices? Lesson 2 p 57. Your choices are:
    (42)BitLocker To Go
    (43)EFS
    (44)DFS
    (45)BitLocker

BitLocker To Go is a new feature in Windows 7 that enables users to encrypt removable USB devices, such as flash drives and external hard disks. Although BitLocker has always supported the encryption of removable drives, BitLocker To Go allows you to use the encrypted device on other computers without having to perform an involved recovery process. Because the system is not using the removable drive as a boot device, a TPM chip is not required. The answer is the technology that is used to provide file encryption for removable storage devices is BitLocker To Go.

12. You are a network administrator. You have enabled encryption for a file that is located in a shared folder. What does this ensure? Lesson 2 p 40-41. Your choices are:
    (46)That the file can only be added as an e-mail attachment.
    (47)That the file can only be read by users who are allowed to do so.
    (48)That the file cannot be written to a removable storage device.
    (49)That the file is marked with the Read-Only attribute.

GET READY. To share a folder, perform the following steps:
1. In Windows Server 2003, right-click the drive or folder you want to share and select Sharing and security. In Windows Server 2008, right-click the drive or folder, select Properties, select the Sharing tab, and then click the Advanced Sharing button. Select Share this folder.
3. Type the name of the shared folder.
4. If necessary, you can specify the maximum number of people that can access the shared folder at the same time.

5. Click the Permissions button.
6. By default, Everyone is given Allow Read share permission. Unless you actually want everyone to have access to the folder, you can remove Everyone, assign additional permissions, or add additional people. The answer is that the file can only be read by users who are allowed to do so.

13. You set the Passwords must meet complexity requirements policy to Enabled. Minimum password length is set to 8. Which of these is a valid password? Tell me yes or no for each one and WHY it is valid or not valid. Lesson 3 p 70.
    (50)dorWssaP
    (51)!@#$%^&*
    (52)$$Pwd##!99
    (53)p1a2s3s4

Password complexity involves the characters used to make up a password. A complex password uses characters from at least three of the following categories:
• English uppercase characters (A through Z)
• English lowercase characters (a through z)
• Numeric characters (0 through 9)
• Nonalphanumeric characters (!, @, #, $, %, ^, &, etc.)

The answer is that $$Pwd##!99 is the only one that meets the requirements and would not be easily guessed. droWssaP is just PassWord backwards – it only suffices 2 of the categories and it must suffice 3. !@#$%^& does not have any English characters at all or any numbers. p1a2s3s4 only suffices 2 of the categories and it must suffice 3.*

14. A strong password contains what? Lesson 3 p 70. Your choices are:
    (54)A minimum of 5 characters.
    (55)Letters, numbers and special characters.
    (56)A private key
    (57)A history of usage.

Same explanation as above. A complex password uses characters from at least 3 of the following categories:

• English uppercase characters (A through Z)
• English lowercase characters (a through z)
• Numeric characters (0 through 9)
• Nonalphanumeric characters (!, @, #, $, %, ^, &, etc.)

15. You support a Windows Server 2003 Active Directory forest with multiple domains. Each domain stores user accounts for users at a specific geographical location. You need to apply a consistent password policy to Active Directory users through group policy. You want to keep the effort needed to apply and maintain the policy to a minimum. What should you do? Your choices are:
    (58)Define password policy at the site level for each site.
    (59)Define password policy at the domain level in each domain.
    (60)Define password policy at the user's container in each domain.
    (61)Define password policy at the domain level in the forest's root domain.

You can find your answer here: https://technet.microsoft.com/en-us/library/cc748850(v=ws.10).aspx

The Account Policies settings in Group Policy are all applied at the domain level. Default values are present in the built-in Default Domain Controller Policy for Password Policy settings, Account Lockout Policy settings, and Kerberos Policy settings. The domain Account policy becomes the default local Account policy of any Windows®-based computer that is a member of the domain. The answer is to define password policy at the domain level in each domain.

16. What is password history used to enforce? Lesson 3 p 71. Your choices are:
    (62)Minimum time between password changes.
    (63)Guesses before locking an account.
    (64)Restrictions on password reuse.
    (65)Maximum time between passwords.

Password history is the setting that determines the number of unique passwords that must be used before a password can be re-used. This setting prevents users from recycling the same passwords through a system. The longer the period of time a password is used, the greater the chances it can be compromised. Microsoft allows you to set the password history value between 0 and 24. Ten is a fairly common setting in standard environments, although Windows Server 2008 defaults to 24 on domain controllers. The answer is that password history is used to enforce restrictions on password reuse.

17. You need to ensure that users attempting to log in are automatically blocked from logging in after a specific number of failed logon attempts. What should you create? Lesson 3 p 71. Your choices are:
    (66)A password policy.
    (67)A security group.
    (68)A software restriction policy.
    (69)An account lockout policy.

Account lockout refers to the number of incorrect logon attempts permitted before a system locks an account. Each bad logon attempt is tracked by the bad logon counter, and when the counter exceeds the account lockout threshold, no further logon attempts are permitted. This setting is critical because one of the most common password attacks (discussed later in the lesson) involves repeatedly attempting to log on with guessed passwords. The answer is to ensure that users attempting to log in are automatically blocked from logging in after a specific number of failed logon attempts, you should create an account lockout policy.

18. You need to create a password policy to ensure that domain account passwords must be reset every 2 weeks. What should you do? Lesson 3 p 72. Your choices are:
    (70)Enforce password history.
    (71)Define password complexity requirements.
    (72)Specify a minimum password age.
    (73)Specify a maximum password age.

Maximum Password Age: The maximum password age setting controls the maximum period of time that can elapse before you are forced to reset your password. This setting can range from one to 999 days, or it can be set to 0 if you never want passwords to expire. A general rule for this setting is 90 days for user accounts; although for administrative accounts, it's generally a good idea to reset passwords more frequently. In high security areas, 30 days is not an uncommon setting.