Cybersecurity

Technology, Information Technology

Question 3 Vulnerability is a fault in a system that an attacker/hacker uses to reduce the security of the information inthe system. Microsoft XP is known to be vulnerable to several threats; some of them include the following:

Microsoft windows XP do not allot adequate memory for SMTP control replies hence allowing hackers to be able to read parts of e-mail messages through the use STARTTL commands. This is known as SMTP memory allowance vulnerability. (Vetterling, 2002)

Windows XP is vulnerable in HTTP services where an attacker who notices this flaw can win an absolute control of computer system and be able to manipulate the already installed programs and do any other thing to the system with full user rights.

Argument injection in packager. exe is another vulnerability of windows XP. This allows an attacker to interfere with the system by using the (/), slash, character that makes the command prior to the slash to be effected, which is the hackers' command (Ren, 2010).

Question 2

The common criterion is an internationally recognized set of standards that are used to successfully evaluate the security of a system like the operating system. It enhances the confidentiality of the user to a system as its certification is recognized globally and therefore all systems purchased throught the world are subjected to the same level of security standards. (Caplan, 1999)

The common criterion ensures that customers can trust the system they are purchasing or using in terms of confidentiality, availability and integrity. Before a product is introduced to the market a vendor must submit the

system for certification to an accredited testing laboratory. He has to specify the security target (ST) which describes an outline of the system, possible security threats and how the security details will be implemented in the system. The testing laboratory then checks the product to verify its security in order for certification. The common criterion is hence a trustable method to ascertain the security of a system. (Elof, 2003)

References

Caplan, K. & Sanders, J. L.(1999). Building an International Security Standard, 1. Retrieved from http://ieeexplore. ieee. org/xpl/freeabs_all. jsp? arnumber= 774938

Eloff, J., and Eloff, M. (2003). Information Security Management. Retrieved from http://www. sis. pitt. edu/~jjoshi/TELCOM2813/Spring2005/SecManParadigm2. pdf

Ren, K. (2010). IEEE Transactions on Smart Grid, Special Issue on Cyber, Physical, and System Retrieved from https://lists. cs. columbia. edu/pipermail/tccc/2010-June/015911. html

Vetterling, M., Wimmel, G.,& Wisspeintner, A. (2002). Secure Systems Development Based on the Common Criteria: The PalME Project, 27. Retrieved from http://dl. acm. org/citation. cfm? id= 605486