You are administering a print server running Windows Server 2012. You want to perform maintenance on a print device physically connected to the print server. There are several documents in the print queue. You want to prevent the documents from being printed to the printer, but you don’t want users to have to resubmit the documents to the printer. What is the best way to do this?

A. Open the printer’s Properties dialog box, select the Sharing tab, and then select the Do Not Share This Printer option.

B. Open the printer’s Properties dialog box and select a port that is not associated with a print device.

C. Open the printer’s queue window, select the first document, and then select Pause from the Document window.

D. Open the printer’s queue window, and select the Pause Printing option from the Printer menu.

Step 1: Answer

Option D Open the printer's queue window, and select the Pause Printing option from the Printer menu.

Step 2: Explanation

Option A. Wrong: An unshared printer will carry on processing tasks that are currently in the queue.

Option B. Incorrect: Users will need to resubmit the jobs that were in the queue if the port is changed.

Option C. incorrect: The remaining tasks in the queue will not stop printing if the first document in the queue is paused.

Option D. Correct answer; after choosing to pause printing, the files will stay in the print queue until you begin printing. All of the documents in the queue are covered by this choice.

  Henry notices that a malware sample he is analyzing downloads a file from imgur.com and then executes an attack using Mimikatz, a powerful Windows password account theft tool. When he analyzes the image, he cannot identify any recognizable code. What technique has most likely been used in this scenario?

A.    The image is used as decryption key.

B.    The code is hidden in the image using steganography.

C.    The code is encoded as text in the image.

D.    The image is a control command from a malware command and control network.

Step 1: Answer

**B.**The code is hidden in the image using steganography.

Step 2: Explanation

Because of its simplicity and adaptability, users of social media and social news websites like Reddit, Twitter, and Digg prefer the picture hosting and sharing service Imgur.

When malicious PowerShell code with triple-encoded malicious tools was uncovered in 2020, this real-world illustration was found. The first package was hidden using steganographic methods and downloaded as a picture from imgur.com or other websites. The code was likewise Base64 encoded both before and after RSA encryption, and it was encrypted. Henry should be aware that a downloaded image can include hidden information even though steganography is not very popular.

         Isaac has been asked to write his organization’s security policies. What policy is commonly put in place for service accounts?

**A.**They must be issued only to system administrators.

**B.**They must use multifactor authentication.

**C.**They cannot use interactive logins.

**D.**All of the above

Step 1: Answer

**C.**They cannot use interactive logins.

Step 2: Explanation

A user account specifically developed to provide a security context for services running on Windows Server operating systems is known as a service account. The service's capacity to access local and network resources depends on the security context. Services are required to run a number of functions in the Windows operating systems.

The greatest insider threat of all can emerge from compromised service accounts. Service accounts performing interactive logins, which are typically performed by human users, should be a clear warning sign for any security team, and these instances should be used as infrequently as feasible.

Depending on the needs of the application they are being used for, service accounts have domain administration rights.

   Gabby wants to protect a legacy platform with known vulnerabilities. Which of the following is not a common option for this?

**A.**Disconnect it from the network.

**B.**Place the device behind a dedicated firewall and restrict inbound and outbound traffic.

**C.**Rely on the outdated OS to confuse attackers.

**D.**Move the device to a protected VLAN.

Step 1: Answer

**C.**Rely on the outdated OS to confuse attackers.

Step 2: Explanation

An operating system (OS) that is no longer in common use or that has been replaced by a more recent iteration of an older technology is referred to as a legacy platform, sometimes known as a legacy operating system. Many businesses that employ computers have legacy platforms and applications that are essential to their operations.

Not only can outdated software make your security susceptible to malicious human activity. Additionally, it makes it susceptible to system failure. A software programme that the seller no longer supports is considered to be outdated. This implies that any newly discovered programme bugs won't be fixed.

Businesses using obsolete legacy systems are more susceptible to cyberattacks. In fact, studies show that each hour, over 10,000 new malware threats are found.  If your technology is not always up to date, your risk is constantly increasing at exponential rates

Nora has rented a building with access to bandwidth and power in case her organization ever experiences a disaster. What type of site has she established?

**A.**A hot site

**B.**A cold site

**C.**A warm site

**D.**A MOU site

Step 1: Answer

Cold site

Step 2: Explanation

A cold site has been established by Nora. A cold site is a place that can be connected to the internet but lacks systems; these places often have access to power and bandwidth, but because they are merely rented spaces, they must be completely prepared to function in the event of an emergency. Warm locations have some or all of the systems and infrastructure that Dory requires, but they lack the data. A hot site is an environment that is completely functioning and has all of the technology, software, and information required to run an organisation. Although they are expensive to operate and maintain, businesses who cannot afford downtime utilise them. A disaster recovery site is different from a memorandum of understanding (MOU).