Jasmyn Wilhelm 10 October 2024

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Homework 7

Short Answer Questions (short answers should generally be at least three to four sentences in length. However, it is important to be as concise as possible when responding.) or you may choose to **Upload a Two-Minute Audio or Video recording** to answer the following questions.

Module 5 & 6

1. **What are the benefits of folder and file auditing?**

The method of monitoring and examining modifications, accesses, and actions pertaining to files and directories in a system is called file auditing. Early threat detection, prevention, standard compliance, improved incident response, investigation, and improved data management are just a few advantages it provides. Professionals in cybersecurity can also use it to examine the cybersecurity infrastructure of their company.

2. **What are the advantages and disadvantages of using Microsoft Encrypting File System to protect files and folders?**

A built-in feature called Microsoft Encrypting File System (EFS) encrypts files and directories so that only authorized users can access them. It can be used to recover lost files and is user-friendly. It cannot, however, protect files on other drives or systems, nor is it completely secure. Since EFS can only be used with the NTFS file system on Windows, using strong passwords and backup keys is essential for increased security.

3. **What are the main characteristics of XML Paper Specification (XPS)?**

A file format created by Microsoft called XML Paper Specification (XPS) guarantees standard document formatting on various devices and printers. Because of its fixed layout, which keeps fonts, graphics, and design components intact, systems can read and handle it with ease. Like PDF documents, XPS documents are made to be easily shared and printed.

4. **What are the advantages of using a Separator Page?**

The job information such as user name, date, time, printer name, and job number are contained on a Separator Page, which is a printable Microsoft Windows Server page. It helps with task organization, job tracking, and user accountability in the Microsoft Windows Server environment. Separator Pages help in keeping a clean and organized work environment by having everyone occupied with different tasks.

Listen to “Episode #111: ZeuS of the DarkNet Diaries podcast which can be found at https://darknetdiaries.com/episode/111/

Based on the podcast, answer the following questions.

5. **Describe the significance of the ZeuS malware in the evolution of online banking threats.**

2007 saw the release of the popular trojan malware Zeus, at a time when cybersecurity and the internet were still developing fields. It was significant because it made it possible for novice hackers to quickly and easily target banks through a basic graphical user interface. The virus was very powerful and inflicted serious harm on its targets. In 2007, its capacity to evade detection by antivirus software was one of its main advantages. Zeus was a strong and scary threat at the time because of his stealth and ease of use.

6. **Explain the concept of a 'money mule' and its role in the ZeuS operations.**

The hackers behind Zeus used money mules to avoid FBI detection and to stop the FBI from connecting the online financial thefts to the Russian hackers. They made checks to the hackers, added the stolen funds to their personal accounts, and moved the money to their bank accounts. The hackers used Craigslist to hire the money mules, pretending that their operations were legitimate.

7. **How did the FBI and international authorities attempt to take down the ZeuS botnet?**

In order to take down the Zeus botnet, the FBI collaborated with foreign authorities, and Evgeniy Bogachev, the botnet's inventor, was charged with bank fraud and money laundering. They shared resources and intelligence with international law enforcement organizations such as Europol and the National Crime Agency of the United Kingdom. In order to stop the infected PCs from communicating with the botnet's command and control center, authorities have targeted and taken control of servers and domains connected to the botnet. The FBI worked with cybersecurity companies to create defenses and conducted public awareness campaigns while examining the malware.

Resources

Zeus – Darknet Diaries. (n.d.). https://darknetdiaries.com/transcript/111/