Example of windows and linux vulnerabilities essay

Technology, Computer

Technology surrounds us in various forms, and we accomplish results that would have been highly impossible without the commonly used technology, the Computers. As we become more familiar and assimilated to the computers, their flaws become our weaknesses. Every computer system runs on an operating system such as Windows, Linux, or Mac OS, and these systems can be prone to threats from attack sources, which exploit the weaknesses and vulnerabilities. Windows and Linux have their own advantages and disadvantages; however, their vulnerabilities cannot be ruled out. This paper discusses the differences of Windows and Linux vulnerabilities and a few methods to protect the system from these vulnerabilities.

Windows operating system is more prone to vulnerabilities, as Windows was initially aimed as a single-user operating system, where any user could gain administrator rights over the system. The disadvantage of such login was favorable for the viruses that made use of such feature by setting themselves into the system without any authorization from the administrator. Windows had multiple versions of old operating system on which the programs accessed the whole system freely. This led Microsoft to enhance the security of Windows in order to be compatible with the older OS. Linux, an open source software product, consists of distinct file system that requires administrator rights that is provided by the root or user password, in order to install. Viruses and Worms cannot install themselves on Linux because the root and user password cannot be obtained easily. Vulnerability in Windows is mainly caused by the buffer overflow that provides an opportunity to the malware that exploits the system. Many files

with the . exe and . scr extension can be run on Windows, which can be vulnerable, if opened, without scanning them with an anti-virus. In Linux, the user must read the e-mail, save the attachment, and later provide executable

permissions to the attachment, and then execute the file. This is one such example that makes Linux less vulnerable than Windows. Linux is made up of packages and there are security problems with the packages, such as ORBit, gnome, usermode, PAM, esound, initscripts, ypserv, wu-ftpd, screen package, and Linux ipchains firewall. The ORBit and esound package used a source of random data that was easily guessable, allowing an attacker with local access to guess the authentication keys used to control access to these services (Tanik & Yoo, 2002).

Buffer overflow is also possible in Linux, especially in Red Hat Linux through the Vixie Cron package. The users can set environment variables through the crontab using this package, and it is prone to provide root access to the attackers. A vulnerability assessment or vulnerability analysis involves recognizing what could occur that would adversely affect the consistency, reliability or privacy of the computing environment (Mann & Mitchell, 2000, p. 14).

A computer user or an organization must first understand the most common methods of attack on the operating system. This understanding will allow devising new controls that will limit an attacker’s capability to recognize threats, and the organization can address these vulnerabilities and realize the threat. Once vulnerability is detected, the best option is to remove it. There are many methods to address vulnerabilities, and the best option must

be chosen depending on situation. A host-based auditing tool is theoretically more comprehensive than a network-based vulnerability assessment tool simply because it has greater access to system information than a network-based tool (Mookhey & Burghate, 2005, p. 37). Some operating systems employ various techniques in order to make life harder on the attacker, such as address space layout randomization or non-executable stacks. Though Linux has vulnerabilities, it is a powerful operating system and will be an excellent choice for not only personal UNIX users but also distributed computing (Tanik & Yoo, 2002).

References

Mann, Scott. Mitchell, Ellen L. (2000). Linux System Security: An Administrator's Guide to

Open Source Security Tools, Illustrated. Reprint. Prentice Hall Professional. Print.

Mookhey, K. K. Burghate, Nilesh. (2005). Linux-- Security, Audit and Control Features.

Illustrated. ISACA. Print.

Tanik, Haluk. Yoo, Seung. (2002). Linux Securities and Vulnerabilities. Retrieved from

http://cs. ucsb. edu/~koc/ns/projects/00Reports/TY. pdf Oregon State University. Web.