

Lab 6 assessment and questions essay



Dennis Thomas IS4560 Mr.

Schnur LAB 6 ASSESSMENT & QUESTIONS 1. Workstation and desktop devices are prone to viruses, malware, and malicious software, especially if the user surfs the Internet and World Wide Web. Given that users connect to the Internet and World Wide Web, what security countermeasures can organizations implement to help mitigate the risk caused from viruses, malware, and software? Setting policies and securing all the domains of the network. 2.

Your employees e-mail file attachments to each other and externally through the organization's firewall and Internet connection. What security countermeasures can you implement to help mitigate the risk of rogue e-mail attachments and URL web link? Use Anti-virus scanners and malware detection to try and defend against spam or malicious file attachments. Don't run programs of unknown origins. Disable hidden file name extensions, use virus protection. 3.

Why is it recommended to do anti-virus signature file update before performing an anti-virus scan on your computer? This is recommended to show the last time there was an update and show who did it. 4. Once a file is found malicious on your computer what are the default settings for USB/removable device scanning? What should organizations do regarding use of USB hard drives and slots on existing computers and devices? Your USB won't be scanning and detecting the virus but you have to install an anti-virus program to scan and detect it. Your program will not remove the file but remove the virus inside the file.

5. If you find a suspect executable and wish to perform “dynamic analysis” what does that mean? An executable file is file that performs indicated tasks according to encoded instructions is the analysis of computer software that is performed by executing programs built from the software system on a local processor for dynamic program analysis to be effective the target program must be executed with sufficient test input. 6. What is...