Jasmyn Wilhelm 16 November 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 10

1. **What are the main problems related to fragmented files?**

Fragmented files slow down performance and increase hardware wear and tear since a computer must look for each piece. They are more susceptible to corruption or destruction, particularly during crashes or power shortages. Because these files are spread out, recovering them is challenging, and defragmenting the system can be time-consuming and temporarily slow.

2. **Why is backing up an organization's servers important?**

Backups are essential for protecting data in the event of natural disasters, technical malfunctions, or cyberattacks.

- They protect against ransomware and guarantee that no data is lost forever.
- Backups must be maintained by many organizations for compliance or auditing purposes.
- Backups minimize downtime and provide a way of recovering deleted or outdated data.

Without backups, businesses risk major disruptions or the irreversible loss of important data.

3. **Discuss in detail the creation of a DNS implementation plan.**

One essential tool for internet users to find websites is a DNS plan. It involves figuring out how many servers and security features are required, identifying which servers are in charge of primary operations and backups, and putting in place a system that reacts quickly. To guarantee the system's operation and stop hacking, continuous testing, security precautions, and updates are crucial.

4. **What are the advantages and disadvantages of using DHCP?**

By automatically allocating a device's address to every network client, DHCP makes establishing connections simple and eliminates human error. However, some devices require permanent addresses, and if the server fails, it might malfunction, increasing the risk of strangers entering. Backup servers and specific procedures for essential equipment can be established to fix these issues.

Listen to “Episode #73: WannaCry of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/73/

Based on the podcast, answer the following questions.

5. **How did the WannaCry ransomware attack impact the UK's National Health Service(NHS), and what measures did hospital staff take to continue operating?**

The NHS in the UK lost access to its computer systems due to the WannaCry ransomware. With its affected computer systems, the NHS was unable to provide proper treatment for patients, so they were forced to turn away patients at hospitals. The WannaCry ransomware attack on the UK's National Health Service (NHS) forced hospitals to use written patient information and healthcare workers to use offline medical equipment.

6. **Explain the significance of the EternalBlue exploit in the spread of the WannaCry ransomware. Why was this exploit particularly dangerous?**

The EternalBlue vulnerability was important to the WannaCry ransomware attack because it took advantage of an SMB weakness allowing threat actors to remotely take over machines running Windows. Because WannaCry is a type of malware known as a worm along with being ransomware, it was able to spread across multiple systems during the beginning of its deployment. The WannaCry exploit was harmful because it encrypted all computer data and made computers useless.

7. **What role did security researcher Marcus Hutchins play in stopping the WannaCry ransomware, and what unexpected method did he use to achieve this?**

A "kill switch" in the WannaCry ransomware was discovered by British security researcher Marcus Hutchins in 2017, stopping attacks across the world. He set up an unregistered domain to examine the malware's activities and prevent it from running on compromised computers. Hutchins' quick response, which showed WannaCry's eagerly written and faulty code, stopped further damage to businesses worldwide.

Resources

WannaCry – Darknet Diaries. (n.d.). https://darknetdiaries.com/episode/73/