Lucas Esquivel

CYSE 280

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

While physical networking connects computers through cabling and other hardware, virtual networking extends these capabilities by using software management to connect computers and servers over the Internet. This provides greater flexibility to virtual switches in comparison to physical switches. This also means that virtual switches can be changed, fixed, or modified on demand whereas for physical switches it requires an addition of switches or fixing the current switch that is presented.

**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?**

Production checkpoints are "point in time" images of a virtual machine, which can be restored later in a way that is completely supported for all production workloads. This is achieved by using backup technology inside the guest to create the checkpoint, instead of using saved state technology. Standard checkpoints capture the state, data, and hardware configuration of a running virtual machine and are intended for use in development and test scenarios. Standard checkpoints can be useful if you need to recreate a specific state or condition of a running virtual machine so that you can troubleshoot a problem.

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

Admins should spread FSMO roles within a forest and domains amongst different domain controllers because if one domain controller goes missing another will be able to take its place. It makes Active Directory a much more secure, stable, and utilizable tool.

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

Some of the advantages of using read-only domain controller is that it produces better access to the authentication resource on the network as well as it provides better logon times than compared to accessing across a WAN link. Some disadvantages are that an RODC usually needs a writeable domain controller to work properly. For example, users can't change passwords, computers can't join the domain, accounts whose passwords haven't been cached can't logon, and Group Policy doesn't work properly if no writable RODC is available. This means that an RODC doesn't provide the same failure safety as a writeable DC.

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

During the first bank break they pretended to be PCI auditors and tried to get inside the building. One of their jobs was to put a USB key into random computers and hack the network.

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

One of the first and main key points is that the security guy should have stopped them at the entrance when they were on their phone, but he didn’t. Another key strategy is when they were at an ATM center and a lady asked what they were doing in the room. They said they were doing PCI auditing, but the lady should have said that she didn’t have them authorized in that room. A third key strategy is when they asked that same woman to enter a password and instead of consulting with her manager or saying “I don’t think I’m allowed to do that” she did it anyways.

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

At first there was a confrontation between them and a lady that was working as security there and ended with the guy being put in handcuffs. After a while he is able to social engineer or “smooth talk” his way free and that’s when later on they end up stealing things like badges and some other stuff.