Amrita Anand, Brajesh Patel / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 3, Issue 4, Jul-Aug 2013, pp.887-891

Fighting Against Intrusion and Proposed Behaviour Based Healing System on Real Time Traffic

Amrita Anand*, Brajesh Patel**
* (Department of Computer Science,,student of M.E (4th sem), S.R.I.T, Jabalpur, R.G.P.V University, Bhopal (M.P.),India
** (Department of Computer Science, HoD (M.E), S.R.I.T, Jabalpur, R.G.P.V University, Bhopal (M.P.),India

ABSTRACT

Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious activity. With the ability to analyze network traffic and recognize incoming and on- going network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic. 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 gives a comparison between signature based and anomoly based IDS,we capture real time traffic using ourmon and concenterate to work on attack on TCP,UDP,ICMP protocol.

***Keywords*:** anomaly, attack ,IDS, ourmon ,UDP.

I. INTRODUCTION

Internet is forcing organizations into an era of open and trusted communications. This openness at the same time brings its share of vulnerabilities and problems such as financial losses, damage to reputation, maintaining availability of services, protecting the personal and customer data and many more, pushing both enterprises and service providers to take steps to guard their valuable data from intruders, hackers and insiders..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]. Intrusion Detection System has become the fundamental need for the successful content networking There are two types of IDS: The one is Network based IDS(NIDS) and the other is Host-based IDS(HIDS). The NIDS monitors the packets from the network and HIDS analyzes the audit data of the operation system. There are also two major categories of the analyzes techniques of IDS: the anomaly detection and the misuse detection. Anomaly detection uses the established normal profiles to identify any unacceptable deviation as the result of an attack. Misuse detection uses the "signatures" of know attacks to identify a matched activity as an attack instance. Both of them can be used in the NIDS or HIDS. Due to the i ncreasing 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.

This paper presents a comparison between different techniques s u c h a s signature based and anomaly based technique. Fast attack using time based detection technique for intrusion detection system. In this methodology we capture the network to make no connection made toward host and concenterate to work on TCP, UDP and ICMP protocol The rest of the paper is structured as follows. Section 2 discuses 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 a n a l y s i s and r e s u l t . Finally, section 5 conclude and discuss the future directions of this \work.

II. 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].fig 1 shows the method of signature based technique.

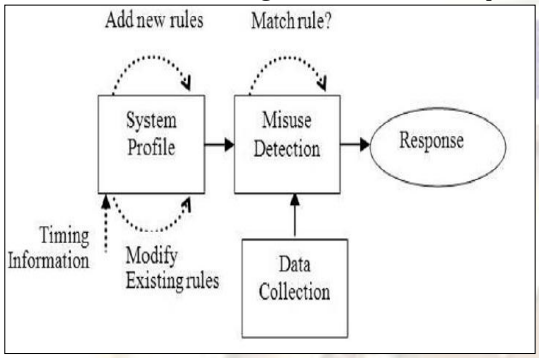

Figure1. Signature based technique

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 fig 2.

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

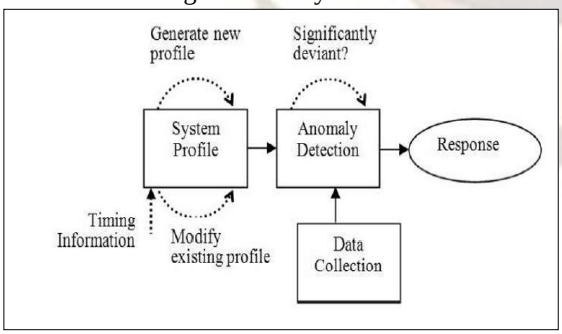

Figure2.Anamoly based technique

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.

Table 1.Comparison between Anomaly and Signature based IDS

Parameters	**Signature based IDS**	**Anamoly based IDS**
False Negative Alarm	Newly created malicious attack go undetected which lead to False negative	Rate of false negative alarm is comparativl y low
Update	It require regular update in database ,so it can detect new attack	No regular update is required
Susceptibility to attack	It proves to be difficult against evasive attack.	Rate of detection to evasive technique are significantly higher in comparison to signature based.
Coverage of NIDS	It is able to detect external attack but it is not to able to detect internal attack	It can detect both internal and external attack.

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 toavoid any redundant features selected for the intrusion

detection system.We found that in our suevey that researcher concenterate only on tcp connection . Xiao et al.concentrated on detecting DDoS attack by considering only TCP-SYN flag without others protocol. Kanlayasiriet. al only concentrated on port scanning activity by focusing only at TCP-SYN but it feature will not capable to detect any fast attack from UDP protocol.Faizal used a time based approach in intrusion detection to detect fast .In their Researcher used the classification table is chosen as one of the test used to assess the model. Using the classification table, the percentage of the detection attack rate and detection normal rate can be calculatedbut they tested their research on real traffic but concentrated only on tcp connection

III. 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

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.

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 take 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 use ourmon tool and RRDTool database for making knowledge base.

Ourmon is an open-source network management and anomaly detection system .It monitors a target network both to highlight abnormal network traffic and measure normal traffic load. network monitoring system is an open-source tool for real-time monitoring and measurement of traffic characteristics of a computer networkThe Ourmon network measurement system architec-ture consists of two parts: a front-end probe and a back- end graphics engine system. Optimally these two parts should run on two separate computers in order to minimize the application compute load on the probe itself . It display real-time data in a graphical format .

Proposed Algorithm-

a) Capture network traffic (flows)-

- number of flows per second
- number of packets per second
- number of bytes per second
- average number of packets per flow per second
- average number of bytes per flow per minute number of unique IP address seen per second 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:

1. TCP work weight:

IP source: (syn +fin + reset)/total pkts
2. TCP worm weight:
IP src: syn - fin > N
where N is 20.
3. TCP error weight:
*IP src: (syn - fin) * (reset+ICMP_errors)*
4. UDP work metric:
*IP src: (UDPs – UDPr) * (ICMP_errors)*
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.

IV. RESULT

Fig 3 shows a breakdown of network-wide TCP control packets, including SYNS, FINS, and RESETS. This may be of use for spotting SYN anomalies as well as other kinds of anomalies. It can sometimes be possible to spot an attack on this graph. Fig 5In this anomaly detection engine check the number of different kinds of ICMP unreachable errors

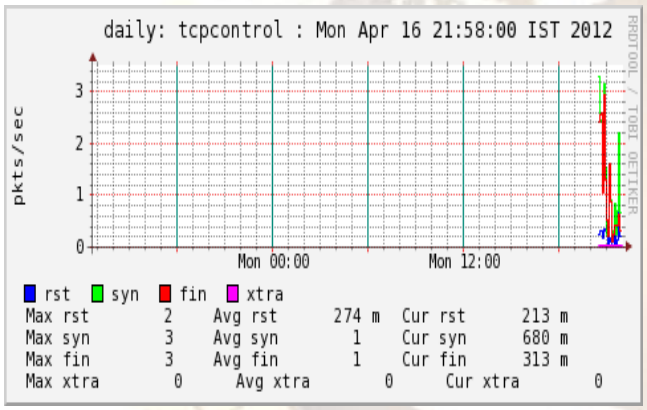

Figure 3TCP CONTROL

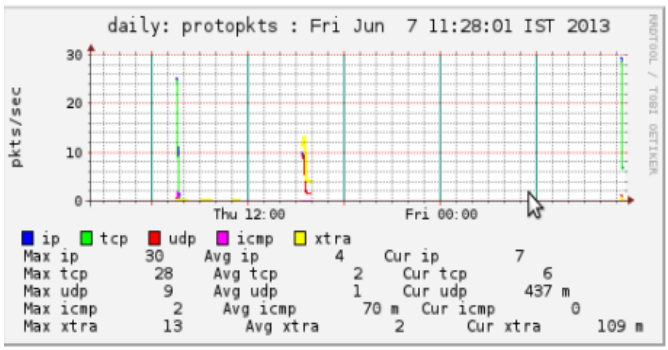

Figure 4 Network flow

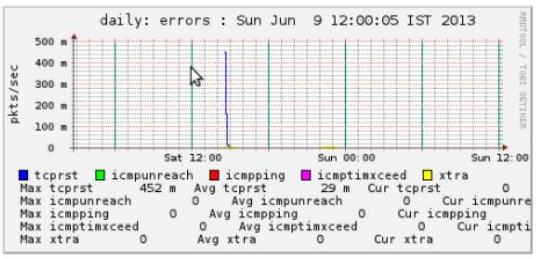

Figure 5 Network error

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

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)2004;110-120.
[3] Kruegel C, Vigna G. Anomaly Detection of web-based attacks. Proc. ACM conference on Computer and Communications Security (CCS 03)2003;251-261.
[4] Wenke Lee. (1999). A Data Mining Framework for Constructing Feature and Model for Intrusion Detection System. PhD thesis University of Columbia.
[5] Cuppen, F. & Miege, A. (2002). 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. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.

[7] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005). 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. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.

[11] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.

[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, 2003.