98-367 MU2a Authentication, Authorization & Accounting Questions and Answers with Explainations

Which are common symptoms of a virus infection? (Lesson 5 p 135-136)

Poor system performance. Unusually low levels of available memory. Poor performance while connected to the Internet. Decreased response rates. Longer start-up times. Instances in which your browser closes unexpectedly or stops responding. Changes in your browser’s default home or default search pages. Unexpected pop-up advertising windows. Addition of unexpected toolbars to your browser. Instances in which unexpected programs automatically start. Inability to start a program. Malfunctions in Windows components or other programs. Missing programs or files. Unusual messages or displays on your monitor. Unusual sounds or music played at random times. Creation and/or installation of unknown programs or files. The appearance of unknown browser add-ins. Corrupted files. Unexpected changes in file sizes.

Creating an antivirus quarantine area causes what? (CS)

The area will be isolated from other files on the system so that they cannot infect them.

How does a worm differ from other viruses? (Lesson 5 p 135)

A worm is a self-replicating program that copies itself to other computers on a network without any user intervention. Unlike a virus, a worm does not corrupt or modify files on the target computer. Instead, it consumes bandwidth and processor and memory resources, slowing the system down or causing it to be unusable. Worms usually spread via security holes in operating systems or TCP/IP software implementations.

What is a Trojan Horse? (Lesson 5 p 135)

Trojan horses derive their name from the Trojan horse story in Greek mythology. In short, a Trojan horse is an executable program that appears as a desirable or useful program. Because it appears to be desirable or useful, users are tricked into loading and executing the program on their systems. After the program is loaded, it might cause a user’s computer to become unusable, or it might bypass the user’s system security, allowing his or her private information (including passwords, credit card numbers, and Social Security number) to be accessible by an outside party. In some cases, a Trojan horse may even execute adware.

You work as a security consultant. One of your clients informs you that as of today he is unable to access any of his personal files on his Windows 10 computer. The user's computer displays a message box that prompts him to submit a Bitcoin payment to a 3rd party in exchange for a decryption key that will unlock his files. What type of malware has infected the user's computer? (not in the book!!)

Ransomware.

What is malware? (Lesson 5 p 134)

Malicious software, sometimes called malware, is software that is designed to infiltrate or affect a computer system without the owner's informed consent. The term "malware" is usually associated with viruses, worms, Trojan horses, spyware, rootkits, and dishonest adware. As a network administrator or computer technician, you need to know how to identify malware, how to remove it, and how to protect a computer from it.

All users have been denied all permissions to a file. You need to access the file as quickly as possible. You are logged on as an administrator. What should you do first? (Lesson 2 p 39)

The owner of an object controls what permissions are set on the object and to whom permissions are granted. If for some reason, you have been denied access to a file or folder and you need to reset the permissions, you can take ownership of the file or folder and then modify the permissions. All administrators automatically have the Take Ownership permission for all NTFS objects.

When securing your network, you would disable inheritance to (Lesson 2 p 36)

When permissions are assigned to a folder, by default, they apply to both the folder and any subfolders and files of that folder. To stop permissions from being inherited in this way, you can select the "Replace all existing inheritable permissions on all descendants with inheritable permissions from this object" in the Advanced Security Settings dialog box. The dialog box will then ask whether you are sure you want to do this. You can also clear the "Allow inheritable permissions from parent to propagate to this object" check box. When the check box is clear, Windows will respond with a Security dialog box. When you click on the Copy button, the explicit permission will be copied from the parent folder to the subfolder or file. You can then change the subfolder's or files explicit permissions. If you click the Remove button, it will remove the inherited permission altogether. Therefore, the answer would be When securing your network, you would disable inheritance to prevent folder permissions on a folder from being used for sub folders.

You work as a security compliance officer for your company. As a part of their security training, all employees must be able to identify and define basic malware types. How should you define the malware types? Select the correct answers below.

(yes) Zero-day attack: An exploit for an unknown vulnerability

(yes) Back door: An undocumented administrative portal

(no) Buffer overflow: An undocumented administrative portal

(yes) Virus: Malware that requires a host file to propagate

(no) Trojan horse: Malware that requires a host file to propagate

Which type of malware replicates itself without reliance on a host file?

Worm.

You work as a domain administrator for your company. All user computers in the organization run Windows 10 Enterprise Edition. One of the company's employees modified NTFS permissions on her network-based project folder in such a way that no administrator has access. You need to ensure that you and other domain administrators can access the employee's project folder. What should you do first? (Lesson 2 p 35)

Take ownership of the folder. Full Control will allow Permission to read, write, modify, and execute the files in a folder; change attributes and permissions; and take ownership of the folder or files within

What is the minimum shared folder permission that is required for a user to delete a file? (Lesson 2 p 41)

Change: Users with this permission have Read permissions and the additional capabilities to create files and subfolders, modify files, change attributes on files and subfolders, and delete files and subfolders.

What is a security group used for? (Lesson 2 p 31)

A security group is used to assign rights and permissions and to gain access to network resources.

You administer your company's Windows Server 2012 R2 file server. It has 2 NTFS data volumes, D: and E:. You move a file from drive D: to drive E:. What happens to the files original permissions? (Lesson 2 p 39)

When copying and moving files, you will encounter one of three scenarios:

- If you copy a file or folder, the new file or folder will automatically acquire the same permissions as the drive or folder it is being copied to.

- If a file or folder is moved within the same volume, that file or folder will retain the same permissions that were already assigned to it.

- If a file or folder is moved from one volume to another volume, that file or folder will automatically acquire the permissions of the drive or folder it is being copied to.

Since you are moving files from one drive to another, the last option will happen -- permissions will be inherited from the destination folder.

What is a smart card? (Lesson 2 p 22)

A smart card is a pocket-sized card with embedded integrated circuits consisting of nonvolatile memory storage components and perhaps dedicated security logic. Nonvolatile memory is memory that does not forget its content when power is discontinued. This kind of memory may contain digital certificates to prove the identity of the person who is carrying the card, and it may also contain permissions and access information. Because smart cards can be stolen, some do not have any markings on them; this makes it difficult for a thief to identify what the card can be used to access. In addition, many organizations require users to supply passwords or PINs in combination with their smart cards.

What are the features of a public key in asymmetric encryption? (Lesson 2 p 46)

Asymmetric encryption, also known as public key cryptography, uses two mathematically related keys for encryption. One key is used to encrypt the data, while the second is used to decrypt it. Unlike symmetric key algorithms, this method does not require a secure initial exchange of one or more secret keys to both sender and receiver. Instead, you can make the public key known to anyone and use the other key to encrypt or decrypt the data. The public key could be sent to someone or could be published within a digital certificate via a Certificate Authority (CA). Secure Sockets Layer (SSL)/Transport Layer Security (TLS) and Pretty Good Privacy (PGP) all use asymmetric keys. Two popular asymmetric encryption protocols are Diffie-Hellman and RSA. For example, say you want a partner to send you data. To begin the asymmetric encryption process, you send your partner the public key. Your partner will then encrypt the data with the key and send you the encrypted message. You will next use the private key to decrypt the message. If the public key falls into someone else’s hands, that person still could not decrypt the message because you need the private key to decrypt a message that has been encrypted with the public key. (Answers for this specific question are likely to be it is distributed by certificate and it is used to encrypt data.)

You normally log on as a standard user. You need to occasionally run programs that require administrator privileges. You want to keep the potential security risk to a minimum. What should you do? (Lesson 2 p 24)

Because administrators have full access to individual computers or entire networks, it is recommended that you use a standard non-administrator user account to perform most tasks. Then, when you need to perform administrative tasks, you can use the Run As command or the built-in options that are included with the Windows operating system.

What is biometric security? (Lesson 2 p 22)

Biometrics is an authentication method that identifies and recognizes people based on physical traits, such as fingerprints, face recognition, iris recognition, retinal scans, and voice recognition. Many mobile computers include a finger scanner, and it is relatively easy to install biometric devices on doors and cabinets to ensure that only authorized people enter secure areas.

You work as a security analyst for your company. As part of the company's latest security initiative, all users are required to authenticate to network resources with a second authentication method. All user computers run Windows 8.1 Enterprise Edition. The company's CIO states that she wants to implement virtual smart cards for all corporate employees. You need to analyze the existing environment to identify solution prerequisites. Which of the following is a requirement for implementing virtual smart cards? I do not like this question... (Lesson 2 p 54)

Virtual smart card technology from Microsoft offers comparable security benefits to physical smart cards by using two-factor authentication. Virtual smart cards emulate the functionality of physical smart cards, but they use the Trusted Platform Module (TPM) chip that is available on computers in many organizations, rather than requiring the use of a separate physical smart card and reader. Virtual smart cards are created in the TPM, where the keys that are used for authentication are stored in cryptographically secured hardware.

Which protocol can centralize authentication for dial-up, Virtual Private Network (VPN), and IEEE 802.11 Wi-Fi access connections? (Lesson 4 p 99)

RADIUS stands for Remote Authentication Dial-In User Services. NPS is the RADIUS server and proxy service in Windows Server 2008. When NPS functions as a RADIUS server, it provides authentication, authorization, and accounting (AAA) services for network access. When used for authentication and authorization, NPS interacts with the Active Directory to verify user or computer credentials, as well as to obtain user or computer account properties when a computer attempts an 802.1x-authenticated connection or a VPN connection. Therefore, the RADIUS protocol can centralize authentication for dial-up, VPN and IEEE 802.11 Wi-Fi access connections.

To implement multifactor authentication you should use what? (Lesson 2 p 21)

When two or more authentication methods are used to authenticate someone, a multifactor authentication system is said to be in place. Of course, a system that uses two authentication methods (such as smart cards and passwords) can be referred to as a two-factor authentication system.

What does mutual authentication mean? (Lesson 2 p 25)

Mutual authentication is when users are authenticated with the server and vice versa. They both verify each other.

Which would you audit to detect attempts to guess user passwords? (Lesson 3 p 71)

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. So you would look for logon/logoff failures.

You want to implement a consistent audit policy for your Active Directory domain. Which should you use? Lesson 3 p 77-78)

Before we look at using Group Policies to enforce password settings, we should describe exactly what a Group Policy (also known as a Group Policy Object) is. A Group Policy Object (GPO) is a set of rules that allow an administrator granular control over the configuration of objects in Active Directory (AD), including user accounts, operating systems, applications, and other AD objects. GPOs are used for centralized management and configuration of the Active Directory environment. Therefore the Group Policy Editor should be used to implement a consistent audit policy for your Active Directory.

A website requires a user to enter both a password and a text message-based personal identification number (PIN). Which type of authentication does that website use? (Lesson 2 p 21)

When two or more authentication methods are used to authenticate someone, a multifactor authentication system is said to be in place. Of course, a system that uses two authentication methods (such as smart cards and passwords) can be referred to as a two-factor authentication system.