

CYSE 280 – Windows Systems Management and Security

Professor Malik A. Gladden

Homework 5

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

The biggest difference between the two is that one is something you can plug cables into and the other you cannot. A physical switch guides information through cables that act like an access point that can extend the reach of a device connected to it. Then a virtual switch is software within a device. One key component is that virtual switches do not share resources between the connected devices. So, it's an isolated environment commonly used for 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 can be described as images within a virtual machine that can be brought back. A standard checkpoint captures the state that the data was last left to. Standard checkpoints are great for recapturing the state of a broken device to better find solutions.

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

It is important to FSMO roles within a forest and domains with different domain controllers because if we only had one it would create problems and issues. Such as latency and failure to complete operations.

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

One of the advantages of using RODC is that there is not sufficient security in a data center. Another is when there is not enough bandwidth for network connections. Then the biggest disadvantage of RODC is updated it can be a hassle. It does not support direct updates and instead of to go through a DNS in a domain controller.

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

First, they had to put USB keys into random computers in the bank to gain access to the network. They were able to hack into an ATM repair room and gain information about software usage. Then they successfully enter the network by logging into a locked computer in the call center.

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

The first key strategy the client could have implemented is the security guard at the entrance. He should have questioned and stopped them for verification but did not. The second is in the ATM center where the woman did stop them but was convinced quickly that they were supposed to be

there. Lastly, when they asked the person next to an empty computer to log in, they should have gotten permission from the manager before being convinced again.

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

They were caught on surveillance the night before and were arrested. While being arrested they resorted to using the get out of jail free card, Which was a letter to describe that it was a test to check security.