Cis 312 7,8,9 questions

Technology, Information Technology

Computer Science and Information Technology Windows Tools and BSOD Errors Q1. A. We used various ways to research tools used in Windows environment. First, we checked personally on the Window tab to ensure familiarity with the primary features. Secondly, I combined this search with documented information about such tools in Windows environment. A critical reflection reveals that PsTools Suite such as the PsList tool is one of the most suitable for administrators because it allows management of local and remote systems.

B. I combined personal experimentation with Windows and review of documented materials to search for information about tools commonly used in Windows environment. For systems administrators, the PsList tool is a useful tool for enabling greater control over both local and remote systems, a key function in system administration.

Q2.

A. Two methods for troubleshooting BSOD errors in Windows 8 are i. using safe mode, and ii, using Windows Boot Genius, a robust screen repair program. The Windows repair program is more useful to system administrators because it has over 20 OS repair tools that can help fix almost all boot issues including BSOD. Windows 9 xs/Me Resource Meter can also help in determining whether computer has sufficient FSRs (Soper, 2004).

B. The two primary methods of BSOD troubleshooting in Windows 8 include the BSOD screen repair program and the utilization of safe mode repair. The former method is more suitable for systems administrator because it enables repair of virtually all boot issues in Windows 8.

Network Connections

Q1.

A. Networking components considered in home office to maximize functionality are the structure of management information (SMI), Management information base (MIB), and SNMP agents. SMI would help in defining data types allowed in MIB while the IB would help in holding value for managed objects based on packets that arrive from previous system reset. Lastly, SNMP agents components would help in executing all relevant MIB objects

B. The best networking components for maximizing functionality are SNMP components: SMI, which describes MIB data types, MIB that stores clock ticks since system resetting, and SNMP agent component, which define information contained in MIB to help in the management of used applications.

Q2.

A. Various vendor support sites help in troubleshooting home internet connections. The most useful sites include the Network Diagnostic tool, Microsoft Automated Troubleshooting Services tools, as well as manual troubleshooting via http://www. microsoft. com, http://www. msn. com, http://support. microsoft. com/gp/vendors/en-us, and http://windowshelp. microsoft. com/Windows/en-US/Help/33307acf-0698-41ba-b014-ea0a2eb8d0a81033. mspx for wired connections. Microsoft support sites are credible and robust.

B. Vendor supported sites for troubleshooting home connections include http://windowshelp. microsoft. com/Windows/en-US/Help/33307acf-0698-41ba-b014-ea0a2eb8d0a81033. mspx used for wired connections, and

http://www. msn. com for manual troubleshooting. Both http://www. msn. com and http://www. microsoft. com are very useful to customers because of their credibility.

Ethical Concerns and Crime in Technology

Q. 1

A. Technology plays a critical in the today's workplace. Consequently, although companies have a right to monitor technology usage, this should affect employee privacy. Constant monitoring of information technology can help companies to enhance information security. However, the need for enhanced security should never impede on user privacy. The primary position is that although security and privacy can be competing objectives in today's workplace, companies have no moral (or even legal) right to intrude employee privacy on flimsy grounds of system monitoring.

B. Constant security monitoring is an obligation of any company running information systems. However, implementing strong security system does not necessarily mean intruding user privacy. Companies should never view security and privacy as exclusive goals. Rather, companies should protect both the security of its IT as well as the privacy of its users.

Q. 2

A. It is virtually impossible for cybercriminals to perpetuate this crime without technology. This means that technology serves as a tool for propagating crimes. In particular, technology equips cybercriminals with the tools and techniques for carrying out sophisticated attacks that are difficult to detect.

B. It is impossible to create the crime without using technology. That is,

technology allows attackers to launch information system attacks that defy defense systems whilst allowing the criminals to remain anonymous.

References

Soper, M. (2004). Absolute Beginners Guide to A+ Certification. Que Publishing.