Comparative Study on Network Vulnerabilities and Intrusion Detection System

Ajay Kumar & Dr. Saurabh Shrivastava
Research Scholar ,Mewar university, RajasthanBundelkhand University, Jhansi.

Received: September 03, 2018 Accepted: October 30, 2018

ABSTRACT *Intrusion and attack continue to happen in a network by exploiting vulnerabilities.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 the 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 other. Accordingly, this work highlights the vulnerability existing and measure to fortify them. Major IDSs have been explored. Finally, a comparative study in 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.*

Keywords: *Vulnerability, IDS, IDS comparative study, Need of IDS, Vulnerabilities exploitation*

Introduction

With the increasing need of 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 were compromised and had to pay 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 on security (Singh, 2014a; Singh, 2014; Singh & Raghuvanshi). Even mobile based cloud computing is not secure and need to be protected at several levels (Singh, Mathur, & Kumar, 2012).

Attack in 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 appropriate level (Singh, 2014a). Vulnerabilities in application and hardware have been exploited 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 competitive advantage or to damage the network (Benjamin, 2010). Magnitude of damage caused have enhanced in recent times. Even the r**escuers** are unable to recover the network. For instance, encryption of data caused at leading university, hospital and other business venture.

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 same has been exploited by the adversary. Section 4 explores the major IDS and finally this work ended with the comparative study on major IDS in the market.

Related work

Vulnerability detected can be used to put the services downtime or to compromise the data. Financial activities reliance on technology has grown manifold. Owing to the usage, cost of downtime is higher for financial institution. Vulnerabilities correlation with respect to financial institution was carried out by (Roumani, Nwankpa, & Roumani, 2016). Study reveals that vulnerability is correlated to the number of financial records maintained by the financial institution.

Proposed a novel dynamic shell code analyzer named 'shellzer', a shellcode that was a binary file, capable to exploit the vulnerabilities and automation of the task by introducing the tool named Shellzer. Tool was tested on over 24,000 real world samples for the wider acceptance and results generated were 98% accurate. Tool was capable to find out the vulnerability from the deployed network.

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 non-volatile 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), that 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 finding revealed that the software coded in the language 'C' and 'C++' are the 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. Study has undertaken the heterogeneous protocol in mind. In addition, work has also presented the security requirements and architectures in the heterogeneous CPS environment.

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. 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. Attacker exploits the vulnerabilities and succeeds in attacking the target. Vulnerabilities are discovered in hardware as well as software, once traced can caused 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 the 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 threat, CERT is maintaining a dedicated page to notify the latest vulnerabilities and link of the patches that can be used for plugging the vulnerability.

Upon deeply understanding the vulnerability trend, it is noticed that vulnerabilities are declining regularly. Developers deserve full praise for introducing the vulnerabilities free software or with minimum vulnerability. Since, 2006 onwards it is falling regularly. In the 2018, again more vulnerability has 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

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 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, need to safeguards the resources in real time has been further intensified.

In initial phase, the principle focus was to safeguard the computer node with anti-virus and firewall. However, they were not enough and new methods were evolved. IDS are 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.

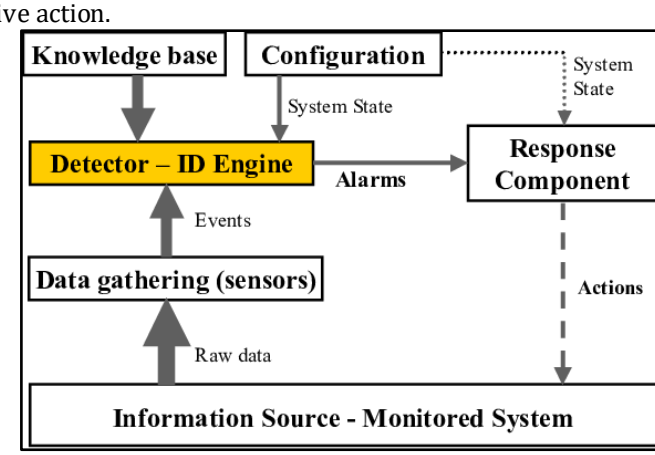

Figure 1: IDS Architecture (Sabahi, Farzad and Movaghar, Ali)

IDS Tools

In order to thwart the intrusion, open source and proprietary type of tools exist. Proprietary tools are preferred due to their ease of use and strong support by the vendor(s). Open source are preferred due to cost and its flexibility of customization. In IDS market, open source based IDS have registered the lead and enjoys rich market share.

Proprietary

Proprietary software is vendor specific software and cannot be accessed freely. Proprietary IDS system is to be purchased by the user. Such types of software based tools are also termed as license software. License is applicable for fixed period. During the licensed period, upgradation and advancement are provided free of cost by the vendors.

Proprietary software is also appreciated due to their rich support that is spread all the time throughout the year. All timed support pattern is particularly adopted by company with multi-nation presence. Cisco Stealthwatch 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 intrusion detection system

In a network, resources such as node can be compromised. Accordingly, IDS are categorized into network based IDS or host based IDS. Each of them has been discussed in 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 system supported. Beyond, Host based intrusion detection or the network based intrusion detection was also taken into account.

Table 1:Major IDS Comparison

IDS	HIDS/NIDS	Unix	Linux	Windows	Mac OS
SolarWinds Log and Event Manager	Both	No	No	Yes	No
Snort	NIDS	Yes	Yes	Yes	No
OSSEC	HIDS	Yes	Yes	Yes	Yes
Suricata	NIDS	Yes	Yes	Yes	Yes
Bro	NIDS	Yes	Yes	No	Yes
Sagan	Both	Yes	Yes	No	Yes
Security Onion	Both	No	Yes	No	No
AIDE	HIDS	Yes	Yes	No	Yes
Open WIPS-NG	NIDS	No	Yes	No	No
Samhain	HIDS	Yes	Yes	No	Yes
Fail2Ban	HIDS	Yes	Yes	No	Yes

Conclusion

Vulnerabilities are the major source of attacks and caused by exploiting them at several layers. Among them, application vulnerability is considerably sensitive. In addition, insiders are also causing high damage to the network and to be controlled at appropriate level. IDS is the strong measure to mitigate the undesired activities in a network. Understanding and selection of IDS is significant for the user's perspective since rich understandingof 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.

Acknowledgement

We are thankful to Dr. Jitendra Singh, for his valuable input and guidance in completion of this research article.

References

1. Benjamin, P. (2010, 8). System for intrusion detection and vulnerability assessment in a computer network using simulation and machine learning. Google Patents.
2. Criado, R., Flores, J., Hern{\'a}ndez-Bermejo, B., Pello, J., & Romance, M. (2005). Effective measurement of network vulnerability under random and intentional attacks. Journal of Mathematical Modelling and Algorithms, 4, 307-316.
3. Garcia-Teodoro, P., Diaz-Verdejo, J., Maci{\'a}-Fern{\'a}ndez, G., & V{\'a}zquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. computers \& security, 28, 18-28.

4. Gleichauf, R. E., Randall, W. A., Teal, D. M., Waddell, S. V., & Ziese, K. J. (2001, 10). Method and system for adaptive network security using network vulnerability assessment. Google Patents.
5. Goseva-Popstojanova, K., & Perhinschi, A. (2015). On the capability of static code analysis to detect security vulnerabilities. Information and Software Technology, 68, 18-33.
6. Kannan, S., Karimi, N., Sinanoglu, O., & Karri, R. (2015). Security vulnerabilities of emerging nonvolatile main memories and countermeasures. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 34, 2-15.
7. Roumani, Y., Nwankpa, J. K., & Roumani, Y. F. (2016). Examining the relationship between firm_s financial records and security vulnerabilities. International Journal of Information Management, 36, 987-994.
8. Singh, J. (2014). Comprehensive solution to mitigate the cyber-attacks in cloud computing. International Journal of Cyber-Security and Digital Forensics, 3, 84-93.
9. Singh, J. (2014). Cyber-attacks in cloud computing: A case study. International Journal of Electronics and Information Engineering, 1, 78-87.
10. Singh, J., & Raghuvanshi, K. (n.d.). Study on the Development of Cloud Security.
11. Singh, J., Mathur, K. S., & Kumar, V. (2012). Enhancing security in mobile cloud computing. Proceedings of M4D 2012 28-29 February 2012 New Delhi, India, 28, 460.
12. Wilton, S., Sedat, B. D., Irizarry, A., Borohovski, M., & Braun, A. K. (2018, 9). Determining Security Vulnerabilities in Application Programming Interfaces. Google Patents.
13. Yoo, H., & Shon, T. (2016). Challenges and research directions for heterogeneous cyber--physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture. Future generation computer systems, 61, 128-136.