Computer crime

Computer CrimeQuestion #2 Computer CrimeDaniel KilburnComputer Science 300Professor ChristensenMay 11, 2007Question #2 Computer CrimeThe Penetration Attack: This type of attack involves breaking into a system using the known security flaws of the system. Once the intruder has penetrated the system he has access to the entire systems resources. Acting as an authorized user the intruder can perform any task that suits his needs.

Data can be altered, removed, or copied. Viruses and Trojan Horses can be inserted. And the system can be forced to perform functions without the owners??™ knowledge or permission. Known Penetration Attacks have happened to Universities where students have attempted to alter their grades. In the business sector, disgruntled employees have attempted to steal propriety information for personal profit or to cause damage to their employer. Financial services are often targeted to collect financial data and make fraudulent withdrawals. These attacks can be accomplished either through direct access to the system, through backdoors known to insiders, or through the introduction of Viruses, or Trojan Horses from outside sources. Depending on the intruders??™ intent, the attack can be localized to a specific system.

If connected to a LAN, or WAN network it can become a regional or even a global attack. Through the use of Phishing, Viruses and Trojans inserted into e-mails or planted from suspect websites. These types of attacks are becoming more frequent as more people and systems come online. The creators of these programs have their own industry.

It is possible to find damaging and malicious software free for the taking on the internet, and elaborate Phishing kits can be purchased making it easier for the non-code writer. It is speculated that some international criminal organizations co-op the better programs. Besides it being easy to find malicious software on the internet the computer industry is lending a helping hand. Even before reputable software hits the stands, white papers detailing a programs flaws can be found all over the internet, providing detailed ways for hackers to write new code to commit their crimes.

The ease of setting up an official looking website with an official sounding name makes it easy for the uneducated computer user to fall prey to an attack, just by responding to an official looking e-mail from a company they happen to do business with. Though most people think of these types of attack as coming from some vile bug in the system, the most prevalent form of Penetration attack comes from users either freely giving up their credentials through Phishing scams. Or by visiting counterfeit websites where malicious software can de inserted on the victims computer.

This is not a crime limited to the United States it has already reached a global audience. Nations with populations that have money to spend, and are connecting to the internet will be the primary targets. Perpetrators are increasingly being found in the former Soviet Union countries of Eastern Europe, Asia, and the Caribbean.

This type of crime will continue to be a problem as long as there is something of value to be taken from cyberspace. The continued proliferation of technology and wiring of the population will constantly keep a supply of

uneducated users available to the predators of the world, and distance is not a problem. ReferencesKizza, J. M. (2003). Ethics and Social Issues in the Information Age. David L.

Carter, Ph. D., FBI Law Enforcement Bulletin. Retrieved 5 April 2007 from. http://nsi. org/Library/Compsec/crimecom. htmlThompson, C. (2004).

The Virus Underground. In De Palma, P (Ed) Annual Editions, Computers in Society (2007)mputer Crime