EMPLOYBILITY OF INTRUSION DETECTION USING IP AND MAC ADDRESS TRACING IN CLOUD COMPUTING NETWORK

Raghav Mittal

ABSTRACT

Intrusion and attack continue to happen in a network by exploiting vulnerabilities.The fortification at several layers has been carried out in order to strengthen the security, yet malicious software enters into one's computer. Advance IDS is widely used to prevent potential Intrusion in a network. Wide ranges of IDS exist in the market to counter-attack. IDS suited for one scenario may be ill-suited to others. Accordingly, this work highlights the vulnerability existing and measure to fortify them. Major IDSs have been explored. Finally, a comparative study is widely used IDS has been presented for the wider understanding of all the stakeholders and enables them to select the IDS that suits well in their case.

INTRODUCTION

With the increasing need for information sharing, connectivity among networks have grown manifold. Vulnerability in one network can adversely impact the other Network. Once compromised may lead to deletion of data, modification of data, or may encrypt the data for the ransom. Even world's well secure system was compromised and had to pay a ransom in order to free their data. New emerging paradigm cloud computing is also not safe and witnessed several attacks that have shaken the world's confidence in security (Singh, 2014a; Singh, 2014; Singh &Raghuvanshi). Even mobile-based cloud computing is not secure and needs to be protected at several levels (Singh, Mathur, & Kumar, 2012). An attack on a network is caused by injecting the malware in a network or any other node. Injection happens by way of exploiting the vulnerabilities (Gleichauf, Randall, Teal, Waddell, &Ziese, 2001). Insiders are also emerging as the major threats and need to be checked at the appropriate level (Singh, 2014a). Vulnerabilities in application and hardware have been exploited by the Network or nodes. Attacks from outside the Network are caused by intruding into a network and monitor the activities of a network. This Intrusion may be to gain a competitive advantage or to damage the Network (Benjamin, 2010). The magnitude of damage caused has enhanced in recent times. Even the rescuers are unable to recover the Network. For instance, encryption of data caused at leading university, hospital, and other business ventures. The rest of the paper is organized as: Section 2 has undertaken the major work in the area. Section 3 enumerates the network vulnerabilities and the way the same has been exploited by the adversary. Section 4 explores the major IDS, and finally, this work ended with a comparative study on major IDS in the market.

RELATED WORK

Vulnerability detected can be used to put the service's downtime or to compromise the data. Financial activity's reliance on technology has grown manifold. Owing to the usage, the cost of downtime is higher for the financial institutions. Vulnerabilities correlation with respect to the financial institution was carried out by (Roumani, Nwankpa, &Roumani, 2016). The study reveals that vulnerability is correlated to the number of financial records maintained by the financial institution. Proposed a novel dynamic shellcode analyzer named 'shelter,' a shellcode that was a binary file, capable of exploiting the vulnerabilities and automation of the task by introducing the tool named Shellzer. The tool was tested on over 24,000 real-world samples for the wider acceptance, and results generated were 98% accurate. The tool was capable of finding out the vulnerability from the deployed Network. The usage of Nonvolatile main memory (NVMM) is growing. Researchers (Kannan, Karimi, Sinanoglu, & Karri, 2015) have highlighted the vulnerability in NVMM that has emerged due to its nonvolatile property. In NVMM, data remains even after the system is put off since the sensitive information such as password may be lying in the NVMM and proposed by Sneak Path Encryption (SPE), which is a hardware-based intrinsic encryption technique for memristor-based NVMM. Authors claimed it to effective in securing the data at the same time would not cause any overhead on performance.

Static method to discover the software faults and the security vulnerabilities in the software system was used by (Goseva-Popstojanova&Perhinschi, 2015). Authors have used the static code analyzer to figure out

The vulnerability and in turn conducted the empirical study on the effectiveness of the analyzer and shortcoming. Their findings revealed that the software coded in the language 'C' and 'C++' is highly vulnerable. This was followed by Java-based applications. Tools used could not effectively notify the vulnerabilities in the aforementioned language application itself. (Yoo& Shon, 2016) Outline the research challenges that have emerged in the heterogeneous CPS environment based on IED 61850. The study has undertaken the heterogeneous protocol in mind. In addition, work has also presented the security requirements and architectures in the heterogeneous CPS environment. An application programming interface (API) is widely used for interaction with the system, and its vulnerability can be detected by security software (Wilton, Sedat, Irizarry, Borohovski, & Braun, 2018). However, few of them went unnoticed, particularly during the authentication phase, using the third party system. The same was widely discussed by (Wilton, Sedat, Irizarry, Borohovski, & Braun, 2018) to highlight the vulnerabilities.

Network Vulnerabilities

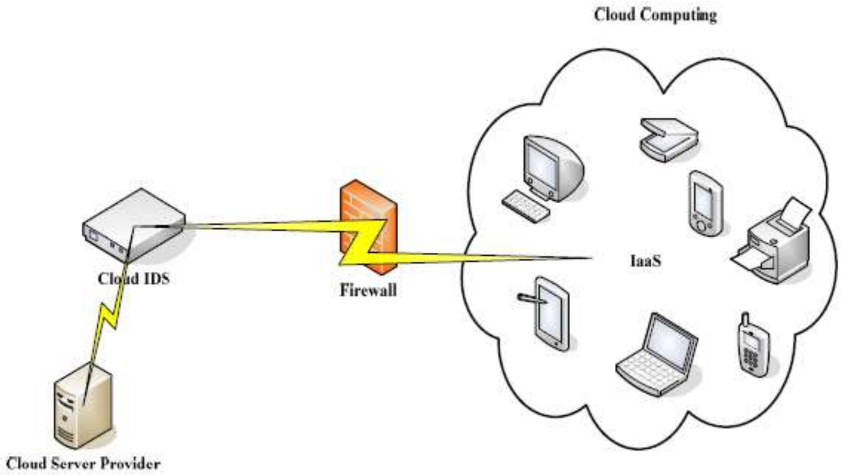
Attack on a host or Network is possible only if vulnerabilities exist. The attacker exploits the vulnerabilities and succeeds in attacking the target. Vulnerabilities are discovered in hardware as well as software, once traced can cause havoc (Criado, Flores, Hernandez-Bermejo, Pello, & Romance, 2005). For instances, vulnerabilities in adobe flash, and adobe acrobat reader has caused several attacks. In a remedial action, Adobe released the patch to fix the vulnerabilities. By that time, it has done great damage. Vulnerabilities can be defined as bug or misconfiguration in a software system that is used by the adversary to attack the Host or network system. Considering the gravity of the threat, CERT is maintaining a dedicated page to notify the latest vulnerabilities and links of the patches that can be used for plugging the vulnerability. Upon deeply understanding the vulnerability trend, it is noticed that vulnerabilities are regularly declining. Developers deserve full praise for introducing the vulnerabilities of free software or with minimum vulnerability. From 2006 onwards it is regularly falling. In 2018, again, more vulnerability had been discovered, particularly at the end of the year, it has already touched the last year figure. Analyzing the monthly pattern, it is revealed that no specific month is widely liked by the attackers to exploit the vulnerabilities; instead, it is spread almost evenly across the year.

MAJOR INTRUSION DETECTION SYSTEM

The intrusion detection tool varies in functionality and the licensing term. Accordingly, a number of IDS exist in the market and enjoy the market share. In this section, we have undertaken the major IDS that prevail in the market.

Need for IDS

Along with ease in services, several new challenges that were not experienced earlier in Network have also surfaced (Garcia-Teodoro, Diaz-Verdejo, Macia-Fernandez, & Vazquez, 2009). For instance, attacks on a network have turn sophisticated from the earlier one. Therefore, we need to safeguards the resources in real-time that have been further intensified. In the initial phase, the principal focus was to safeguard the computer node with anti-virus and firewall. However, they were not enough, and new methods were evolved. IDS is a new sophisticated hardware or software that is used to safeguard the Network. It monitors the traffic and traces for any malicious activities and triggers the corrective action.



IDS Tools

In order to thwart the Intrusion, open-source and proprietary types of tools exist. Proprietary tools are preferred due to their ease of use and strong support from the vendor(s). Open source is preferred due to cost and its flexibility of customization. In the IDS market, open source-based IDS have registered the lead and enjoy a rich market share.

Proprietary

Proprietary software is vendor-specific software and cannot be accessed freely. The proprietary IDS system is to be purchased by the user. Such types of software-based tools are also termed as licensed software. The license is applicable for a fixed period. During the licensed period, up-gradation and advancement are provided free of cost by the vendors. Proprietary software is also appreciated due to its rich support that is spread all the time throughout the year. All timed support pattern is particularly adopted by the company with a multi-nation presence. Cisco Stealth watch enterprise, Kerio control, Darktrace, etc. are the prominent examples of proprietary IDS. Integrating the IDS along with the anti-virus, is the emerging trend.

TYPES OF THE INTRUSION DETECTION SYSTEM

In a network, resources such as nodes can be compromised. Accordingly, IDS are categorized into Network-based IDS or host-based IDS. Each of them has been discussed in the following sub-section. Host based Network based Periphery based

IDs Comparative study

Major intrusion detection software has been analyzed based on the variety of operating systems supported. Beyond, Host based intrusion detection or the Network-based intrusion detection was also taken into account.

CONCLUSION

Vulnerabilities are the major source of attacks and caused by exploiting them at several layers. Among them, application vulnerability is considered sensitive. In addition, insiders are also causing serious damage to the Network and to be controlled at an appropriate level. IDS is a strong measure to mitigate undesired activities in a network. Understanding and selection of IDS are significant for the user's perspective since a rich understanding of IDS will enable users to choose the most appropriate one for them. Accordingly, Intrusion can be mitigated to a great extent both in a network and Host.