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.

   Physical switches and virtual switches both help computers communicate, but they work in different ways. Physical switches are actual pieces of hardware you can touch, while virtual switches are software-based and live inside computer systems. Physical switches are like standalone tools or parts of larger setups, while virtual switches are part of software setups, often for things like running multiple virtual computers on one physical machine. Physical switches are powerful but can be inflexible, while virtual switches are more adaptable. Managing physical switches involves adjusting settings directly, while virtual switches are controlled through software interfaces. Physical switches might offer special features, but virtual switches work with software tools like firewalls and balancing. While physical switches need upfront money and upkeep, virtual ones might save hardware costs but need good underlying systems and software maintenance.

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 acts like a snapshot of a virtual machine taken when everything inside it is paused to ensure that all the data is in a stable state. It's useful for important tasks like managing databases where data integrity is critical, and any loss could be costly. In contrast, a standard checkpoint simply freezes the VM without ensuring that everything inside it is stable. It's quicker and easier to use, making it ideal for testing or experimenting with software where data safety isn't as much of a concern.

The benefits of one over the other depend on the situation. Production checkpoints keep your data safe and consistent, making them ideal for important tasks in live environments, while standard checkpoints are faster and easier, making them perfect for experimenting or testing software where data safety isn't as critical. Overall, choosing between them depends on the specific needs of the task at hand and production checkpoints ensure data integrity in critical environments, while standard checkpoints offer speed and convenience for testing and experimentation.

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

   Spreading Flexible Single Master Operations roles across different domain controllers within a forest and domains is important for a few reasons. Firstly, it ensures that if one domain controller fails, the whole system doesn't go down because another one can step in. This also helps to balance the workload among different controllers, so none of them gets overwhelmed. Plus, having these roles on multiple controllers means there's a backup if one fails, which is crucial for keeping things running smoothly. If there's a disaster, like a server crashing, having these roles spread out makes it easier to recover without causing too much downtime. It also makes managing the system simpler and reduces the risk of security issues.

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

   Using a read-only domain controller has its pros and cons. On the plus side, it enhances security by keeping sensitive data safer, which is handy in places with weaker physical security like remote offices. It also speeds up logins for users in those locations by storing login information locally. Plus, it's easier to manage than regular domain controllers since it doesn't need as much attention. But, it can't do everything a regular one can, it's limited in what it can change and update. Setting it up can be a bit tricky and may cause some initial delays as it gets everything synced up. And even though it needs less day-to-day management, it still needs regular check-ups to make sure it's running smoothly.

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?

   They performed an OSINT on the Bank and found they were going through an audit. Then they decided they were going to show up to the Bank acting as PCI auditors. They then entered the Bank to find some sort of access point to attack. They then entered this back office where they accessed the Network by manipulating a woman by entering her password, then they saw a man exit his desk with his computer still on and they hacked that one as well. After all of that and a lot of fear they were confronted and decided they did enough there and left.

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 need for better physical security is high. What I mean is to look out for shoulder surfing, no holding doors open for anyone, and making sure to lock your computer whenever you leave your desk and make sure it's not messy and no important documents are on it.
   - They need to implement stronger social engineering training. What I mean is that these guys were able to just walk in and the employees did the right thing by asking who they were but that's it. They need to have better authorization. They should've checked those guys paperwork, credentials, etc. to confirm that they say who they say they are. And the lady who just typed her information into the computer next to her to open it up for the guys to work on was crazy. She should never do that and needs to get taught the consequences of what could happen if she does that again, but after the attack I'm sure she learned her lesson.
   - They need to have better awareness. I mean there was two American guys in the middle of an office trying to get into a computer. They were barely pressured into leaving. They stated it was uncomfortable, but uncomfortable doesn't mean forced to leave. They need to learn that if you see someone in a private room that you don't know you need to ask questions and be prepared for anything.

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

   They came by the bank at night, and they slipped one of their malicious USB sticks through the gap in the locked door in hopes someone will find it and plug it into a computer. However, they slipped it in a door that is never used, and the security team saw it the next morning and was confused why someone was there because nobody ever uses that door. They checked the security cameras and saw them so when the next morning when the guys came back the security team was prepared. One of them gets slammed on the hood and gets arrested, guns drawn, and the driver was getting ready to flee. However, a lady pulled out a gun and pointed it at the driver but slammed him on the hood as well and arrested him. Everyone is yelling at each other, confused, and the guys are still trying to play it off as "pest controllers." The guys were sitting on the side of the road getting interviewed and questioned on why they were there at 11 o'clock at night. They still thought they could play it off until a security guard mentioned the USB card. That's when the guys pulled out the letter from the head security guy who allowed the guys to test the banks security. Once they read the letter everything calmed down and no charges were pressed on the guys.

Due February 8, 2024