Your supervisor has requested you perform some actions to hardening a newly-installed Windows 2012 server that will host a new corporate website. Which of the following actions should you not perform as part of your hardening?

Install the latest patches and updates

Verify any unnecessary ports have been closed

Execute a PHP script you downloaded from the Internet to verify the web server’s functionality

Delete any PHP default configuration files

Answer: C

Explanation: You should not download and execute any scripts from the Internet without knowing their functionality and whether they can cause an additional vulnerability to your system. When hardening a new system, you should ensure the latest patches and updates have been installed. You should also ensure that any unnecessary applications, services, ports, and protocols have been uninstalled, closed, or disabled. Also, any default configuration files should be deleted after installation. (Lesson 06\_02 Unnecessary applications)

Bob from accounting has heard that you are studying for your Security+ exam. He asks you to come by his desk to take a look at his laptop. He proudly pulls out a laptop running Windows 7 and begins to show you how he has installed a good anti-malware solution, enabled his host-based software firewall, uninstalled any programs he doesn’t regularly use, and tells you how he updates it routinely to ensure he is well protected. When he double-clicks on his Computer icon, you see his hard drive uses FAT32 as its filesystem. What do you recommend Bob do to increase his security?

Recommend he reformat his hard drive as NTFS because it is more secure

Recommend he reformat his hard drive as ext4 because it is more secure

Recommend he reformat his hard drive as APFS because it is more secure

Recommend he convert his hard drive to NTFS because it is more secure

Answer: D

Explanation: Bob is running Windows 7, so he can use either FAT32 or NTFS for his filesystem. NTFS is more secure than FAT32 and should be used. Windows allows users to convert their FAT32 filesystems to NTFS by using the convert command from the command prompt. This will convert the filesystem without any loss of his files. If Bob reformats his hard drive as NTFS, all his files would be lost. Bob cannot use ext4 because he isn’t running Linux and cannot use APFS because he isn’t running OS X. (Lesson 06\_10 File Systems and Hard Drives)

You are a newly-hired security administrator at Small Time Corporation and have been attempting to ensure all your computers are up to date with their patches. The company has a Windows domain environment and has disabled Windows Update on all of its workstations. You just heard that Microsoft released a security update this morning to prevent its Windows 8.1 and Windows Server 2016 operating systems from falling victim to a new ransomware attack that has been spreading quickly across the country. Your company does not have a test network setup yet to test the new security update/patch. What should you do?

Turn on Windows Update so the workstations can automatically receive the security update

Download the security update from Microsoft’s website and manually install it on all of the workstations

Download the security update from Microsoft’s website, manually install it on a single workstation to see if it works properly, and then install it on the rest of the workstations

Download the security update from Microsoft’s website, ask your boss to allow you to build a test network, install and test the security update on the test network, and then install it on all your workstations and servers

Answer: C

Explanation: You should never install a security update or patch into your production network without first testing it. Since your company doesn’t have a test network, you should pick a single workstation that is the least critical to your business operations. If the installation performs correctly without issues, you can then install it on the other workstations. It is a good idea to have the company build a small test network, but if this security update is necessary to prevent a quickly-spreading piece of ransomware, you likely don’t have the time to wait for that test network to be built and ready. (Lesson: 06\_07 Patch Management)