Hybrid System Between Anomaly Based Detection System and Honeypot to Detect Zero Day Attack

Nisreen Innab
Department of Information Security
Naif Arab University for Security Science
Riyadh, Saudi Arabia
nisreen.innab@nauss.edu.sa

Eman Alomairy
Department of Information Security
Naif Arab University for Security Science
Riyadh, Saudi Arabia
eman.omairy@nauss.edu.sa

Lamya Alsheddi
Department of Information Security
Naif Arab University for Security Science
Riyadh, Saudi Arabia
4370885@nauss.edu.sa

Abstract—Honeypots are systems designed to lure the potential attacker to a real system by make him busy with emulated system. Its primary objective is gathering information about the attacker as possible to avoid any future similar attacks. Another method for protecting the systems against attacks is anomaly based detection system, where its main goal is to monitor the traffic to detect any known worm behavior based on the previous knowledge of the environment. In this paper, we will mention some techniques to avoid Zero day attacks. Then we will analyze the strengths and weakness of both approaches that are honeypot and anomaly based detection. As a result, to integrate both approaches in one hybrid model as enhanced solution of detecting the Zero day attack that may occur in the system.

Keywords- Zero-Day attack*; *SWORD*; *cascading style sheet (CSS)*; *anomaly-based detection*; *honeypot*; *malware.

I. INTRODUCTION

Malwares are depends on the self-duplication such as worms exploit the time of not knowing that there is an attack, or not realizing by intrusion systems [1]. This exploiting of vulnerabilities in the system also called Zero-day attack, which described as threat of unknown weaknesses in the computer software or application where either the patch of the vulnerability has not been applied or the security team not aware of it yet as shown in figure 1 [2].

There are common approaches to detect unusual activities in the system and ensure the confidentiality, integrity, and availability of the information in either network or host levels. In network level a firewall, network Intrusion Detection Systems (NIDSs), and anti-spyware software are used to monitor the network packets flow.

Zero-day attacks are dangerous and threaten all users of these infected systems. While its very useful to hackers in many ways to make money. These detectors can play fictional profits from these gaps in several different ways such as selling these gaps for developers of these systems or their owners, sell these gaps across sites "black markets", sell these gaps for spyware companies and Governments, and exploited by the hacker.

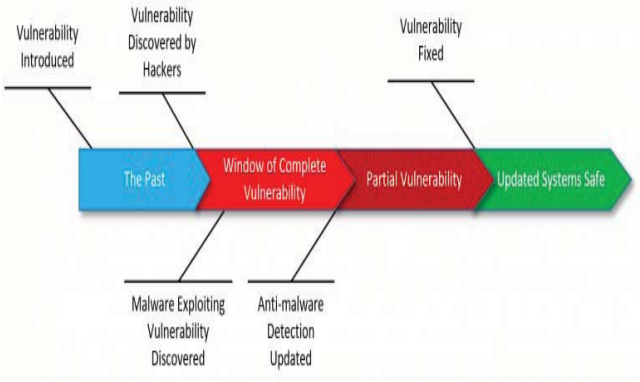

Figure 1. Zero –Day Vunerability Timeline

978-1-5386-4110-1/18/$31.00 ©2018 IEEE

II. UNKNOWN VULNERABILITY ATTACK

A Zero-day attack is an attack for a vulnerability that is unknown to the public community [4]. Different mechanisms are submitted to detect the Zero day attack; one of these mechanisms is intrusion detection systems (IDS), in particular network based intrusion detection systems (NIDS).
This also categorized as:
1- Anomaly based (ANIDS): which estimates the normal behavior of the system and make alarm when abnormal behavior occurs.
2- Signature based (SNIDS): which analyze data to find patterns, if these patterns matched with previous known malware, the alarm will triggered.
The problem is that Zero day attack cannot be detected with Signature based (SNIDS) because it is detect attacks that match with known signatures while the Zero day attack deals is an unknown vulnerability attack [5].
A related methodology with signature-based identification is supervised classification, which utilization instances of known malware on manufacture. An order model that recognizes the known dangers from other projects. Managed arrangement methodologies also specification those same constraint as signature-based detection in that they both perform poorly on new and evolving malware. In addition, if we have a classification model it is a challenge to different malware classes [6].

II. ZERO DAY ATTACK DETECTION MECHANISMS

Many researches and studies concerns the detecting Zero day attacks regardless of the type of attack. Zero day frequently is harmful for systems; therefore, here are some mechanisms to detect the unknown attacks (Zero-day).

A. Enhanced SWORD System

While the internet is rapidly developed, new vulnerabilities also are established. This growth makes vulnerabilities and the worms exploiting it unknown titled as Zero day attack. This problem leads the developers to design, develop, and evaluate an essential behavior-based worm detection framework called Self- Propagating Worm Observation and Rapid Detection (SWORD) [7].

Figure 2 shows the component of the SWORD are: 1- Casual similarity identification: it defines the connection similarity to pervious connection. 2- Destination address distribution analysis: it defines the current destination pattern is not like the normal pattern. 3- Continuity analysis: method to analyze current patterns of worm connections. 4- Infected host detection: it defines what server is infected. 5- Behavior based worm classification: identify the type of worm based on its behavior [7].

Since the detection of the infected servers from Zero day attack should be accurate and fast, SWORD is enhanced form of detecting the Zero day attack from administrative domain to operate at host level without requiring intrusive monitoring systems installed on end-hosts. It is not necessary to be at individual host itself but in the gateway point of the network. [8]

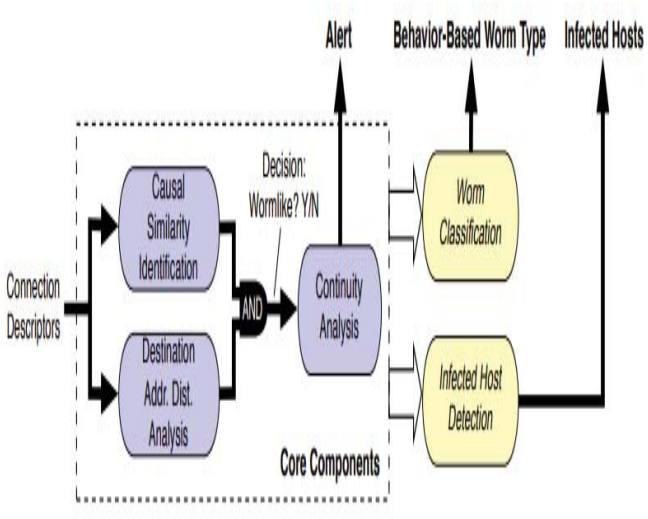

Figure 2. The architecture of SWORD

B. cascading style sheet (CSS)

The phishing websites is a hacker's fake websites, which look like a legitimate website, that the attacker use it to trick the user to obtain sensitive information. Some phishing websites identified as malicious site that exploit browser vulnerabilities to install malicious codes [9, 10].
One of the methods to detect the known phishing websites is black list. The problem with this method is the time delay between detection of the phishing website and adds it to the black list. Therefore, we should use Cascading Style Sheets (CSS) detection algorithms to detect unknown phishing websites [11].
CSS provides a unique signature for the websites because it contains all information about web page such as font, colors, layout, spacing, and any information about how the website looks in the browser as shown in figure 3. The attacker may exploit the CSS for a legitimate website in order to make a phishing one by taking legitimate website style sheet, copy it to the phishing website. To prevent this process by using CSS, we use algorithm which convert the content to lines then analyze it by compare it with the white list database. If more than half of the lines are similar to one of the website listed in the white list, then the website is marked as phishing website. This detection method used successfully in eBay and PayPal [11].

978-1-5386-4110-1/18/$31.00 ©2018 IEEE

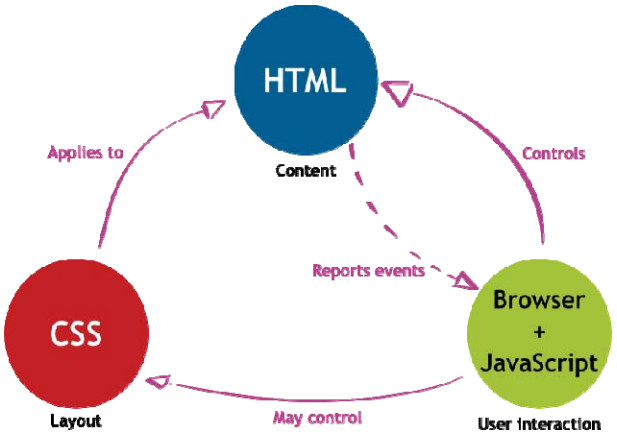

Figure 3. Cascading Style Sheet (CSS)

C. *Anomaly-based detection*

Anomaly based detection system is one of the intrusion detection system techniques. This type learns from the environment that installed in, to determine what is the normal behavior in the network would be [12].

The strength of anomaly based IDS is the ability of detects the unknown attacks (zero day attacks). Figure 4 shows anomaly detector flow [13].

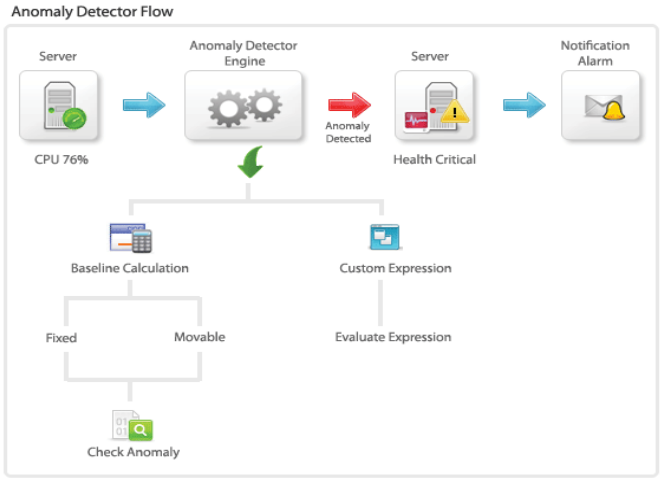

Figure 4. Anomaly based detection

D. *Detection using Honeypot*

A honeypot is a device or system works in a network, designed to be a trap for the networks hacker, so when targeting this device by the hacker we follow him and know the way he thinks and what will do with our device and catching him. So, all interaction with a honeypot is monitoring by the owners of network.

First, as presented in figure 5, firewall (or router) is set up to redirect traffic and activity on ports to a honeypot where the hacker expects associating with a genuine server. Then the alert mechanism is created with the objective that when honeypot is in danger, the alert is initiated. All the log records are saved on other machine with the goal that when the honeypot is in danger, the hacker cannot be able to delete these files.

Honeycomb is realized as a Honeyd extension. The idea of Honeycomb assumes that any activity directed to the honeypot can be considered an attack [14].

Honeycomb automatically generates signatures for all incoming traffic. If a similar pattern does not yet exist then new signatures are created. Existing signatures are updated whenever similar traffic has been detected, in this way, the quality of signatures increases with each similar attack. The mechanism creates signatures for all traffic directed to the honeypot.

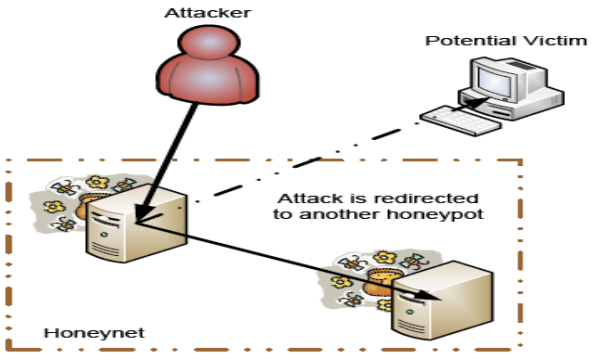

Figure 5. Detection using honeypot

III. PROTECTION OF ZERO-DAY ATTACKS

There is no way to protect systems as 100% of such types of attacks. Systems need to be protected as much as possible by taking due precautions. Some of these precautions are [15][16]:

- Organization must follow the security measures and recommendations in formulating policies on firewalls in their networks and ensure that they match the requirements of the organization.
- Educate staff and users through training about Security awareness, such as not to download files via email from unknown destinations.
- The organization must divide its networks and restrict access.
- Limit privileges as users only have access to the required information.
- Prevent users from downloading untrusted software by using application white listing.
- The organization must understand its network well and know the environment to reduce potential risks.
- The system must be continuously updated.
- Develop incident security plans for any possible exposure to minimize their impacts.

978-1-5386-4110-1/18/$31.00 ©2018 IEEE

- The Security organizations must identify and counter Zero-day exploits by cooperate and share information rapidly to identify new and unknown attacks.

IV. STRENGTHES AND WEAKNESSES

The main issue in anomaly-based detection is the high rate of false positives that is non-infected hosts were flagged as being infected by the system. While anomaly-based detection strengths that it could be used with Artificial Immune system to distinguish between normal and abnormal traffic in the network to detect Zero day and minimize the false positive [10]. Moreover, Dynamic anomaly based detection is collecting the information executed as results from programs that used to detect malicious code in the detection phase, then check for any conflict with what learns in training phase.

Honeypots had constrained field of view. Just observe action mounted against them. If an attacker breaks into an organization network, avoids the honeypot, and attacks a variety of production systems then the honeypot will be unconscious of the action. Sometimes a hacker can recognize a honeypot because he has prior knowledge of his characteristics and behaviors (fingerprinting). Indeed, the use of honeypots introduces risk. Honeypots once attacked, can lead to attack other computer systems on the network.

Some of strengths of honeypot that there no need to develop complex algorithms to implement honeypot. It is very simple, just set up a honeypot in the network, and then it will begin the work. It can decrypt any encrypted malicious activities. Honeypots used to catch outsider and insider threats. Any connection of the devices within the network with the honeypot shall be suspicious and may be evidence to the user that he has exceeded his privileges.

V. RESULTS

While anomaly based detection system being more effective when it is used with another system to minimize false positive alarms and latency. We suggest using it with honeypots in the network. Honeypots will keep attacker busy with virtual network that will give anomaly system a time to determine the target infected host. In addition, anomaly based detection learns from network environment the normal behavior, trying to make anomaly based detection learns from honeypot results will increase the defense efficiently depending on failure attempts of attacks. Figure 6 shows the proposed model diagram.

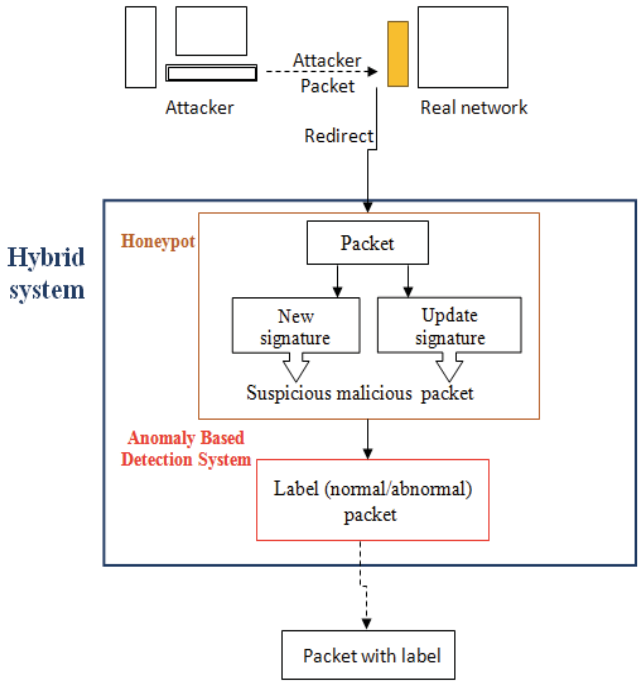

Figure 6. Hybrid system between Anomaly based detection system and Honeypot.

VI. CONCLUSIONS AND FUTURE WORK

Organizations need to protect their system from a core exploit, which is Zero-day attack. The research explore some techniques that used to detect and protect against it. Then the research expose the strength and weaknesses of two main approaches that are anomaly based detection and honeypot to protect against the Zero day attack based on a review of other researches. We proposed a hybrid model of anomaly based detection and honeypot as a powerful mechanism for Zero-day detection. It is necessary in the future research to conduct tests and implementation for the proposed model.

REFERENCES

[1] Reshma R. Patel and Chirag S. Thaker, " Zero-Day Attack Signatures Detection Using Honeypot" Proceedings published by International Journal of Computer Applications® (IJCA) International Conference on Computer Communication and Networks CSI- COMNET-2011.

[2] (2017) Zero Day Attack [Online] Available at : https://www.techopedia.com/definition/29738/Zero-day-attack. [accessed May 2017]

[3] (2007, October 27) What is Zero Day attack? [Online] Available at : https://askleo.com/whats-Zero-day-attack/. [accessed May 2017]

[4] L. Bilge and T. Dumitras, “Before we knew it: an empirical study of Zero-day attacks in the real world,” in Proceedings of the 2012 ACM conference on Computer and communications security, 2012, pp. 833–844.

[5] Hannes Holm," Signature Based Intrusion Detection for Zero-Day Attacks: (Not) A Closed Chapter?", 47th Hawaii International Conference on System Science, 2014.

978-1-5386-4110-1/18/$31.00 ©2018 IEEE

[6] Prakash Mandayam Comar, Lei Liu, Sabyasachi Saha, Pang-Ning Tan, Antonio Nucci, " Combining Supervised and Unsupervised Learning for Zero-Day Malware Detection", Proceedings IEEE INFOCOM, 2013.

[7] Jun Li, Shad Stafford, and Toby Ehrenkranz, "SWORD: Self-propagating Worm Observation and Rapid Detection", Department of Computer and Information Science, University of Oregon.

[8] Shad Stafford, Jun Li, Toby Ehrenkranz," Enhancing SWORD to Detect Zero-Day-Worm-Infected Hosts", Department of Computer Science, University of Oregon, 2007.

[9] Innab, N., Al-Rashoud, H., Al-Mahawes, R., & Al-Shehri, W. (2018). Evaluation of the Effective Anti-Phishing Awareness and Training in Governmental and Private Organization in Riyadh. 21st Saudi Computer Society National Computer Conference (SCS-NCC'2018) - IEEE

[10] Innab, N., Alamri, A.(2018). The Impact of DDoS on E-commerce. 21st Saudi Computer Society National Computer Conference (SCS-NCC'2018) - IEEE

[11] Michael Blasi , " Techniques for detecting Zero day phishing websites ", A thesis submitted to the graduate faculty in partial fulfillment of the requirements for the degree of MASTER OF SCIENCE, Iowa State University ,2009.

[12] Harish Valayapalayam Kumaravel ," AN ANOMALY-BASED INTRUSION DETECTION SYSTEM BASED ON ARTIFICIAL IMMUNE SYSTEM (AIS) TECHNIQUES", Thesis of Master of Science, Purdue University, Indiana, 2016.

[13] Detect Anomalies with Dynamic Baselines [Online] Available at : https://www.manageengine.com/products/applications_manager/application-anomaly-detection.html. [accessed May 2017]

[14] Ahmed Obied," Honeypots and Spam", Department of Computer Science University of Calgary, Canada.

[15] Jason M Syversen," METHOD AND APPARATUS FOR DEFENDING AGAINST ZERO-DAY WORM-BASED ATTACKS".

[16] "ZERO-DAY DANGER: A Survey of Zero-Day Attacks and What They Say About the Traditional Security Model", FireEye Security Reimagined.

978-1-5386-4110-1/18/$31.00 ©2018 IEEE