IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

Vulnerability Signatures and Log Analysis: A Survey

Poornima .M[1], Ramakrishna M.V[2]

Associate Professor, ISE, SJBIT, Bangalore, India[1]

Professor, ISE, SJBIT, Bangalore, India[2]

Abstract: Computer security has become a major concern of modern technological era and the history of security leads to a better understanding of emergence of security technology. One such field is concerned with protecting computer assets from attackers. Logs contain a huge wealth of information. Logs provides a sight of running system. Vulnerability is a kind of bug used by an attacker .log analysis for system security could be signature based or anomaly based. Both of these signatures are could either be network based or host based. In this paper a survey is done to study the current practices in generation of vulnerability signatures and analysis of logs.

Keywords: Logs, vulnerability signature, anomaly signatures, network based, host based.

I. INTRODUCTION

In computing environment a log file is a file that records every events that occur in an operating system or other software runs, database operations, or messages between different users of communication software. Computer system logs provide a insight into the state of a running system. Log data can be used for various purposes especially in the event of failure, statistical purpose as well as backup and recovery. Log analysis helps in optimizing or debug the system performance**.** Logdata can be used to make predictions and pro-visioning for the future, and another use of log analysis is to make a pro-file of resource utilizations, workload, or user behavior. Logs are also used for security applications like detecting breaches or different behavior, and for performing Depending on the system and the threat model, logs of any kind is susceptible for Security analysis: logs related to firewalls ,login sessions, ,system calls, network flows, and so on. Log analysis for security will be signature based in which user detects specific behavior that are known to be malicious or anomaly based in which the user looks for deviation from specific behavior and flags this as suspicious. Signature methods can detect attacks that matches known signatures. Anomaly methods on the other side faces the difficulty of threshold setting for calling an anomaly suspicious.[1]

Vulnerability is a kind of bug that will be used by an attacker to alter the intended operation of a software program in a malicious way. Vulnerabilities that may lead to the compromise of Sensitive information are being reported continuously [9] where the main reason could be limited programming skill and lack of security awareness. With the advent of the technology there is parallel growth of attackers discovering new vulnerabilities and exploits An exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to the intruder. Vulnerability exists in operating systems, applications or hardware we use. For example, if we do not run antivirus and antimalware software, our laptop or mobile device is vulnerable to infections. Similarly, if you fail to routinely update your operating systems or application software, these will remain vulnerable to software problems that have been identified and patched alternatively.

An exploit is an actual input that triggers vulnerability with malicious intent and devastating consequences. The term exploit is commonly used to describe a software program that has been developed to attack an asset by taking advantage of vulnerability. The objective of many exploits is to gain control over an asset. For example, a successful exploit of database vulnerability can provide an attacker with the means to collect all the records from that database. The successful use of exploits of this kind is called a data breach. Exploits are also developed to attack an operating system or application vulnerability to gain remote administration or "run" privileges on a laptop or server.

One of the popular defense mechanism for exploit is signature based method. These defense systems are in need of new signatures, as new vulnerabilities are explored [2].A vulnerability signature is a representation of vulnerability signature.A vulnerability signature recognizes inputs that exploit Vulnerability.
A security application faces the distinct challenge of an adversary. To avoid the notice of a log analysis tool an adversary tries to behave in such a way that the logs generated during the attack looks exactly same as log generated during correct operation. The survey papers discussed here is categorized into three areas of study that is log, generation of vulnerability signature and analysis of vulnerability signature.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

II. OVERVIEW OF LOG AND VULNERABILITY SIGNATURE

A LOG

As stated earlier In computing a log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software. Logging is the act of maintaining a log and the messages are written into this log file.

A transaction log is a file of the communication between a system and the users of that system, or a data collection method that automatically captures the type, content, or time of transactions made by a person from a terminal with that system. For Web searching, a transaction log is an electronic record of interactions that have occurred during a searching episode between a Web search engine and users searching for information on that Web search engine. Many operating systems, software frameworks, and programs include a logging system. A widely used logging standard is syslog Ding Yuan et.al has presented a tool called Log enhancer to enhance log message in software to collect causally related diagnostic information .diagnosing software failures is difficult due to the complexity of Trouble shooting any complex software system .it is common that only the runtime log that is syslog generated by a system can be shared, but the adhoc nature of this report is insufficient for detailed failure diagnosis. This tool automatically enhances existing log code to aid in future post failure debugging [6]

B generation of vulnerability signature

A patch is a software which is designed to update a computer program or its supporting data to fix or improve it, which includes fixing security vulnerabilities bugs, generally people are disinclined towards applying patch immediately against a attack because patches are usually not reliable.

Shield has proposed a framework for manually creating vulnerability signatures by modeling network protocols, and the overall advantage of analysis is the generated signature is guaranteed to be faithful to the vulnerability as it appears in the program[3]

DavidBrumley, et.al has presented a framework for generating vulnerability signatures, given a sample exploit they have proposed a technique for automatically generating a signature and their formulation works for vulnerabilities that can be exploited by multiple paths[2].

Almorsy et. al. have proposed an approach where instead of depending on some formal methods to locate vulnerability instances where the analyzers has to be developed for locating specific vulnerabilities, their approach uses a formal vulnerability signature described using object constraint language(OCL) .using this formal signature they have performed program analysis of the target system to locate signature matches..a newly discovered vulnerability can be easily identified in a target program provided a formal signature for it exists[5].

COVERS: an automated signature generation method was introduced to give protection against large scale repetitive attacks. Covers utilizes the fact that all memory error exploit involves corruption of pointer values, and this value must be included in the error input. It uses forensic analysis of victim's server's memory to correlate attacks of the input received over the networks. This approach is context based vulnerability oriented. The signature generated by covers looks for vulnerability characteristics.

C Analysis of vulnerability signature

KarenA.Garcia et.al has introduced the postmortem intrusion detection problem, which consists on pinpointing the execution Of an exploit, If any, for a given log file. Postmortem intrusion detection is valuable for postmortem of computers because it speeds up the process of gathering evidence of intrusion detection, and also it speeds up the process of building an attack signature. An attack signature is very valuable for IDS construction. They have reduced the burden of analyzing a system call log file by means of factoring out repetition[4].Central to the intrusion detection mechanism is a classifier which separates abnormal behavior from normal one. This classifier is built upon a method that combines a hidden markov model [7] with K-means technique.

Wang Nan et.al has proposed a novel anomaly detection algorithm by comparing the incrementation of compressed data length based on grammar-based compression, in this paper they measure the strangeness of sequences in anomaly detection. This method utilizes the full knowledge about the structure of the data set. It can be used to find high level misbehavior as well as low level intrusions. They have used the algorithm on finding bugs in fine grained execution logs and intrusion detection in system call traces.

III. CONCLUSION

With the advent of computing systems and their usage within most organization network and system administrators have been responsible for performing log analysis. as per the survey done some of the issues found are log analysis is often considered as reactive-something which is to be done after a problem has been identified through some means

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 5, May 2017

rather than proactive, to identify ongoing activity and look for signs of problems. secondly there is a vulnerability database that describes vulnerability found, but does not describe the behavior of the applications when being attacked so there is a scope to correlate the vulnerability database and the behavior.

REFERENCES

[1] Adam oliner, Archana ganapathi,and wei XU "Advances and challenges in Log Analysis" February2012|vol. 55|no. 2|communicationsoftheacm
[2] DavidBrumley,JamesNewsome,DawnSong,HaoWang,andSomeshJha,"Theory and Techniques for Automate Generation of VulnerabilityBasedSignatures"IEEETRANSACTIONSONDEPENDABLEANDSECURECOMPUTING,VOL.5,NO.4,OCTOBER-DECEMBER2008
[3] H.J. Wang, C .Guo, D. Simon, and A. Zugenmaier, " Shield : Vulnerability-Driven Network Filters for preventing KnownVulnerability Exploits, "Proc.ACMSIGCOMM '04,Aug.2004
[4] KarenA.García, RaúlMonroy, LuisA.Trejo, Carlos Mex-Perera, and Eduardo Aguirre "Analyzing log files for postmortem intrusion detection" IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 42, NO. 6, NOVEMBER 2012
[5] MohamedAlmorsy,John Grundy,andAmani S. Ibrahim, "supporting automated vulnerability analysis using formalized vulnerability signatures", ASE, September 2012, Essen, Germany.
[6] DingYuan JingZheng SoyeonPark YuanyuanZhou Stefan Savage, "Improving Software Diagnosability via Log Enhancement", ASPLOS' 11 March2011,NewportBeach,California,USA.
[7] L-R Rabiner, a tutorial on hidden Markov models and selected applications in speech recognition, Proc,IEEE,vol 77,no.2,pp.257-286,feb 1989
[8] Z Liang and R Sekar," Fast and Automated generation of attack signatures: a basis for building self protecting servers", Proc ACM,CCS(2005) pp 213-222.
[9] Kirti randhe, "Security Engine for prevention of SQL Injection and CSS Attacks using Data Sanitization Technique", IJIRCCE, 2015.
[10] N. Wang, J. Han, and J. Fang, "Anomaly sequences detection from logs based on compression," Comput. Res. Repository, vol. abs/1109.1729, pp.1–7, 2011