© 2015 IJSRSET | Volume 1 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Detection of UDP and HTTP Anomalies on Real Time Traffic Based on NIDS using OURMON Tool

Mahendra Kumar Rai, Vijay Shankar Mishra
Shri Ram Institute of Technology (SRIT), Jabalpur, Madhya Pradesh, India

ABSTRACT

UDP traffic has recently been used extensively in flooding-based distributed denial of service (DDoS) attacks, most notably by those launched by the Anonymous group. the use of this criterion to classify UDP traffic with the goal of detecting malicious addresses that launch flooding-based UDP DDoS attacks. We conducted our experiments on real time network traffic including large corporations (edge and core), ISPs, universities, financial institutions, etc. In addition, we also conducted experiments on ourmon tool of our own. All the experiments indicate that proportional packet rate assumption generally holds for benign UDP traffic and can be used as a reasonable criterion to differentiate DDoS and non-DDoS traffic. We designed and implemented a prototype classifier based on this criterion and discuss how it can be used to effectively thwart UDP-based flooding attacks.

Keywords: UDP, DDOS, IDS, HTT, NIDS

I. INTRODUCTION

Intrusion Detection System [4] can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. The intrusion detection part of the name is a bit of a misnomer, as an ID does not actually detect intrusions it detects activity in traffic that may or may not be an intrusion. These devices, similar to firewalls, inspect incoming and outgoing network traffic. Unlike firewalls [9], however, they do not alter the traffic flow by dropping or passing certain packets. Rather, they look for malicious traffic that may be indicative of an attack or other misuse and log an alarm with specific data for administrative review.

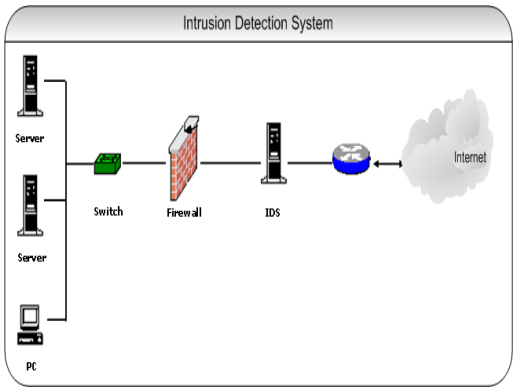

Figure1: Intrusion Detection System

Intrusion detection refers to the monitoring of events and the analysis for signs of intrusions. Intrusion detection systems (IDSs) are software applications which automate these monitoring and analysis processes [5]. IDSs are typically used to detect attacks or violations not detected by other security means; to detect reconnaissance attempts preceding attacks such as with probes and scans. They can also be used to control the quality of an existing security design and administration, or to help diagnosis.

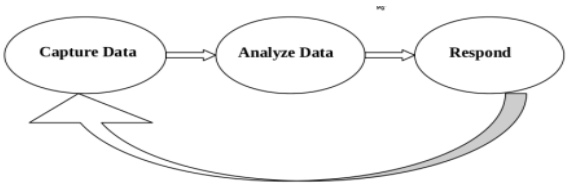

Figure 2: Block Diagram Of IDS

IDS have 3 phases of functioning. First it captures the data passing into and outside a network. Then it watches and analyses the data about its behavior, so that it can know whether it is malicious or not. If it detects that the data is malicious, then it responds to that, for example, blocking the data to protect from future damages.

Advantages of IDS

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity

- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns Tracking user policy violations

II. METHODS AND MATERIAL

2.1Anamoly and Signature Based Technique

Reseacher presented a comparitive study between heuristic approaches and signature based this paper draws a comparitive analysis between on varios parameters comparitive study of security objective of two NIDs provides the basis of paper they found thatheuristic based NIDS effectively meet the organizational objectives of an organization in contrast to a signature based NIDS. The basis for such analysis is determined by the contrasting composition of the two NIDSs. The dependency upon competent personnel by a signature based NIDS is the underlying factor of its inadequacy. A system is not feasible if its performance is based solely on personnel.

2.2 False Positive and False Negative Alarm

In order to determine the accuracy of these two system the false negative and false positive[12,13] are deduced.Signature based NIDS require the use of signature incoproted in the database to match the signature of packets entering into network to match the signature of packets entering into network.Newly created malicious code or unknown virus within the system are classed as false negative.Unlike signature based NIDS ,the rate of false negative[12] is low in heuristc system.Non dependence upon signature and use of statsicial and behaviour to determine new types of malicious code allows for a low false positve rate.Heuristic based NIDS use behavioural pattern of users the occurance of an attack.

2.3 Update

The rapid change of product causes a software to become quickly outdated the direct correlation is evident as the necessity for the frequent update becomes mandatory which is compounded further by obsolence of signature within the database .Dependency of signature based NIDS on update is at the root of problem.This inherent limitation allow system to suffer from attack.

2.4 Competency

An competent[12] network security personnel correlates to an ineffective signature based NIDS Vulnerabilities are introduced, not because of incompetent workers, but because of the requirement placed on workers to identify all known threats. The issue of competency[13] does not impact upon the performance of a heuristic based NIDS. Conversely, its ability to detect threats is dependent upon its ability to determine abnormal patterns within the network. Its capability of learning, through statistical interpretation or modeling of behavioral patterns, whether accepted normal and abnormal behavior

2.5 Suspectibility of Attack

Deploying countermeasures for signature-based systems against evasive attacks proves to be very difficult. Signature based systems utilize the technique of pattern matching. If known signatures are modified in any way that do not meet the pattern of the signatures contained within the database, no alarms are raised and the attack is undetected Heuristic based systems also allow undetected threats into the network system, but its rate of detection to evasive techniques are significantly higher in comparison to signature based systems.

2.6 Coverage of NIDS

The coverage scope of the NIDS is pertinent to its ability attacks that contain signatures are typically external attacks, such as viruses and other malicious code. Heuristic based NIDS, in contrast, are able to cover all aspects of the network, both external and internal threats.

2.7 Threshold Verification For Detecting Attack

In real time network, early detection of fast attack can prevent any further attack and reduce the unauthorized access on the targeted machine .Fast attack[1] can be defined as an attack that uses a large amount of packet or connection within a few seconds The correct threshold value, add an extra advantage for IDS to detect anomalies in the network. the correct threshold value, add an extra advantage for IDS to detect anomalies in the network. Therefore this paper discusses a new technique for selecting static threshold value from a minimum standard features in detecting fast attack from the victim perspective. In this research we are focusing

on detecting fast attack based on the connection made by attacker on a single victim. The normal and the abnormal traffic are differentiated using a threshold value The overall threshold verification process is depicted in figure 2. The observation is done on real time network traffic from a government agencies and simulation traffic from Darpa99. The purpose of the observation is to identify the average connection made by host or hosts to single victim within one second time interval. By doing this, the connection made to single victim can be identified. The result from the observation technique will be compared to select the appropriate static threshold. Meanwhile, for the experiment technique, a small local area network (LAN) was setup. The purpose of the experiment is to identify the normal connection made by each of operating system. By doing this, the normal behavior of host in transmitting network packet to the destination host within one second time interval is identified. The result from each of the operating system will be captured and compared with each other.

PROPOSED WORK

Today's chief 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-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. 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.

We found that in our survey 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 concentrated on port scanning activity by focusing only at TCP-SYN but it feature will not capable to detect any fast attack for UDP protocol.Faizal used a time based approach in intrusion detection to detect fast attack on real traffic but concentrated only on tcp connection our work is inspired from author as he concenteraed only on tcp connection we extend our work to Udp protocol we capture real time traffic tat udp connection real trafficand we can capture activity on UDP port.

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 will use ourmon tool and RRDTool database for making knowledge base. Following algorithm has been used to detect suspicious traffic For (all traffic (incoming/ outgoing) do:

1. Collect real time traffic as flow statistics
    a. TOTAL network traffic capture
    b. DNS statistics
    c. TCP Traffic and SYN count
    d. TCP traffic with PUSH flag
    e. UDP Traffic
    f. HTTP traffic at port 80

2. If (traffic capture > average or DNS > average) then

Calculate TCP work weight (as proposed in main PROPOSED ALGORTIHM):
If (SYN-FIN>18) or (TCP_flag==PUSH)
{
Msg =”HTTP Trojan is detected”
Raise the alert

BLOCK IP address of the suspicious trafficRESET (using TCP RESET)the connection
Send ICMP unreachable msg to attacker
}
Else if (UDP work weight >70)
{
Msg =”HTTP Trojan is detected”
Raise the alert
BLOCK IP address of the suspicious traffic
RESET (using TCP RESET) the connection
Send ICMP unreachable msg to attacker
}
Else if (HTTP captured traffic >average)
{
If(HTTP_Session_duration>normal_duration
OR
HTTP_total_data > normal_data)
Msg =”HTTP Trojan is detected”
Raise the alert
BLOCK IP address of the suspicious traffic
RESET (using TCP RESET)the connection
Send ICMP unreachable msg to attacker
}
Else if (listen to IRC Channel traffic > average flow)
{
Msg =”HTTP Trojan is detected”
Raise the alert
BLOCK IP address of the suspicious traffic
RESET (using TCP RESET)the connection
Send ICMP unreachable msg to attacker
}
Else
{
Go to step 1:
}
}

III. RESULTS AND DISCUSSION

Basic Network Information

The pkts filter displays the number of total packets caught and/or dropped by the kernel packet mechanism (BPF). Drops are nature's way of telling you that you or the person making the DOS attacks. Dropped packets can also occur during attacks. mon.lte output for pkt dropped is as follows-

pkts: caught:9440 : drops:0: caught2:0 : drop2:0

Figure (a) and (b) shows the basic network information. Figure (a) shows number of packets capture and drop on daily basis, while (b) shows on weekly basis.

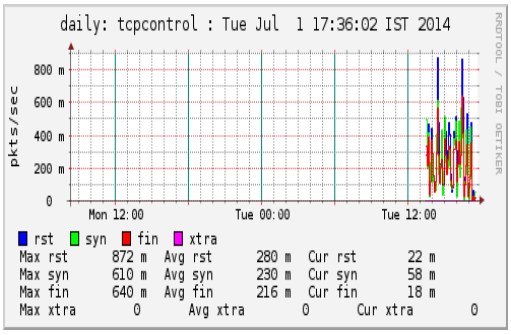

Figure (a)

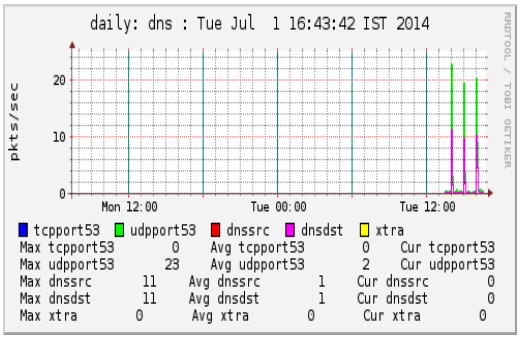

Figure (b)

IV. CONCLUSION

Network traffic is a potential threat to a network or not, there is a need for 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. 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.

V. REFERENCES

[1] 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.

[2] Yan Qial and Xie Weixin, “A Network IDS with Low False Positive Rate,” In Proc. of the 2002 Congress on

Evolutionary Computation, Vol.2, pp. 1121-1126, 2002. 13

[3] Manasi Gyanchandani*, J.L.Rana**, R.N.Yadav* Taxonomy of Anomaly Based Intrusion Detection System: A Review International Journal of Scientific and Research Publications, Volume 2, Issue 12, December 2012

[4] P. Garcıa-Teodoroa, J. Dıaz-Verdejoa Anomaly-based network intrusion detection Techniques, systems and challenges elseivier computer security 2009

[5] Dr. Fengmin Gong, Chief Scientist, McAfee Network Security Technologies Group Deciphering Detection Techniques: Part II Anomaly-Based Intrusion Detection .

[6] Karthikeyan .K.R and A. Indra Intrusion Detection Tools and Techniques – A Survey International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010

[7] Sandip Sonawane , Shailendra Pardeshi and Ganesh Prasad A survey on intrusion detection techniques World Journal of Science and Technology 2012

[8] Mikhail Gordeev Intrusion Detection: Techniques and Approaches www.forum-intrusion.com/archive/Intrusion 2003

[9] V. Jyothsna V. V. Rama Prasad A Review of Anomaly based Intrusion Detection Systems International Journal of Computer Applications

[10] Hu Zhengbing1,2, Li Zhitang1 A Novel Network Intrusion Detection System(NIDS) Based on Signatures Search of Data Mining 2008 Workshop on Knowledge Discovery and Data Mining .

[11] Mohammad Sazzadul Hoque1, Md. Abdul Mukit International Journal of Network Security & Its Applications , AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM Vol.4, No.2, March 2012

[12] Iosif-Viorel Onut and Ali A. Ghorbani Toward A Feature Classification Scheme For Network Intrusion Detection Proceedings of the 4th Annual Communication Networks and Services Research Conference 2006 IEEE 13Faizal M. A.1, Mohd Zaki Mas'ud Threshold Verification Technique for Network Intrusion Detection System International Journal of Computer Science and Information Security, Vol. 2, No. 1, 2009

[13] Xin Zhao, Fang Liu, LuYing Chen, Zhenming Lei RESEARCH ON PORTSCAN DETECTION BASED ON SELECTIVE PACKET SAMPLING Proceedings of AIAI2010

[14] Alper T. Mzrak Detecting Malicious Packet Loss IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, FEBRUARY 2009

[15] Papadogiannakis, A., Polychronakis, M. & P. Markatos, E., (2010). Improving the Accuracy of Network Intrusion Detection System Under. Load Using Selective Packet Discarding. European Conference on Computer System, Paris, France.