CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 5

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Module 3 & 4

1. Discuss the differences between physical switches and virtual switches.

A Physical switch is responsible for connecting multiple devices to a network to communicate with each other or a router. After which you would you be able to connect to the internet, send files, etc. However, Virtual switches essentially do the same thing virtually but without the use of a physical device. This is done through software and is typically used with virtual machines.

2. Compare a production checkpoint to a standard checkpoint. What are the benefits of one over the other, and what are the situations where each would be used?

A Production Checkpoint uses backup technology and Shadow Copy to make sure that data remains accurate and consistent. However, it does not capture the memory state in a Hyper-V session. Standard Checkpoints can capture the memory state and are the traditional form of checkpoints.

3. Why should an administrator spread Flexible Single Master Operations (FSMO) roles within a forest and domains amongst different domain controllers?

It is important because active directory information can have several redundancies in case of unexpected consequences. Having two domain controllers at each physical site is important because of this and it is good practice to utilize backups often. The Larger the environment the more important this becomes.

4. What are the advantages and disadvantages of using a read-only domain controller (RODC).

RODC is more secure than other domain controllers however it is less functional. In other words, the RODC doesn't have domain admins password hash synced on the server so if stolen it is less of a security issue. Having said that, without that information it makes the controller useless outside of this fact.

Listen to "Episode #69: Human Hacker of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/69/Links to an external site.

Based on the podcast, answer the following questions.

5. Describe what happened during the first Bank break in Jamaica and what did they hack?

The plan was to use USB drives to hack devices by simply plugging them in at the bank. During this time, they were to photograph and record other information covertly using a phone. They were able to hack the network, ran two different machines, and were able to exit.

6. Explain three of the five key strategies that the client could have implemented to prevent the first Bank in Jamaica from being hacked.

They could have improved their physical security by patting them down and checking for odd devices attached to them. They should make sure that the employees are aware that unknown personnel should not ever ask them to log in to a device without clearance. Overall, the cybersecurity/security fundamentals should be taught and added to employee training to prevent things such as leaving keys unattended and opening doors for others.

7. Give an overview of what transpired when the human hackers pretending to be a pest control worker.

The human hackers were able to easily go through the front gate without question. Lied about being pest control and were taught how to use the ATMS, were let into several doorways, and were given access to several computers. This was all recorded and photographed by the hackers and they were intended to be used later for network hacking and badge cloning. The only step left was for them to pack up and escape by faking their names on a business card and having a fake call with their fake boss in order to get the all-clear from security.

Due September 28, 2023