Intrusion detection

Running head: intrusion detection Intrusion Detection Affiliation September 2009 Computers are commanding tools that facilitate users to store and perform operations on huge amounts of data rapidly. Almost every organization, no matter what is size of organization, makes use of computers to manage bookkeeping, track inventory, and store documents. As organizations grow, they often need several people to enter and process data at the same time. For this to be advantageous, those people must be capable to share the data each person enters. Networking computers turns out to be advantageous in this state of affairs. Networks are merely a collection of computers linked by cable or other media so they can share information (Nash, 2000). There are different evils also associated to these network structures also. Personal information theft, business information hacking and virus attacks are the contemporary problems organizations are facing nowadays in the network communication and data transfer areas (Frederick, 2002). Because of the rising amount of intrusions and since the local networks and Internet have turned out to be so ubiquitous, businesses more and more applying a variety of systems that monitor Information Technology security breaches (Sans, 2009).

Network Intrusion as its name represents, attempts to identify attempted or applied intrusions into network and to establish suitable actions for the intrusions. Intrusion detection includes an extensive collection of methods that differ on several axes. A few of these axes comprise: (Silberschatz, Galvin, & Gagne, 2004):

The time period that detection takes place: in real time (while it is taking place) or following the information only.

The types of input inspected to identify intrusive action. These could

comprise user shell commands, process system calls, as well as network packet headers or contents. Several types of intrusions might be identified only by correlating information from various such sources.

The variety of action capabilities. Basic and straightforward types of actions consist of changing an administrator of the possible intrusion or in some way halting the potentially intrusive action, for instance, killing a course of action engaged in actually intrusive activity. In a complicated type of action, a system might clearly redirect an intruder’s action to a trap. A false resource exposed to the attacker with the aim of observing and gaining information about the attack; to the attacker, the resource appears real.

These levels of freedom in the design of space for detecting intrusions in systems have brought an extensive variety of solutions acknowledged as intrusions detection systems (IDS) (Silberschatz, Galvin, & Gagne, 2004). The accomplishment of the Intrusion detection system or IDS offers a great advantage for the detection of the possible security concerns and attacks on time and effective handling of these concerns (Sans, 2009). An Intrusion detection system or IDS is hardware and software based system to identify unwanted efforts at accessing, disabling or manipulating computer systems, mostly in the course of a network, such as the Internet. These efforts can take the shape of attacks, as examples, in the form of malware, crackers or disgruntled workers (Bradley, 2009). An intrusion detection system is also utilized to identify numerous forms of malicious behaviors that are able to compromise the security as well as trust of a computer system. This comprise network attacks besides data driven attacks on applications, vulnerable services, host based attacks like that privilege escalation, access to sensitive files, unauthorized logins and malware (for example Trojan

horses, viruses, and worms) (Comptechdoc, 2009).

By seeing the importance of the intrusion detection system and its vital significance for the deployment at business and organizational areas, I have decided to work on intrusion detection and its associated aspects as a semester project. This research based project will offer a detailed analysis and examination of main areas and possible security concerns that organizations are facing in the business and organizational structures. This assessment will offer us to develop a list of main security concerns we are facing nowadays and its possible forms. The analysis of the intrusion detection will offer us the opportunity for the analysis of the main security concerns we are facing and effective handling of these security imitations. This project will provide a deep insight into the intrusion detection and detailed analytical examination of the network attacks, data driven attacks on applications, vulnerable services, host based attacks like that privilege escalation, access to sensitive files, unauthorized logins and malware (for example Trojan horses, viruses, and worms). In this way this project will completely address the main security concerns and intrusion detection techniques for the network security implementation. In this research based project I will use the authenticated academic journals, for retrieving the possible help and assistance regarding the project completion. The web based better information resources will also be incorporated in this project.

References

Bradley, T. (2009). Introduction to Intrusion Detection Systems (IDS). Retrieved 09 28, 2009, from http://netsecurity. about. com/cs/hackertools/a/aa030504. htm

Comptechdoc. (2009). Network Intrusion Detection. Retrieved 09 28, 2009,

from http://www. comptechdoc.

org/independent/security/recommendations/secintdet. html

Frederick, K. K. (2002). Evaluating Network Intrusion Detection Signatures, Part One. Retrieved 09 29, 2009, from http://www. securityfocus. com/infocus/1623

Nash, J. (2000). Networking Essentials, MCSE Study Guide. California: IDG Books Worldwide, Inc.

Sans. (2009). Intrusion Detection FAQ: What is Intrusion Detection? Retrieved 09 28, 2009, from http://www. sans. org/resources/idfaq/what_is_id. php

Silberschatz, A., Galvin, P. B., & Gagne, G. (2004). Operating System Concepts (7th Edition). Wiley.