OPEN ACCESS INTERNATIONAL JOURNAL OF SCIENCE & ENGINEERING

PROTECT SYSTEM USING DEFENSE TECHNIQUES OF ZERO DAY ATTACKS

Gajanan P Bherde[1], Dr. M.A.Pund[2]

Department of Computer Science & Engineering, PRMIT&R Badnera, Amravati, India[1,2]

pundmukesh@gmail.com

Abstract: **Every organization connected to the internet is a common threat of zero-day attacks. Zero-day attacks will not be noticed until a specific vulnerability is actually identified and reported. Zero day offensive difficult to defend, mainly to be completed without being detected. Zero day attacks from protected network applications and systems are a difficult challenge for organizations to name security. The study on detection of zero-day attacks was analyzed. 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, we propose a new approach for analysis and detection of zero-day attacks.**

I INTRODUCTION

Over the past few years, due to the rapid spread of network services, digital protection of the computing environment has become the biggest challenge. An incredible flood of new devices is challenging the traditional way to secure a network of organizations. Major software releases introduce important new features very often that lead to unexpected vulnerabilities. Therefore, determining the number of known vulnerabilities present in a system alone is not enough to measure the security level of an entire network. To ensure that the network system is connected to a known vulnerability, it is necessary to have a firewall or IDSs. Due to the secure network configuration, the value is scarce and vulnerable to zero-day attacks. Zero-day attacks pose a serious threat to your organization's network because they can exploit an unknown vulnerability. An unknown vulnerability can cause harm at any level of security of the system because the patch is not available. Moreover, the security risk level of unknown vulnerabilities is difficult to measure due to their predictable nature. According to Symantec's internet threat report in 2016, targeted attacks from the previous year 125 of 2015 have increased. In addition, new zero-day vulnerability was discovered every week, on average, in 2015. The zero-day vulnerability was reported in 8 zero-day vulnerability 2011 and doubled in 14 zero day vulnerability 2012 and 23 zero-day vulnerability 2013. In 2014, the number was held relatively stable at 24. However, the explosion of zero-day vulnerability in 2015 reaffirms the critical role of Zero-Day attack. 82 zero-day vulnerability was reported in 2016 until May of the month. These estimates include only the vulnerabilities that were eventually reported. Figure 1 shows that the zero-day vulnerabilities from 2011 to 2018.

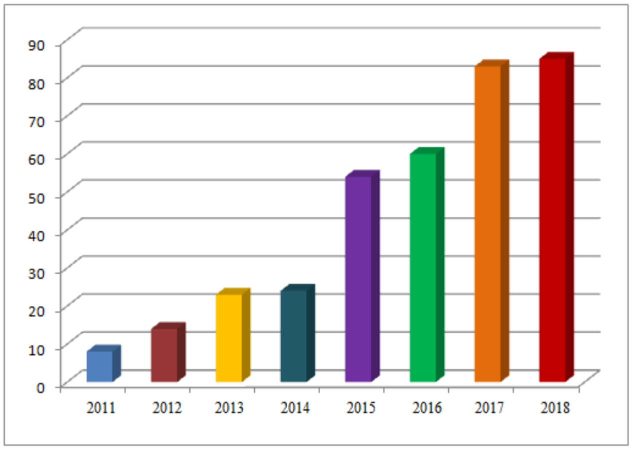

Figure 1: 2011 – 2018 Zero day Vulnerabilities

Zero-day attacks are attacks against unknown system defects and have no patches or fixes. With conventional defenses, it is extremely difficult to detect zero-day attacks. Attackers are very skilled and their malware can cause irreparable harm without being detected on the system for months or years, so dealing with unknown vulnerabilities is obviously a difficult task. It is obviously difficult to discover and exploit many effective unknown solutions such as IDS/IPS, firewalls, anti-virus, software upgrades and patching to tackle known attacks.

Zero-day vulnerabilities are the most harmful of all the dangers facing the computing environment of an organization. They exposed the flaws of the system to attackers before the patches were available. When the zero-day vulnerability is unknown, the software vendor will not know about the flaw. According to FireEye report, vulnerabilities discovered by cybercriminals are not generally known for an average of 310 days, including software vendors.

In this paper we implement the system for detecting the attack the technique implements: Signature based detection and Knowledge based detection system. If the Signature based method fails to detect the new attacks. Knowledge based detection system detect the new attacks and stored in the ontology database.

II LITERATURE REVIEW

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 [1].

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 [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].

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 [4].

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 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 [5].

This community, in light of the growing trend of security issues, addresses the introduction of vulnerabilities as a way 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 [6].

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 [7].

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 [8].

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 [9].

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 [10].

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 [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 2 shows the proposed system architecture.

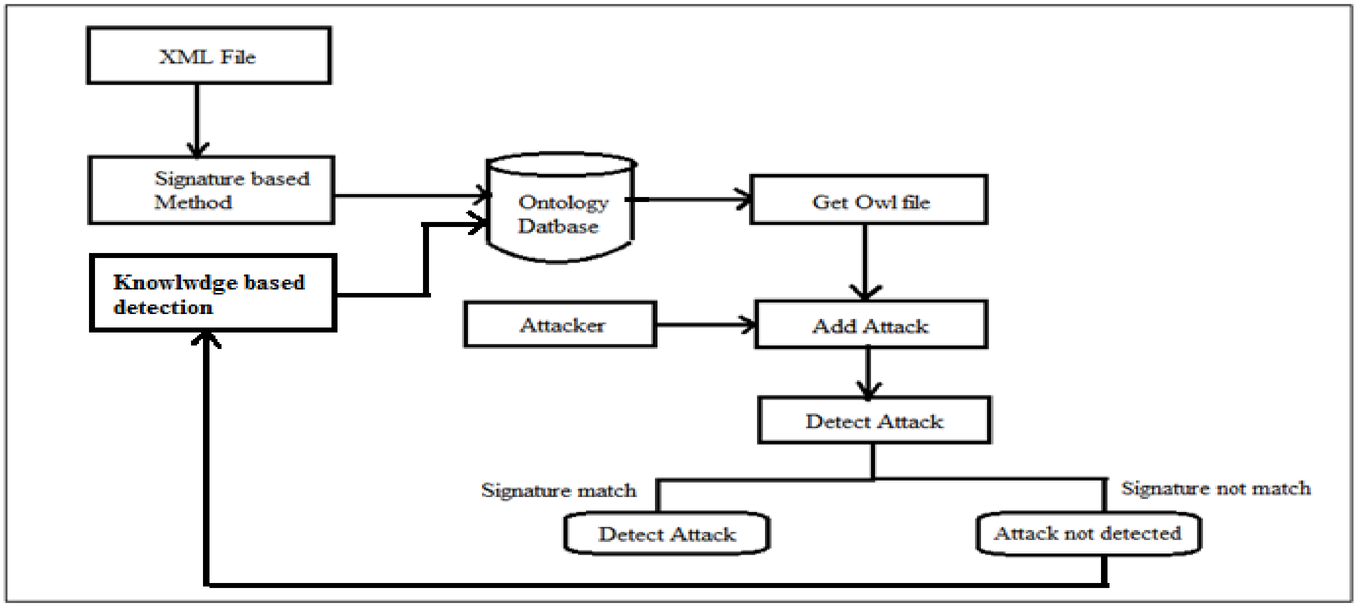

Figure 2: Proposed system Architecture

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.

- Signature Based Detection:
  The signature-based process is primarily a base system in that it is simple and can be operated online in real time. How to use signature detection to attack a specific signature that you have with an expert. Signature based detection system usually leads to low software detection miss rate, i.e. false positive rate. However, an important limitation of signature-based attack detection is that it does not detect new and unknown attacks, even if there are only minor variations from known payloads.
- Knowledge based detection:
  Another way to protect Web Services from injection attacks is to apply protection based on some kind of previously known and cataloged behavior knowledge base against normal behavior includes all expected actions that define such a profile, including normal and not considered knowledge attacks. This type of attack detection system is capable of detecting the

suspicious behavior of the user, knowing the information about the vulnerability of the system and the description of previous attacks. Normal behavior is defined as the user's profile; another class includes the abnormal behavior of the attacker. If a new attack is found, it is added to the ontology.

IV. RESULT AND DISCUSSION

A. Experimental Setup

The system is built using Java framework on Windows platform. The Net bean IDE is used as a development tool. The system doesn’t require any specific hardware to run; any standard machine is capable of running the application.

B. Experimental Results

Figure 3 shows that the Attack detection times graph. Figure shows that the Existing system Strategy-based ontology detection (SPARQL) started with 170 percent slower detection time than proposed system. Finally we conclude that the proposed system require less time to detect the attacks than existing system.

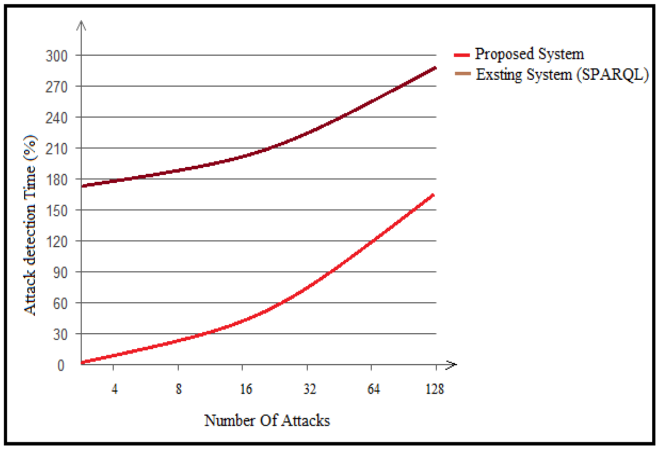

Figure 3: Attack detection Time graph

V. CONCLUSION

Most organizations have vulnerabilities that are the most attractive to attackers and are widely used in software. Most of these vulnerabilities are found in software such as Internet Explorer and Adobe Flash, and are frequently used by many consumers and experts. After discovery, zero-day attacks are immediately added to the attacker's toolkit and exploited. In this paper, proposed an approach for analysis and detection of zero-day attacks. The proposed approach solves the supervised learning techniques and identifies the streams of known and unknown attacks with very high accuracy. The proposed method is more effective and efficient in detecting zero day attacks than the typical statistical-based anomaly detection method.

REFERENCES

[1] 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)

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

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

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

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

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

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

[8] 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

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

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

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

[12] Xinming Ou Su Zhang, and Doina Caragea, “Predicting Cyber Risks through National Vulnerability Database”,ISJ2015.