© 2016 IJSRSET | Volume 2 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Battling Against Intrusion and Behavior Based Healing System on Real Time Traffic Using Ourmon and Wireshark

Neeraj Shukla, Anjali Vishwakarma
Gyan Ganga College of Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

Intrusion Detection System (IDS) has been utilized as a key instrument as a part of shielding the system from this malevolent action. With the capacity to break down system activity and perceive approaching and on-going network attack, majority of system executive has swing to IDS to help them in identifying irregularities in system movement. The gathering of information and analysis on the anomalies activity can be classified into fast and slow attack. Since fast attack activity make a connection in few second and uses a large amount of packet, detecting this early connection provide the administrator one step ahead in deflecting further damages towards the network infrastructure. This paper describes IDS that detects fast attack intrusion using time based detection method. The time based detection method calculates the statistic of the frequency event using Wire shark which occurs between one second time intervals for each connection made to a host thus providing the crucial information in detecting attack.

Keywords: IDS, Wireshark, Anomalies

I. INTRODUCTION

In this information and communication technology age; the society cannot imagine living without the Internet and information systems. Nowadays the Internet plays an important role in stock market, access to weather forecast, E-medicine, E-commerce and even daily newspapers. The networking revolution has fully come of age in the last decade. As the network grows in size and complexity and computer services expands, vulnerabilities within local area and wide area network has become mammoth and causing lot of loop hole in security aspect [1]. The problems occur due to the increasing number of intrusion tools and exploiting scripts which can entice anyone to launch an attack on any vulnerable machines. An attack on network can be in 5 phases, which are Reconnaissance, Scanning, Gaining access, Maintaining Access and Covering tracks [2]. Identifying the first 2 activities will let the administrator to prevent the attack from doing further damage to the service offered by the network.

The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [3]. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete [4]. Both of the attack gives a great impact to the network environment due to the security breach. Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack. IDS acts as the monitoring tool to capture and analyze the network traffic for any anomalies activity.

This paper presents a novel methodology on detecting fast attack using time based detection technique for intrusion detection system. In this methodology the features capture from the network traffic is computed with respect to the time. The derived time based features from this methodology can help identify fast attack since the detection is based on the number of time the attacker made towards the host in second. Thus focusing in the time based features the early detection of the attack can

be achieved and the security personnel can directly do the necessary action to stop further damages.The rest of the paper is structured as follows. Section 2discuses the related work on Intrusion detection system, Section 3 presents the methodologies and the technique use in time based intrusion detection for fast attack. Section 4 elaborates on the analysis and result. Finally, section 5 conclude and discuss the future directions of this work.

II. METHODS AND MATERIAL

Related Work

An intrusion detection system can be divided into two approaches which are behavior based (anomaly) and knowledge based (misuse) [5], [6]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [7], [8]. The misuse or signature based IDS is a system which contains a number of attack description or signature that are matched against a stream of audit data looking for evidence of modeled attack [9]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique [10].

Meanwhile, the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be normal activity on the network or host [4]. The anomaly based system builds a model of the normal behavior of the system and then looks for anomalous activity such as activities that do not confirm to the established model. Anything that does not correspond to the system profile is flagged as intrusive.

False alarms generated by both systems are major concern and it is identified as a key issues and the cause of delay to further implementation of reactive intrusion detection system [11]. Therefore, it is important to reduce the false alarm generated by both of the system. Although false alarm is a major concern in developing the intrusion detection system especially the anomaly based intrusion detection system, yet the system has fully met the organizations' objective compared to the signature based system [12]. The false positive generated by the anomaly based system is still tolerable even though expected behavior is identified as anomalous while false negative is intolerable because they allow attack to go undetected [12]. Based on this motivation, anomaly based intrusion detection system is selected as an approach in detecting fast attack. Furthermore this research also managed to reduce the false alarm using the new model proposed by the logistic regression technique. The success of an IDS depends on the decision upon a set of features that the system is going to use for detecting the attacker especially the fast attacks. This is because the mechanism of a fast attack requires only a few seconds and the technique used by the attacker to launch the attack is also different [13]. To the best of our knowledge, there is no comprehensive classification of features that intrusion detection system might use for detecting network based attacks especially fast attacks. Different researchers use different names for the same subset of feature while others use the same name but different types [14]. Furthermore, understanding the relationship as well as the influence of the features in detecting the fast attack is also necessary to avoid any redundant features selected for the intrusion detection system.

Proposed Work

The increasing popularity of Internet is exposed to an increasing number of security threats [11]. In such open environment Network management and security is one of the most vibrant issue as well as implementing intrusion detection systems on networks and hosts requires a broad perceptive of computer security. The complexity of information technology infrastructures is growing rapidly beyond any one person's ability to understand them, let alone administer them in a way that is operationally secure. Another reason that network security (Intrusion Detection and Prevention Systems) are in demand is that operating environments are not secure. In fact, it could be argued that the demand for openness persuades lax security.

Modern security oriented approaches faces severe challenges due to unknown types of attacks appearing continually. The signature based techniques are not sufficient for defense against unknown attacks. In such circumstance, anomaly-based intrusion detection method is a valuable technology to defense against malicious

activities. Secondly all such methods must test and validated in real time network flow.

Types of Anomalies

1. UDP flood
2. ICMP flood
3. SYN flood
4. DoS and DDoS
5. Trojan & Worms

These are the major anomalies that breach the security of a network or host itself.

Today's another important requirement is prevention of such unauthorized activities that compromised security pillar (Authentication, availability, Confidentiality and Integrity) of data or information. Hence many security measure i.e. IDS with prevention approach have been proposed but the major limitation of IDPS technology still remain , one biggest issue with IPs (or IDPS) is performance lacking with real time, and at last but not the least FALSE ratio is another big challenge for defense against intrusion.

Following problems has been identified-

1. The dilemma between detection speed and false alarms (negative and positive) is the big challenge for security professionals. Resulting low detection efficiency, due to the high false positive and negative rate.
2. Low throughput and high cost, mainly due to the high data rates (Gbps) that illustrate current wideband transmission technologies.
3. The absence of appropriate metrics and assessment methodologies.

For protecting the network or resources from attackers we have proposed security solution for the network and host that detect and prevent above mentioned anomalies of the network. Our approach is based on anomaly detection principal that finds unknown (new or novelty) types of attacks in the system on real time flows.

For achieving this I have going to developed the security system that sniffing the network packets and stored on database, after capturing raw packets we have applied preprocessing on them then these input to Anomaly detector engine where detection has been takes place then the our anomaly detector makes profile and compare with normal profile then actual work of anomaly detector engine has taken place where it compare the profile and see the deviation and inform to system administrator that takes the action against attack.

The key features about propose solution is that its quickness to attack or intrusion fats response and the network and check the unauthorized activities on the system if abnormality have occurred they responsds to them and take the appropriate action to defense against illegitimated packets. We will use ourmon tolls and RRDTool database for making knowledge base.

Proposed Algorithm

a) Capture network traffic (flows)-

- number of flows per minute
- number of packets per minute
- number of bytes per minute
- average number of packets per flow per minute
- average number of bytes per flow per minute
- number of unique IP addresses seen per minute
- number of L2 layer flows
- number TCP packets, port and their control bits (R/S/F) per minute flows
- number of ICMP flows
- number of UDP flows
- DNS statistics
- HTTP flows (for detecting Trojan)

b) Assume it, M= (m1, m2….mn) Calculate Mean, Max and Average

c) Calculate TCP Work Weight, TCP Worm Weight, TCP Error Weight and UDP Work metric.

Then calculate a threshold value say Tv calculated as the mean value over the last 20 minutes plus/minus five times its standard deviation.

Calculation of TCP control bit weight is using following rules:

1. TCP work weight:
   IP source: (syn +fin + reset)/total pkts
2. TCP worm weight:
   IP src: syn - fin > N
   Where N number of control bits. We have fixed its value to *18.
3. TCP error weight:

*IP src: (syn - fin) * (reset+ICMP_errors)*

4. UDP work metric:
   *IP src: (UDPs – UDPr) * (ICMP_errors)*
5. HTTP per minute flows

After that all these five metrics have compared with threshold (Tv) and check the deviation (in ADE) if found call to raise alarm and starts prevention mechanism.

III. RESULTS AND DISCUSSION

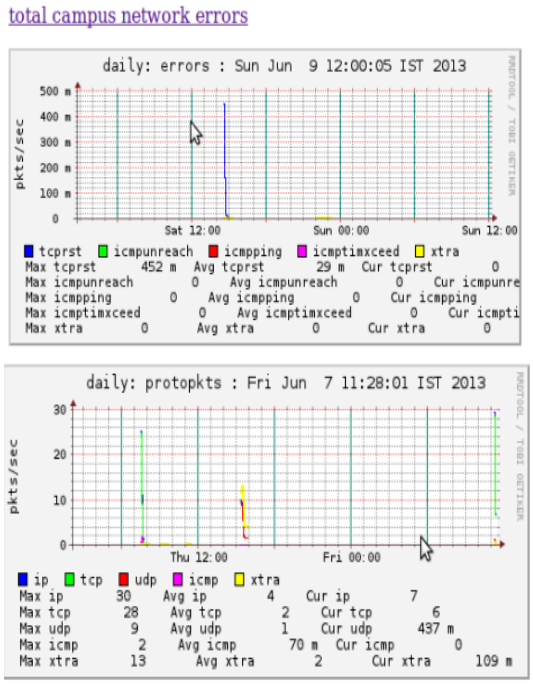
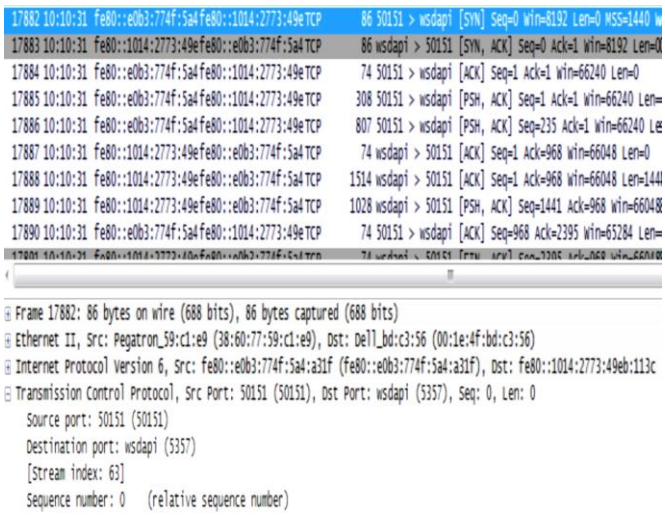


Figure 1 : shows TCP packets for PSH, ACK messages using Wireshark



IV. CONCLUSION AND FUTURE WORK.

Before determining a network traffic is a potential threat to a network or not, there is a need for an IDS to have a method in differentiating whether it is malicious or not. Therefore, this research has introduced a new methodology to identify a fast attack intrusion using time based detection. The method used to identifies anomalies based on the number of connection made in 1 second. The approach is then tested on real network traffic data and the result is then evaluated by using the Classification Table based on the logistic regression model. And also performing port scanning using wireshark for identification suspicious connection From the test and analysis it is shown that the model is suitable for predicting the normal and abnormal behavior in UDP and ICMP protocol using Wireshark.

For further validation, the methodology will be implemented on a different set of real network traffic.

V. REFERENCES

[1] Haitao Sun, Shengli Liu, JiayongChen and Changhe Zhang "HTTP tunnel Trojan detection based on network behavior", Elsevier, Proceedings to the Energy Procedia ESEP 2011: 9-10 December 2011, Singapore, pp. 1272 – 1281, 2011.

[2] Borders K and Prakash A. Web tap:detecting covert web traffic. Proc. ACM conference on Computer and Communications Security (CCS 04)2014;110-120.

[3] Kruegel C, Vigna G. Anomaly Detection of web-based attacks. Proc. ACM conference on Computer and Communications Security (CCS 03)2013;251-261.

[4] Wenke Lee. (2010). A Data Mining Framework for Constructing Feature and Model for Intrusion Detection System. PhD thesis University of Columbia.

[5] Cuppen, F. & Miege, A. (2012). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002.

[6] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2014). Statistical Traffic Modelling for Network

Intrusion Detection. In Proceeding of the IEEE Conference.

[7] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2015). Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference.

[8] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007.

[9] Wang Y., Huang GX. & Peng DG. (2006). Model of Network Intrusion Detection System Based on BP Algorithm. Proceeding of IEEE Conference on Industrial Electronics and Applications, IEEE, 2006.

[10] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2010). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.

[11] Karl Levitt. (2012). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2012.

[12] Garuba, M., Liu, C. & Fraites, D. (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE, 2008.

[13] Robertson S., Siegel EV., Miller M. & Stolfo SJ. (2003). Surveillance

[14] Detection in High Bandwidth Environment. In Proceeding of IEEE Conference on the DARPA information Survivability and Exposition, IEEE, 2013.