Jasmyn Wilhelm

Student ID: 01155323

1. Discuss the difference between physical switches and virtual switches.
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?
3. Why should an administrator spread Flexible Single Master Operations (FSMO) roles within a forest and domains amongst different domain Controllers?
4. What are the advantages and disadvantages of using a read-only domain Controller (RODC).

---

1) Virtual switches can create isolated networks for specific types of communication and provide enhanced communication. Some operating systems and VM's will only respond to requests from computers on a physical network. Physical switches can be divided into seperate VLANS that act as individual physical switches. While most hypervisors allow the creation of virtual networks, physical switches must connect to the computer network interfaces through Ethernet.
2. A production Checkpoint is provided by a backup service in a guest operating system, but a standard Checkpoint is provided by Hyper-V and captures the state of running programs. Checkpoints are useful when needing to revert to a previous version of a VM. Production Checkpoints can cause fewer problems as it uses less resources. However, standard Checkpoints can save the VMs running state in the snapshots directory.

3. Flexable Single master Operations (FSMO) is where certain domain and forest functions are required to be coordinated from an individual domain Controller. The PDC Emulator in modern domains is what talks to the domain to allow password changes and sent present time data to each computer. The RID (Relative Identifiers) master issues ranges in sequential order to the domain Controllers throughout the domain. Due to the RID Master assigning unique domains, it is guaranteed for the ranges to be unique in the domain objects and when the Controller is out of the assigned ranges the RID Master will assign more. Lastly, the Infrastructure Master works with GUIDS, DNs, and the user group memberships. To avoid complications, the Infrastructure Master should assigned to a domain Controller without a group Catalog.
4. Read-only domain Controllers, or RODC's, store a read-only version of a database in Active Directory. RODC's can provide increased security throughout a network and denies any attemps made to change sensitive data in the stored copies. The functionin is limited for RODC's which can be seen as a disadvantage. The limitations prevent the creation of accounts and resetting password which are popular features used throughout Active Directory.

DarkNet Diaries Episode 69: Human Hacker

5. Describe the pretext Chris and his team used during their penetration test in Jamaica and how they got access to the bank's ATM testing center.
6. Explain three of five key strategies that the client could have implemented to prevent the first bank in Jamacia from being hacked.
7. Give an overview of what transpired when the human hackers pretended to be pest control workers.

/ /

5. During Chris's teams penetration ~~test~~, they pretended to be auditors completing a yearly PCI review. They were briefly stopped at the guard gate, but ultimetly let through after claiming "we're here to do some banking". Next, Chris and Ryan dressed in shirts with the company logo, grabbed their fake business cards, and hollow clipboard that carries supplies not meant to be seen just walking around. By pretending to take a phone call, Chris and Ryan made it to the ATM testing center, collected pictures, and hacked into two computers.
6. When the duo first entered the building they were not stopped which was the first flaw made by the bank. Secondly, when Ryan and Chris snuck behind a woman entering the ATM center, they were not questioned or asked for a deeper understanding of why they had to be in that secure area.

When an employee willingly enters their password without question or hesitation, that shows mistake number 3. Flaw four of the bank ocurred when an employee left their desk with their computer unlocked and sensitive information left out. Lastly, when the security guard called the teams "contact", it was allowed to take place over Chris's phone and no detailed questions asked.

7. While the team reconed, they were unaware a particular door was never used. Once placing a usb through a crack, suspicions arosed by the employees which made them check the security cameras. Ryan and Chris were then on camera and when they tried to continue their plan, from the night before, they were caught, handcuffed, and held at gun point. However, they did get information that the facility has no security passed 7:00 pm, when getting unhandcuffed, and they were able to return the next day after seven and complete their assignmen