Branden Barnes

Professor Gladden CYSE 280

10/5/2023

Windows System Management and Security: Module 3 & 4

1. A physical switch connects a device to the network using an ethernet cable. A virtual switch connects virtual networks through virtual operating systems such as Hyper-V. Virtual networks can communicate through virtual switches using IP. There are three types of virtual switches: external, internal, and private virtual switch.
2. The main difference between a standard checkpoint and a production checkpoint is the state of running programs being saved. Standard checkpoints use Hyper-V to provide functionality in saving running programs using snapshots directory. Production checkpoints do not save running programs, for this reason they cause fewer problems when applied. The production checkpoint is less resource-intensive because they use backup service instead.
3. You should spread FSMO roles within a forest because if one were to go down then having a spread amongst different domain controllers will forgive fault tolerance. In the process of role seizure, if a domain controller were to go down you can force another domain controller in its place. When that domain becomes available again, the assumed role will destruct and the FSMO role can be applied again.
4. Some advantages of using (RODC) include security benefits. Passwords are controlled to a point where if there is a breach, the intruder can only access for certain branch office users. You can also force active directory to reset the passwords for all user accounts.

Disadvantages include, not everyone can edit when set to read only. Also, privileges and password changes can become complicated.

Episode #69: **Human Hacker of the DarkNet Diaries podcast**

5. The objective of the bank heist in Jamaica was to penetration test the bank in broad day light. The plan was to put malware into usb's and plug them into the network. They had done OSINT and found an American audit. They then tried to become a PCI auditor. They hacked the ATM and the Network.
6. First, the client should have implemented stricter in person security. Second, better employee security on rooms and computers. Last, making sure that contacts are valid and not fake.
7. The beginning of the pest control hack was to leave a usb stick through the gap of a door in hopes of someone finding it and plugging it in. They get caught the next time they go to pull in and they both get put into handcuffs. They eventually gave up in trying to lie, and gave the letter of affirmation to the security guards showing that they were hired by their boss to try to break in. After all the confirmation they ended up getting information enough to break in, where they left their pest control equipment as a little tease to the security guards.