**Lucas Esquivel**

**CYSE 280**

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

File Auditing can provide details of user accounts that have taken steps to access protected data, documenting the actions taken and the files and folders impacted. This can be cross-referenced with the intended security controls to ensure they are correct. File auditing is a way that ensures safe and secure file server environments where all critical data stored remain safe and out of reach of outside threats and exploits.

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

Advantages of using Microsoft EFS is that it provides protection and security to your folders and files by encrypting them. It also doesn’t cost a penny for Microsoft users as it is already integrated software within the OS and it is also transparent to authorized users, meaning authorized users do not need a password and login credentials. Some disadvantages are that Once a user logs in successfully, no additional authentication is required to access his own EFS encrypted data. Therefore, divulging of the user's password automatically leads to access to that data.

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

The XML Paper Specification (XPS) defines an open document format that uses Extensible Markup Language (XML) to create a document format that is platform-independent, openly published and royalty-free.  The XPS format consists of XML markup that defines the composition of a document and visual appearance of each page along with rendering rules for displaying or printing the document.

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

Separator pages can help to organize paper copies of documents and folders. You can choose whether to have separator pages generated whenever a new folder is encountered during printing, acting as a folder break, or to have separator pages printed instead of printing actual documents.

**5.  What is ZeuS and how does it work?**

ZeuS is a malicious botnet toolkit hackers could use to build a botnet. With ZeuS you could do thinks like launch phishing emails and trojan attacks. ZeuS could be integrated into any malicious code for whatever malicious purpose you want it to do.

**6.  How did law enforcement agencies and security researchers attempt to take down ZeuS?**

Law enforcement and the FBI started the coordinated seizure of computer servers around the world that had backbone of both Gameover ZeuS and Cryptolocker. Recognizing that seizures alone would not be alone they began taking other measures. These measures were in the way of preventing the criminals from being able to send hundreds of thousands of infected computers to contact the servers.

**7.  What were some of the challenges in combating ZeuS?**

Some of the challenges they had was realizing that seizures alone weren’t enough because the criminals could easily and quickly establish new servers in other locations. Another challenge they faced was just how massive in size this botnet was. It had the capabilities of overwhelming and destroying entire operative systems so they really needed to plan and think of a strategy that would get them to destroy ZeuS.