Potential forensic techniques for investigating insider attacks

Technology, Information Technology

Topic: Discuss potential forensic techniques for investigating insider attacks. Also discuss how insider attackers can defeat these techniques. Insider attacks occur when a user of an organization uses an unauthorized system to find information about the organization. In order to do this, the user must counter the computer security system and the forensic techniques used by this system. Attacks done by inside users has proven to be more costly and harmful than the attacks done by outsiders as the inside users have more information about the internal processes of the organization and they also have an access to various resources of the organization. Insider attacks is often destructive of the organization`s reputation as well. Therefore, all organizations must try to stop insider attacks and investigate these attacks through advanced forensic techniques. One such forensic technique is the intrusion detective system (IDS) which checks all incoming and outgoing network activities of an organization. It is a system which helps in identifying those patterns which are suspicious and which may indicate an attack as someone attempts to break into a system. Although IDS may detect system attacks, it alone might not be able to deter both insider and outsider attacks. This is because the accuracy of IDS to detect attacks may affect the entire process of the organization. IDS may overlook an actual attack or even issue alerts for a normal event. This false positive may be highly costly for the organization as the IDS will collect useless data for a normal user. The costs of IDS include damage, operational as well as response costs. An organization should try to minimize these costs as much as possible so that normal system process is not affected. Unfortunately, the IDS can be evaded by attackers who learn to act as legitimate users. In order to beat an anomaly detector, which detects discrepancies by comparing the current network to the baseline, the attacker should learn to impersonate as a legitimate user. Another forensic technique is proactive intrusion detection system which tries to overcome the limitations of IDS. This system tries to expose both the legitimate users and attackers to different modes of IDS, in a way that poses no threat to the legitimate users but detects those attackers who have learnt to use the system as legitimate users. Therefore, these attackers will get detected by this forensic technique which is far more effective than a common IDS. 2. Discuss the techniques to identify potential on-line sexual crime that could be posted via online dating forums. You may use one example to illustrate this. Sexual crime includes different forms of sexual behaviour portrayed by humans. Different countries have unique laws pertaining to sexual crime. The western culture is more tolerant to some sexual activities but there are serious laws for other crimes for example rape, child sexual abuse, human trafficking etc. other cultures with strong religious customs constitute a large range of sexual activities as crime. General sexual rules followed by most of the countries include laws against rape, sexual harassment. The law also requires the government or other authorities to regulate and control obscene material over the internet and censor these materials. With the advance of information technology, it has become difficult for authorities to regulate such activities, especially over the internet. Authorities have been able to investigate acts of crime involving terrorism, fraud etc but the number of these crimes have continued to increase. These crimes are posing a threat to the continued advancement of technology and online sexual crime is on a rise. There are several techniques to identify potential online sexual crime and the most effective is to develop a forum where individual can file complaints against such crime. Regulating authorities of all countries should make it easier for citizens to file complaints against sexual crime by developing an easily accessible forum. The citizens should be made aware of such forums through advertising and other forms of promotions. These forums can prove to be highly effective as the dating forums are often found by internet users through surfing and these individuals can then tell the authorities by filing complaints. Filing a complaint will not solve such problems. The authorities should make sure that these complaints are acknowledged and the offenders of sexual crime are punished. These complaint forums will give the citizens a chance to raise their voices against sexual crime such as child pornography and other obscene materials. Another technique is to regulate and monitor all the dating forums and other related online sites. This can prove to be highly effective as the all materials posted or exchanged on such sites will be monitored by the appointed authorities and any offensive transaction or material could be easily traced to its source. This technique will also discourage such materials and exchanges, as the individuals will be aware of the close examination being done by the regulatory authorities. Works Cited: Question 1: " A layered approach to insider threat detection and proactive forensics." Insider threats. N. p., n. d. Web. 23 Oct. 2012. . " Proactive detection of insider attacks." Illinois Education. N. p., n. d. Web. 23 Oct. 2012.