Identification of Zero Day Vulnerabilities and Its Techniques Used to Protect System

Gajanan P Bherde, Dr. M.A.Pund

Department of Computer Science & Engineering, PRMIT&R, Badnera, Amravati, India.

pundmukesh@gmail.com

Abstract- Little is known about the duration and prevalence of zero-day attacks, which exploit vulnerabilities that have not been publicly revealed. Knowledge of new vulnerabilities gives cyber criminals a free pass to attack any target of their choice while remaining undetected. Unfortunately, these serious threats are difficult for dev, because, in general, the data are not available until after an attack is discovered. In addition, zero-day attacks are rare events that are unlikely to be observed in honey pots or laboratory experiments. In this paper we described the zero day attack methods for identifying the attacks and how to kill these identified attacks. Finally we show that our proposed system is more accurate and efficient than existing system.

Keywords: Zero day attack, vulnerabilities

I. INTRODUCTION

In today's network systems, organizations are very careful to protect their networks, but even if they have a responsible and sustained investment in defense, they are still not listed in the list of security vulnerabilities for a bypassing organization. In a well-guarded Network, a loophole can be revealed by a persistent investigation of a determined hacker. An attacker could use vulnerability in network configuration to infiltrate a target network. In addition to known vulnerabilities, an attacker can find zero-day through hours, weeks or months of struggling effort through lines of code, and find some weaknesses flaws that systematically oppress the target application, which even developers have not noticed. An attacker's ability to attack on network, cracks the network and to access them secretly. This is how the network is breached by zero-day. Zero-day is a previously unknown, unpatched vulnerability that can be exploited by threat actors to gain entry into a target's network; Cyber criminals exploit zero-day vulnerabilities to increase the success rate of finding attacks. In most cases, information about the vulnerability would not be available until the attack has already taken place.

As a result, attacks using zero-day attacks are difficult to identify and analyze. In the hands of zero-day vulnerabilities, hackers are helping software vendors by providing information about the vulnerabilities that have been discovered, or invented, zero-day exploits have had elements that hadn't previously been revealed; such vulnerabilities are known as zero day vulnerabilities. Attackers incorporate zero-day exploits into their chart lists of vulnerabilities, and once the process and payload of the intrusion program are concocted, the attack can be terminated. There is no protection against zero-day, when in fact the attack was first observed. The traditional security approach finds vulnerabilities by generating a signature, but in the case of zero-day, this information is unknown, so the vulnerability is not disclosed, since the attacker is highly skilled in the conventional defense. It provides a lot of time to the attacker to cause irreparable harm, and for several months or years. According to FireEye, a typical zero-day attack can last an average of 310 days. Therefore, dealing with zero-day is obviously a difficult task.

In this paper, we are working on Zero-Day attack detection technology, "Zero-Day attack" refers to the software Hole unknown vendor of the software. In this security researchers are not able to correct the Zero-Day attack in the system. In this system, two methods are used to detect zero-day attacks. One is signature based and second is knowledge based detection technique. Building a knowledge based strategy system allows you to use ontology technology. The ontology helps build a strategy-based knowledge attack database. The new hybrid attack detection engine brings together the main advantages of the classic approach of knowledge-based and signature-based.

II. LITERATURE REVIEW

In the current state of the global situation, the market is a zero-day exploit where researchers, national, industrial, academic, and criminal elements develop and buy and sell these goods, whether they develop zero day or purchase. They are the state of the country, generally stockpiling them for the future. It may then be used for purposes such as spying, aggressive cyber manipulation, and deterrent effects. But the immediate effect of this stockpile is that it is not exploited. Leaking to the public and therefore not being treated. In a world increasingly networked and code-dependent, this creates the possibility of cyber-disaster with

 DOI : 10.35291/2454-9150.2019.0192

yet unimaginable impact on global stability. Therefore, it is imperative for the state to divulge, responsibly, the exploit of zero-day, through an international framework for global benefits moving from the present. It's not going to be easy for a responsible release of a zero-day attack to be the standard. There are many stakeholders who claim that maintaining stockpiles is beneficial or this is an area that is not feasible to regulate. However, it is possible to develop the international regime, as we have seen with weapons, chemical and biological weapons and other weapons. It prohibits the use of such weapons for their extraordinary ability and impact. Or, if these exploits are deemed equally harmful to the infectious disease, if the countries have established a taboo on the use of zero-day exploits to form a similar organization to who that can deal with international cyber issues, i.e., we believe that the use of them is morally, unlawful, unethical, and unethical [1].

Data exchange between different parts of the Universe is carried out by means of computer networks and the corporate information system (EIS) based on them. Privacy and security are the most important factor that should be maintained in any network systems. This paper discusses the detection of an intrusion attack on the eclipse database using the Ensemble fuzzy association (EFA) and CFA (CFA) algorithm. The proposed methodology creates a rules-based ensemble a model for modeling network diversity metrics to effectively detect zero day attacks and reduce time-consuming. Simulation results show that EFA and CFA have effective detection rates compared to existing systems [2].

Of all the dangers facing corporate IT systems, today's vulnerabilities are the most damaging. Zero-day vulnerabilities can be patched before network attacks are exposed to the correct user. Exploits are not patched every day, and the risk of data breaches increases dramatically. Only a multilayered approach that is fully integrated with the organization's IT defense is a chance to stop them. The author in this paper developed a new hybrid three-layer architecture framework for Zero-Day attack detection and risk-level assessment. The first layer of the proposed framework makes it easy to detect unknown vulnerabilities based on techniques based on statistical, signature and behavior, the second layer focuses on risk measurement, and the third layer includes a centralized database and a centralized server used during the processing of the first layer. The proposed framework is analyzed at the University Of Biklam Ujjain India's Network Environment to evaluate the performance [3].

To compare the vulnerability detection rates of different scanners, it is important to have a separate test suite. This section describes the web applications that are used to evaluate the efficiency of Netsparker and Acunetix web application. The results of this application Web application assessment identify the most difficult vulnerabilities that scanners detect and compare the effectiveness of scanners. The evaluation results can be suggested in areas that require further research to improve the scanner's detection rate [4].

Today's highly skilled attackers are vulnerable to many network applications. On the other hand, the risk of data breaches is rapidly increasing, and the software or application is vulnerable and patched. Its vulnerability (Fri-Sun), hackers put on the target network and steal confidential data. Since the signature information of the Zero-Day attack is unknown, it is difficult to detect zero-day using conventional defenses. Therefore, a new security solution is needed to detect zero-day exploits and to estimate the severity of the zero-day vulnerabilities identified. In our previous work, in this paper the author proposed a approach for the discovery of unknown vulnerabilities. By presenting a framework for configuring an integrated approach to detection and prioritization of zero day attacks, they will enhance previous acknowledgment. The proposed framework follows a probabilistic approach for the identification of Zero-Day attack vectors and ranks the severity of the identified zero-day vulnerabilities. It is a hybrid discovery-based technology that detects unknown defects in networks that have not yet been detected. In order to evaluate the performance of the proposed framework, it was adopted in the network environment of the Vincram University campus in India [5].

A zero-day attack is a cyber attack that exploits an unregistered vulnerability. Zero-Day attack is a very expensive and powerful attack tool. They are used in conjunction with very sophisticated targeted attacks to achieve stealth against standard intrusion detection methods. Zero-day attacks are unknown and difficult to detect because they have no sign. This article describes a new and effective method for detecting zero-day attacks. The proposed technology detects the second-level evaluation and obfuscation of a zero-day attack, automatically generates a signature for a new attack, and uses the global patch feature [6].

Paper analyzed the detection of Zero-Day attack. The fundamental limits of the existing approach are the signature generation of unknown activities and the false alarm rate of anomalous behavior. To overcome these problems, they propose a new approach for analysis and detection of zero-day attacks. They also propose an approach based on machine learning to detect networks with a framework of zero-day attacks to identify abnormal behavior in the presence of networks. The proposed framework uses a supervised classification scheme for the evaluation of known classes with the adaptability of supervised classification to detect new dimensions of classification [7].

This community, in light of the growing trend of security issues, addresses the introduction of vulnerabilities as a way

 DOI : 10.35291/2454-9150.2019.0192

of realizing security issues. Although many efforts are currently underway to codify the practice of SSE for overall security spending, the handling of economic considerations has not yet taken place. In this paper, the author proposes an initial model to capture the SSE investment as a means to reduce the uncertainty of the defender about the vulnerability. This approach is instantiated as an accompanying process to the traditional security model, and the result of the system's life cycle is an increase in security investments, or an increase in security software processes (ROSSP). This model allows for a more comprehensive handling of security investments that integrate pre-security and post-security investments, and reduces the cost of software investments [8].

Zero day vulnerabilities, unknown exploits and divulges safety flaws such as software prior to publication. But how should a nation react to zero day? This question is of concern to the governments of most countries and requires a systematic approach to its solution. The security of the country or the state's critical infrastructure is being compromised by Solidarity cyber criminals. The disruption and avoidance of national intelligence activities and the possibility of critical network security are increasing. Most of these breaches are possible with detectable operational bypasses that are ignored by security administrators. One instance can be detected bypassing the operational responsibility of the regular security updates available from software and hardware vendors. All software is not necessarily the final state, but to control the security of critical national assets by patching vulnerable systems by applying regular updates, the state can detect vulnerabilities and prevent cyber attacks and espionage appropriate for the hunt, this is the first step in this process. This paper discusses the consequences of the zero-day exploits and highlights the dangers posed by this ulcer for unprepared countries [9].

A zero-day attack is a type of attack where people use a lack of software developed by different companies. There is no patch, so it's hard to deal with these types of attacks even when the company's developers are known for it. For any network, such attacks can only be possible a way to get through it to prevent such types of attacks. If the network administrator knows how many such attacks are possible, he can make some changes to his administrator rights. It is established that in day there are more than five thousand vulnerabilities. We propose an entirely new scenario that could lead to a very effective consideration of such vulnerability. Using this method, we can easily provide an opportunity to strengthen the network to prevent its unknown vulnerability [10].

This paper presents an efficient technique for detecting a Zero day polymorphic worm with almost no false positives. The zero-day polymorphic worm not only exploits unknown vulnerabilities, but also changes its own expression for each new infection and uses different keys for each infection payload, so there are many variations of the signature of the same worm and fingerprinting is very difficult. Its ability to rapidly breed and these worms are increasingly serving the internet management process, which poses a threat. If these zero day worms are detected at the right time and are not included, they potentially disable the internet or lead to serious disruption [11].

The author conducted an empirical study on the use of data mining methods on NVD data in order to predict the time to the next vulnerability for this software application. We experimented with various functions built using the information available in NVD and applied various machine learning algorithms to study the predictive power of the data. Our results show that the data in NVD usually have poor forecasting capability, with the exception of a few vendors and software applications. We suggest possible reasons why NVD data did not create a reasonable time-to-next vulnerability prediction model with our current approach, and suggest alternative ways to use the data in NVD for risk assessment [12].

III. PROPOSED SYSTEM

A. Proposes system

Fig 1 shows the proposed system architecture.

In the system architecture, read the XML file and move it to the signature-based method. The database ontology includes all known attacks on the signature format. And the owl file attacker adds the attack. An attacker is a security threat that attempts to delete, destroy, and modify information without any permission or access. The contents of the input file are converted to the signature format. Next, we compare the content signature format with the stored attacks in ontology's. If the signature matches the attack, the attack is detected. Otherwise, no attack is detected. Signature-based methods cannot detect new attacks. Knowledge-based detection system detects new attacks and is stored in the database.

In the system architecture, read the XML file and move it to the signature-based method. The all known attacks on signature format includes into database ontology's. An attacker of the owl file can then exploit the vulnerability. An attacker is a security threat that attempts to delete, destroy, and modify information without any permission or access. The contents of the input file are converted to the signature format. Next, the content signature format is compared with the attack stored in ontology. If the signature matches the attack, the attack is detected. Then the detected attack is killed using firewall. Otherwise, no attack is detected. Signature-based techniques cannot detect new attacks. New attacks that detect knowledge base detection systems are stored in the database.

 DOI : 10.35291/2454-9150.2019.0192

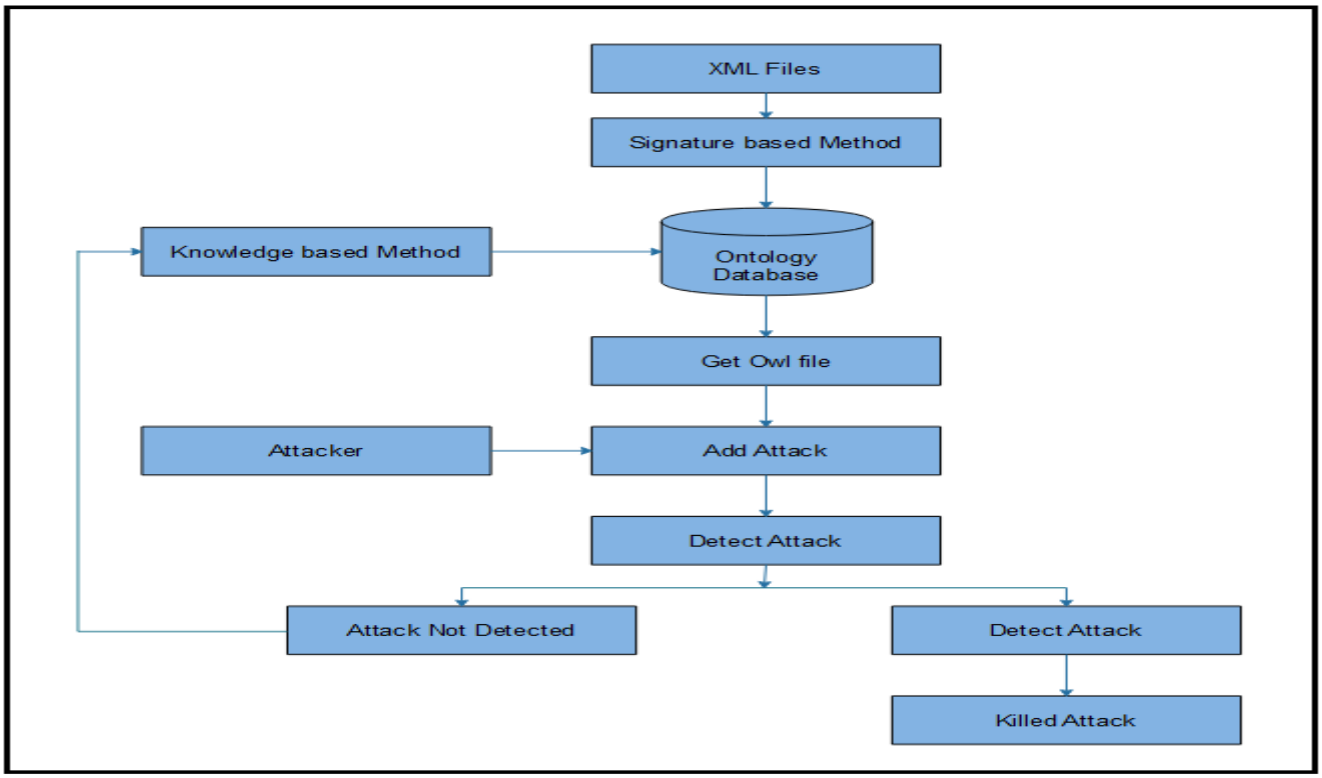

Fig 1: System Architecture

IV. RESULT AND DISCUSSION

Here, the experiment was carried out in order to confirm the accuracy and efficiency of the proposed method. We have to use XML file as a dataset. The performance and accuracy of the system is evaluated by using True Positive Rate (TPR), False Positive Rate (FPR) and Receiver Operating Characteristics (ROC) Curve parameters. Figure 2 and Figure 3 represents the Performance and accuracy of the proposed system.

Polymorphic engines Admmutate, clet, Alpha2, CountDown, JumpCallAdditive and Pex were applied to unencrypted exploits. To evaluate the performance and accuracy of the proposed framework, true positive rate (TPR), false positive rate (FPR) and receiver operating characteristic (ROC) curve parameters are used. As shown in figure 2 and figure 3 represents the true detection rate and the false positive rate of Zero-Day attack accordingly.

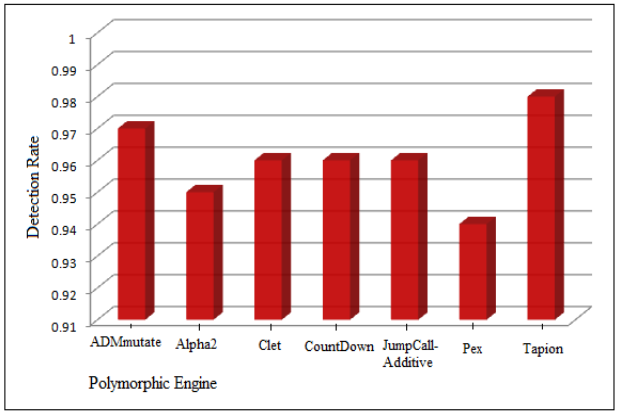

Fig 2: True Positive Rate

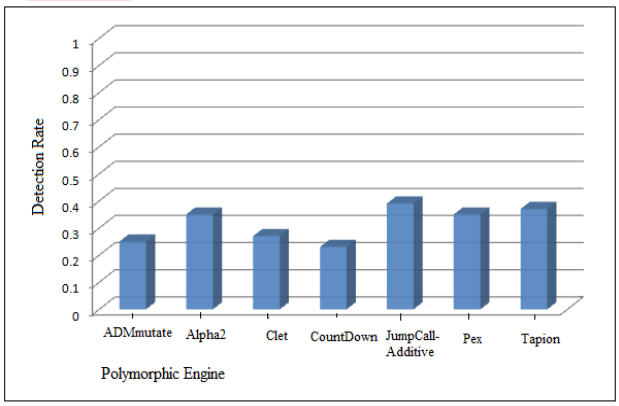

Fig 3: False Positive Rate

Figure 4 show that the Receiver Operating Characteristics (ROC) Curve, its drawn by used to taking the average value of TPR. Figure shows that ROC is closer to 1, this prove the efficiency of proposed system.

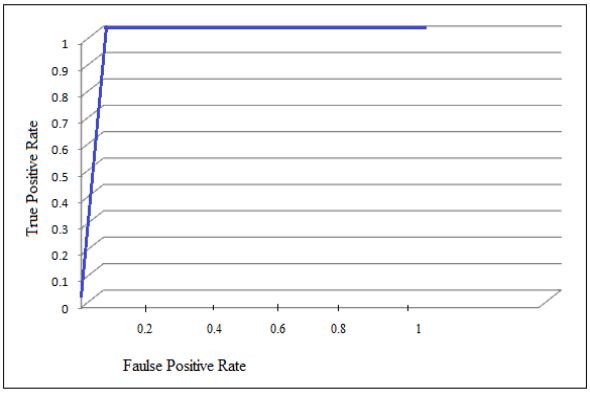

Fig 4: Average value of ROC curve

 DOI : 10.35291/2454-9150.2019.0192

V. CONCLUSION

For the purpose of the detection system, the Web service administrator examined the informative messages for the investigation, and in this study the proposed approach did not generate false positives during detection, the system for attack detection and identification was designed using the method of signature base and knowledge base. This system is a combination of a signature-based system and a knowledge-based system. To prevent this detection and attack, ontology is used and killed these detected attacks by using firewall. Finally we show that our proposed system detection rate is 98 % and false detection rate is 0.3%. The proposed system is more accurate and efficient than existing system.

REFERANCES

[1] Paul Maxwell, "Stockpiling Zero-Day Exploits: The Next International Weapons Taboo", Research gate, Feb 2017.

[2] M. Masthan1 and R. Ravi, "Prevention of zero day vulnerability in network using ensemble fuzzy association and cuttle fish detection", IJCT june 2017.

[3] Umesh Kumar Singh, and Chanchala Joshi, "Scalable Approach Towards Discovery of Unknown Vulnerabilities", IJONS Sept. 2018.

[4] C. Joshi, and U. K Singh, "Performance Evaluation of Web Application Security Scanners for More Effective Defense", IJSRP, June 2016

[5] Chancha;a joshi and Umesh kumar singh, "An Enhanced Framework for Identification and Risks Assessment of Zero-Day Vulnerabilities", IJAER July 2018

[6] Kaur, R.; Singh, M., "Automatic Evaluation and Signature Generation Technique for Thwarting Zero-Day Attacks", March 2014.

[7] Chanchala Joshi, and Umesh Kumar Singh, Suyash Kumar Singh, "Zero day Attacks Defense Technique for Protecting System against Unknown Vulnerabilities", Volume-5, Issue-1, pp.13-18, February (2017)

[8] Chad Heitzenrater, Rainer Bohme and Andrew Simpson, "The Days Before Zero Day: Investment Models for Secure Software Engineering", Distribution Unlimited: 88ABW-2016

[9] A. E. Ibor, "Zero day exploits and national readiness for cyber-warfare", (NIJOTECH) Oct 2017

[10] Harshpal R Gosavi and Anant M Bagade, "A Review on Zero Day Attack Safety Using Different Scenarios", European Journal of Advances in Engineering and Technology, 2015

[11] Kaur, R.; Singh, M., "Efficient hybrid technique for detecting zero-day polymorphic worms," Advance Computing Conference (IACC), 2014 IEEE

[12] Xinming Ou Su Zhang, and Doina Caragea, "Predicting Cyber Risks through National Vulnerability Database", ISJ 2015

 DOI : 10.35291/2454-9150.2019.0192