National Conference on Communication Technology & Network Security In association with
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 7 | ISSN : 2456-3307

A Study on Intrusion Prevention/Detection

Dr. Vinay Ranganathan[1], Ravikant S. B.[2]
[1]Professor, Charan's Degree College, Ulsoor, Bangalore, Karnataka, India
[2]Assistant Professor, Charan's Degree College, Ulsoor, Bangalore, Karnataka, India

ABSTRACT

Today one of the most important challenges in communication is securities interior network. Understanding the basics of any technology is significant if ever aiming to totally perceive that technology. A good security answer not solely solves the protection perplexity, but also reduces the total cost of implementation and operation of the network. This paper highlights all the treads that have an effect on network security like legal problems, privacy concerns and people shortages. The eminent use of recent technologies needs associate hyperbolic have to be compelled to defend valuable data and network resources from corruption and intrusion. Now a day's anybody with a PC and an internet connection can download attacking tool and start attacking. These tools are commonly referred to as kiddle-scripts. Hackers are people who play around with software code in order to understand how it works. They might discover holes with in the systems and can oftenbe veryaltruistic. A crackeris one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. As a result he gain unauthorized access and destroys very important data. There are many threats to port and protocols. Each attack has its characteristic and totally different handling to forestall system from them. There are several network security tools to facilitate network security like firewalls, proxy server, web contents filters and others. The paper gives all emphasis on the key elements of network security and its weaknesses.

Keywords : Network security, Data privacy, Security trends, Security goals, Hackers, Crackers.

I. INTRODUCTION

For several years now, society has been dependent on information technology (IT).With the rise of internet and e-commerce this is more applicable now than ever. People rely on computer networks to provide them with news, stock prices, e-mail and online shopping. People's credit card details, medical records and other personal information are stored on computer systems. Many companies have a web presence as an essential part of their business. The research community uses computer systems to undertake research and to disseminate findings. Computers control national infrastructure components such as the power grid. The integrity and availability of all these system shave to be protected against a number of threats. Amateur hackers, rival corporations, terrorists and even foreign governments have the motive and capability to carry out sophisticated attacks against computer systems. Therefore, the field of information and communication security has become vitally important to the safety and economic wellbeing of society as a whole. Moreover, to expose privacy breaches, security needs powerful intrusion detection and prevention systems (ID/PSs).This paper focuses on providing an up-to-date comprehensive state of the art of ID/PSs based on risk analysis. In Section 1.1, we present a background introduction to ID/PSs. In Section 2, we briefly outline the definition of risk management and its importance in developing well- managed security

systems. In Section 3, we provide a brief overview of ID/PSs, including a description of what ID/PSs are, the functions they serve, the two primary types of detection and prevention systems and different methods of ID that may be employed. Finally, in Section 4, we present the main goal of this work when we discuss in detail, with examples of some threat incidents occurred during the years 2018 and 2019, the requirements driving the necessity of developing anew detection mechanism to detect known and unknown threats based on intelligent techniques such as machine learning and autonomic computing.

II. METHODS AND MATERIAL

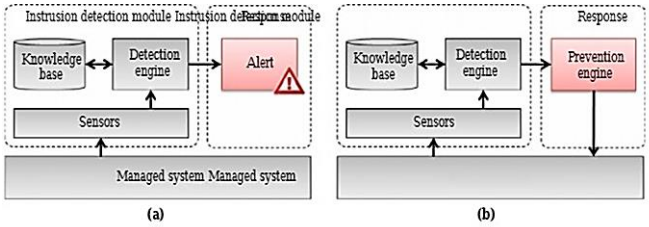
Background

In order to understand the ID/PSs, first one must understand the nature of the event they attempt to detect. An intrusion is a type of attack on information assets in which the instigator attempts to gain entry into a system or disrupt the normal operations of a system. In Brown's et al. (2002) view, intrusions are actions that attempt to bypass security mechanisms of computer systems. They are any set of actions that threaten s the integrity, availability or confidentiality of the information and the information system, where integrity means that data have not been altered or destroyed in an unauthorized manner and where confidentiality means that information is not made available or disclosed to unauthorized individuals, entities or processes. Availability means that system that has the required data ensures that it is accessible and usable upon demand by an authorized system user. Occasionally, an intrusion is caused by an attacker accessing the system from the internet or the network, or from the operating system of the infected machine, or exploits any security flaw of third party (middleware) applications that manages the information system. Attacks that come from these external origins are called outsider attacks. Insider attacks, involve unauthorized internal users attempting to gain and misuse non-authorized access privileges.ID is the process of monitoring computers or networks for unauthorized entry, activity or file modification. An intrusion detection system (IDS) is a software or hardware device that automates the ID process. IDSs can respond to suspicious events in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. Intrusion prevention is the act of intercepting detected system threats in real time by preventing them from continuing to their intended destinations. It is useful against denial of services, floods and brute force attacks (Martin, 2009). An intrusion prevention system (IPS) is a software or hardware device that has all the capabilities of IDS and can also attempt to stop possible incidents. An IPS can respond to a detected threat in several ways: It can reconfigure other security controls in systems such as a firewall or router to block future attacks; It can remove malicious content of an attack in network traffic to filter out the threatening packets; or.it can (re-)configure other security and privacy controls in browser settings to prevent future attacks. Usually, disable prevention features in IPS products cause them to function as IDSs. IPSs are considered to be an extension of IDSs, although IPS and IDS both examine network traffic searching for attacks, there are critical differences. IPS and IDS both detect malicious or unwanted traffic. They both do so as completely and accurately as possible, but they differ in the type of response provided by each. As shown in Figure 1, the main function of an IDS product is to warn of suspicious activity taking place whiles is designed and developed for more active protection to improve upon the IDS other traditional security solutions, which can react in real time to block or prevent those activities. An effective risk management process is an important component of a successful IT security system. Organizations should use risk management techniques to identify the security controls necessary to mitigate risk to an acceptable level. To design an effective

ID/PS, proper requirements capture based on risk management is essential.

Importance of risk management

It is expected that all computer and communication systems, including all the applications, system software's and infrastructure and networking services, are protected from accidents and abuse by a set of safety measures composed from security, privacy, trust, audit, digital forensics and fault- tolerance functions, in order that they areto be available, reliable, trusted, safe, identifiable and auditable. Equally, these functions must provide the necessary facilities to end-users, make them feel safe and trusted in the complex world of information communication technology driven by the web, the internet, mobile and ad hoc wireless networks where today everything from business to leisure has become e-everything. These safety measures are vital in economic terms. Risk is the net negative impact of the exercise of vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. It is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions (Chichakli, 2009). A strong security program reduces levels of threat to reputation, operational effectiveness, legal and strategic risk by limiting an organization's vulnerability to attempted intrusion, thereby maintaining confidence and trust in the institution. Security concerns can quickly erode customer confidence and potentially decrease the adoption rate and rate of return on investment for strategically important products or services. An effective risk management process is an important component of a successful IT security program. The principal goal of an organization's risk management process should beta protect the organization and its ability to achieve its mission, rather than simply its IT assets. Therefore, the risk management process should not be treated as merely a technical function carried out by the IT experts who operate and manage the IT system, but as an essential mission-critical management function of the organization. Risk-based protection strategies are characterized by identifying, understanding, mitigating as appropriate and explicitly accepting the residual risks associated with the operation and use of information systems. To help protect organizations from the adverse effects of on-going, serious and increasingly sophisticated threats to information systems, organizations should employ a risk-based protection strategy along with ID/PSs, as a complete system of protection to ensure the integrity, availability and confidentiality of the information and the information systems.



Notes: (a) IDS; (b) IPS

Figure 1. Typical intrusion detection and intrusion prevention systems

Intrusion detection and prevention systems

Whitman and Mattered (2005) defined ID as the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies or standard security practices. An ID is a device or software application that monitors network and/or information system for malicious activities or policy violations and responds to that suspicious activity by warning the system administrator by one of several ways, including displaying an alert, logging the event or even paging the administrator. Intrusion prevention is the process of performing ID and attempting to stop detected

possible incidents. The IPS is a device or software application that has all the capabilities of IDS and can also attempt to stop possible incidents. IPS is designed and developed for more active protection to improve upon the IDS and other traditional security solutions. An IPS is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets (Martin, 2009). IPSs are designed to protect information systems from unauthorized access, damage or disruption, IDS informs of a potential attack, whereas IPS makes attempts to stop it. IPS has another benefit or advantage over IDS in that it has the ability to prevent known intrusion detected signatures, besides the unknown attacks originating from the database of generic attack behaviors (Beal, 2005).Modern ID/PSs are comprised two basically different approaches, network- based and host-based. A relatively recent addition of special IDS called application-based is a refinement of the host-based ID (Brown et al., 2002). Both servers and workstations are protected by host-based intrusion detection/prevention systems (HID/PSs) through secure and controlled software communication channels between system's applications and operating system kernel. The software is preconfigured to determine the protection rules based on intrusion and attack signatures. The HID/PS will catch suspicious activity on the system and then, depending on the predefined rules, it will either block or allow the event to happen. HID/PS monitors activities such as application or data requests, network connection attempts and read or write attempts to name a few. One potential disadvantage with this approach is that, given the necessarily tight integration with the host operating system, future operating system upgrades could cause problems. Network-based intrusion detection/prevention system (NID/PS) is software or dedicated hardware system that connects directly to a network segment and protects all of the systems attached to the same or downstream network segments. Network ID/PS devices are deployed in-line with the network segment being protected (Martin, 2009). All data that flows between the protected segment and the rest of the network must pass through the network ID/PS device. As the traffic passes through the device, it is inspected for the presence of an attack. When an attack is identified, the network ID/PS discards or blocks the offending data from passing through the system to the intended victim thus blocking the attack. NID/PS will intercept all network traffic and monitor it for suspicious activity and events, either blocking g the requests or passing it along should it be deemed legitimate traffic. One interesting aspect of network intrusion prevention system is that if the system finds an offending packet of information, it can rewrite the packet so the hack attempt will fail, but it means the organization can mark this event together evidence against the would be intruder, without the intruder's knowledge. Regardless of whether they operate at the network, host or application level, all ID/PSs use one of two detection methods; signature-based or anomaly-based (Whitman animator, 2005).

Anomaly detection is designed to uncover abnormal patterns that deviate from what is considered to be normal behavior, whereas ID/PS establishes a baseline of normal usage patterns and anything that widely deviates from it gets flagged as a possible intrusion. Anomaly detection can also vary but one should be aware that if any incident occurs more or less than two standard deviations from the statistical norm would raise an alarm. An example of this would be if a user logs on and off of a machine eight times a day instead of the normal one or two. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. Once again, if a user in an IT department suddenly starts to access accounting programs or recompiles them, then the system must immediately raise an alarm or alert its administrators

(Minnelli and McMillan, 2001).The major benefit of anomaly based detection methods is that they can be very effective at detecting previously unknown threats (Scarf one and Mel, 2007).Usually, in the first stage of a deployment of an anomaly-based ID/PS, the system learns what a normal behavior is. The controlled system is running as usual under the assumption that there is no abnormal behavior. During the learning stage, no attack must occur in the controlled system so that the ID/PS does not learn to ignore the attacks. The learning process can be addressed by variety of means such as machine learning or building statistical behavioral profiles. In the second stage of the deployment, in which the system possibly faces attacks, the ID/PS monitors the activities in the controlled system and compares them to the learned normal behavioral patterns. If a mismatch occurs, a level of "suspicion" is raised and when the suspicion, in turn, trespasses a given threshold, the system triggers an alarm. The main advantage of anomaly detection is that it does not require prior knowledge of intrusion and can thus detect new intrusions. The main disadvantage is that it may not be able to describe what an attack is and may have high false positive rate. Unauthorized behavior is normally detected by their misuse and is also commonly referred as signature detection. However, this method uses known patterns of unauthorized behavior to predict and detect subsequent similar attempts. These specific patterns are called signatures. For host-based intrusion detection/prevention, one example of a signature is "three failed logins." For network intrusion detection/prevention, a signature can be as simple as a specific pattern that matches a portion of a network packet (Whitman and Mattered, 2005). For instance, packet content signatures and/or header content signatures can indicate unauthorized actions. The occurrence of signature might not signify an actual attempted unauthorized access (for example, it can be an honest mistake), but it is a good idea to take each alert seriously. Depending on the robustness and seriousness of a signature that is triggered, some alarm, response or notification should be sent to the proper authorities. The concept behind misuse detection schemes is that there are ways to represent attacks in the form of a pattern or a signature so that even variations of the same attack can be detected. This means that these systems are not unlike virus detection systems, they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. An interesting point to note is that anomaly detection systems try to detect the complement of "bad" behavior. Misuse detection systems try to recognize known "bad" behavior. The main issues in misuse detection systems are how to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match non-intrusive activity (Newman et al., 2004).The main advantage of misuse detection paradigm is that it can accurately and efficiently detect instances of known attacks. The main disadvantage of misuse detection method is that it lacks the ability to detect the newly invented attacks. Signature databases must be constantly updated, and IDSs must be able to compare and match activities against large collections of attack signatures.

III. CONCLUSION AND FUTURE RECOMMENDATIONS

Today's interrelated computer network is a dangerous realm, filled with people that have millions of man-hours available to employ against the strongest of security strategies. The only way to beat them is to know when they are attempting an attack and counter their attempts. Strategy is the key and selecting the right ID or prevention system will be instrumental in ensuring that an enterprise's networks and systems remain secure. As security incidents become more numerous, ID/PS and supporting tools are becoming increasingly necessary. These intelligent ID/PSs and tools should use a combination of several intelligent techniques from the subject areas of autonomic

computing, machine learning, artificial intelligence and data mining to assist them to determine what qualifies as an intrusion, versus normal activity, by building acknowledge base which grows as and when new facts or knowledge come to light.ID/PSs are still a fledgling field of research. However, it is beginning to assume enormous importance in today's computing environment. The combination of facts such as the unbridled growth of the internet, the vast financial possibilities opening up in electronic trade and the lack of truly secure systems make it an important and pertinent field of research and development. Future research and development trends seem to be converging towards a model that is based on multi-agent ID/PSs based on and managed by autonomic computing paradigm together with advanced techniques from natural language processing, artificial intelligence and data mining to help improve anomaly ID, based on itself-managed properties such as self-configuration, self-optimization, self-healing and self-protection. These autonomic computing properties have to be extended to include self-detection and self-prevention. The results from these techniques will aid an analyst to clearly distinguish malicious attack activities from normal everyday on-attack activities. They will make ID/PSs smart and a formidable part of security management system with a rich but simplified alarm handling and presentation of security violation activities for easy human consumption.

IV. REFERENCES

[1]. https://en.wikipedia.org/wiki/Intrusion_detection_system
[2]. Data Protection Technical Guidance Note: (PET) Privacy enhancing technologies (ICO)
[3]. https://searchsecurity.techtarget.com/definition/intrusion-detection-system
[4]. http://www.legalserviceindia.com/articles/articles.html

Cite this article as :

Dr. Vinay Ranganathan, Ravikant S. B., "A Study on Intrusion Prevention/Detection", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 4 Issue 7, pp. 32-37, September-October 2019.
Journal URL : http://ijsrcseit.com/CSEIT19476