World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:11, 2007

Intrusion Detection System Based On The Integrity of TCP Packet

Moad Alhamaty , Ali Yazdian , Fathi Al-qadasi

Abstract**—** A common way to elude the signature-based Network Intrusion Detection System is based upon changing a recognizable attack to an unrecognizable one via the IDS. For example, in order to evade sign accommodation with intrusion detection system markers, a hacker spilt the payload packet into many small pieces or hides them within messages. In this paper we try to model the main fragmentation attack and create a new module in the intrusion detection architecture system which recognizes the main fragmentation attacks through verification of integrity checking of TCP packet in order to prevent elusion of the system and also to announce the necessary alert to the system administrator.

Keywords**—** Intrusion detection system, Evasion techniques, Fragmentation attacks, TCP Packet integrity.

I. Introduction

COMPUTER networks can be considered as an important component of today human life. Since data and information of various organizations and companies are transferred through private and public networks such as global internet network, thus special attention with respect to security parameters of network has emerged and is even increasing progressively. Various techniques in view of elevating the security of network have been implemented which possess the ability of hiding sensible data from being accessible to hackers and also the recognition of various attacks prove to their occurring .As a whole the important tools are increasing the security of the network firewall and intrusion detection system. The main aim of intrusion detection system is analysis and processing of information which get transferred within the network and identify unrecognizable behavior so that in that way .There is the possibility or providing necessary attention to the network administrator, Since mankind himself is the creator of offences, computer system have always remained uncap- able in front of man thoughtful nature. Usually hackers do their best by using different techniques in order to perform their own attack [1].

Moad Alhamaty, master student in the information technology Department in the Tarbiat Modares University. Tel:+98-21-88004432-329, e-mail: alhamaty@yahoo.com.

Dr.Ali Yazdian . Prof Ass. In the Tarbiat Modares University ,e-mail: yazdian@modares.ac.ir.

Fathi Al-qadasi, doctoral student in information technology department, In the Tarbiat Modares University.e-mail: alqadasi_ye@yahoo.com

For example, a hacker is able to perform an attack which has no resemblance what so ever with one of the land marks pertaining to the intrusion detection system or can change offensive signature in such a way that the intrusion detection system considers it as a normal packet. The process according to which we have pushed forward our work in this investigation is as follows:

In the beginning, we have summarized on the TCP Fragmentation attacks so as to provide an appropriate background for understanding the related work. Also, to develop a more transparent view with respect to our investigative background, we have tried to comprehend the related tasks so as on the basis of the out come in the last stage, the obtained results can be compared with those of other investigations. Therefore, we concentrate on finding a solution to the intrusion detection main attacks of fragmentation information packets and also describe the used architecture in the investigation. We also describe the mechanism behind the detection of attack of information packets in a complete way and in the end; we'll mention simulating results and their comparison with obtained results of other performed tasks.

A. Summary on fragmentation attack

One of the drawbacks of intrusion detection system is based upon the ability of this system to be eluded via fragment of information packets [2]. Examples of this attack are DoS attacks which affect the rentability of its working efficiency. These are attacks whose signature is compatible with signature of the intrusion detection system, but the mechanism of some of the Dos attacks is based upon fragmentation of information packets which result in the inability of the intrusion detection system to recognize them [2]. As IDS detects the attack by checking the signature of the attack with its own signature and it can subsequently alarm the network administrator. As such, the hacker tries to permutate the attack signature in such a way that there exists no similarity whatsoever with the IDS database.

One of these attacks (although it possesses a signature to undertake an attack but it performs the attack in a manner that the IDS is incapable to recognize it) is TCP fragmentation attacks. Different techniques for the improvement of IDS against this type of attack have been presented which verify the signature attack. In the TCP packets, although there exists signatures to detect attacks like tiny Fragmentation and overlapping fragmentation [3], but still in the context of fragmentation of information packets other attacks have been

brought forward that can elude the NIDS [4]. We are now going to describe one of these attacks which utilize fragmentation techniques of information packets in view of eluding the IDS:

TCP packets are intentionally configured so that after fragmentation of this packet and its sending within different messages, only 2 byte from this first packet will be sent and upon reaching the IDS it will neither possess a header nor a final destination port which in fact will arrive at the following packet. Therefore the IDS recognize this part as being normal. The next packet owing to the fact (Fragmentation offset =1) requires no processing. And the remainder of the packet passes through to target system and is reassemble and the considered port is opened. In this paper we present a new module to the IDS in the form of an additional design that detect the elusive IDS attacks. Since in this paper we cannot describe all types of attack we will only the remainder ones.

- Overlapping fragmentation attacks.
- Combination of the tiny and overlapping fragmentation attacks.
- Unnamed fragmentation attacks.

II. Related Works

In this section, we review related work in the area of IDSs evasion and the comparison of our approach with other works.

Ptaced and Newsham [4] used semantics preserving IP and TCP transformations to elude every NIDS they tested, they also implemented a tool for Packet manipulation [6]. Similarly, Handley and Paxson [7] discussed evasion techniques based on inherent ambiguities of the TCP/IP protocol. These researchers were the first to systematically address NIDS evasion techniques. Shai Rubin and Somesh Jha have also undertaken other tasks in the NIDS background and they have implemented the AGENT tool for production of an attack rule and his results was very good, approximately 98.5% accurate in detection [8]. other NIDS based on the intelligent by Ozgur Depren and Murat Topallar in the 2005 has presented which can production the rule of the attack and it had good results specially in the DoS attack [9]. and other work in these bases being performed are some of this in TCP packet Normalization and other in the attack detection in the network traffic [10]. But unlike our work, their researchers provide neither architecture module for their work nor form the main architecture of the NIDS for validation of their work but we have illustrated a new architecture module for our work (Evasion Detector) which we put in the intrusion detection system for reprocessing the TCP packet to find the evasion Pattern, In the next section we explain the IDS architecture that it has the sensor for process and detect the attack but its evasive. We present the new part of architecture to permit reprocessing the TCP packet, one time in the sensor in the IDS and the other in the Evasion Detector, when TCP packet Pursuant integrity detection algorithm detected it be passed .other way (not integrity) it can be produce the alarm and the special signature in the IDS Database will be noted for the next check IDS sensor that can be detected.

III. Presented Solution and New Architecture

The presented method is based on a special method for detection of a fragmentation attacks which its purpose being to elude the IDS. This method is constituted of two sections. Its first part is extension architecture in IDS structure and its second part is rules that have a logical equation for extension architecture. In the first stage, we start with IDS architecture then we will explain detection rules mechanism.

A. New Architecture

Intrusion detection systems have a detector that is responsible for detection intrusion. This sensor is a decision making mechanism that is based on intrusion type. Figure (1) shows the main structure of IDS.

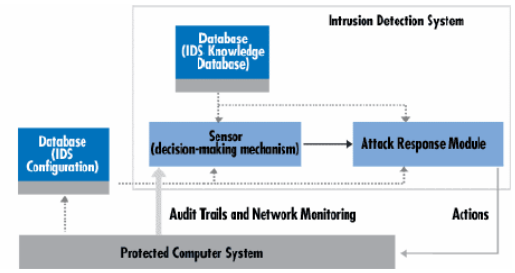

Fig. 1 The structure of IDS

This sensor obtains unrefined information from three sources:

1- From information existing in IDS information bank.
2- Syslog file.
3- Traffic traces and network controlling.

Now, in consideration of IDS architecture, usually NIDS detect each attack by one signature. Thus, if a hacker performs an attack by a small change in attack signature that exists in IDS information bank, since IDS identify this attack by a special sign, IDS cannot detect this attack. Our main idea is to check TCP packet integrity so as not to restrict the check attack special signature. And our work focuses on the packet that whether packet rightly is fragmented or not, until by change attack signature we could detect the attack. So we invent a module in IDS structure that simultaneously occurs with test within system sensor, TCP packet also tested in Evasion Detection Module. Figure (2) show the new architecture.

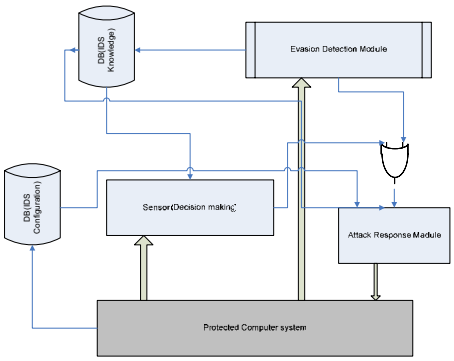

Fig. 2 the new architecture with Evasion Detection Module

Evasion Detection Module can include various parts that check different protocol's packets such TCP, UDP, ICMP. But because our study is on TCP packets, the main algorithms focus on TCP protocol. Evasion Detection Module structure showed in figure (3).

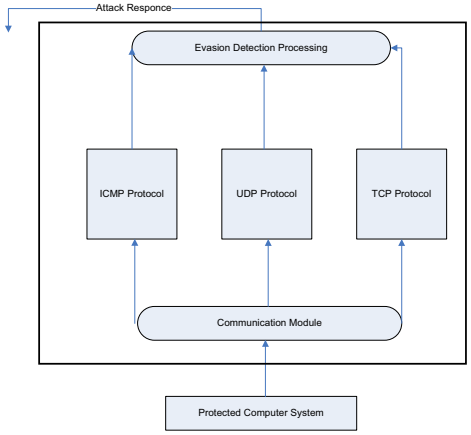

Fig. 3 Evasion Detection Module structure

As mentioned, addition of this module to the main IDS architecture means that one special process has taken place on protocol, so suspicious packets within network traffic pass the IDS and cause occurrence attack. In this way TCP information packet is processed simultaneously in tow functions, in IDS sensor and in Evasion Detector that is specific for evasion detection. Whereas one of these tow mechanisms detect a case of attack, it save its signs in IDS database and give alarm by OR Gate that connected to attack response model.

B. Detection Mechanism

Detection mechanism is synthetically made up of three rules which come in a form of a logical formulae .each one of the rules detects a special attack and all of the rules detect all the attacks. Besides the other attacks the combination of three rules of the logical formulae is as follows:

$$A.L+\overline{A}.S+D.\overline{A}$$

Equation (1)

Which are:

A→ Fragment offset = 0.

L = Transport length of TCP header where in this case ,it shouldn't be less than 4 byte to include interesting header fileds like source and destination port .

S = SYN bit.

D = Don't Fragment bit.

The main rules are as the follows:

Rule (1):

If FO=0 and Transport length (TCP) < 4byte [(S+D) port] then drop packet.

Rule (2):

If FO= 1 and SYN =1 then drop packet

Rule (3):

If DF= 1 and FO>0 then drop packet.

The combination of rule (1)and (2) results in detection of the Tiny + Overlapping fragmentation attacks and the combination of the second section of rule (1) and the second section of rule (2) results in detecting SYN Flood attack. The combination of the rules together in the form of formulae (1) leads to specify a kind of fragmentation which is detected on TCP packet and it also detect the attacks under consideration.

The logical schematic of the synthetic three rules is as illustrated below:

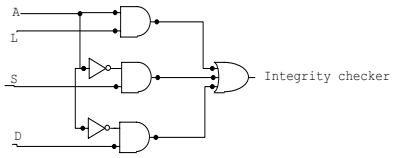

Fig. 4 Logical schematic formulae

IV. Simulation and Results

In order to configure each one of the rules separately and combining them a software application called Sniffer Protable[12] is used and to simulate attacks packet we can use several application such as sniff 'em [13], Engage packet builder [14], IP-tools[15] and Nmap [16], etc. to execute fragmentation we can use tools such as Fragrouter [17] which spilt the TCP into pieces. We used several attack scripts and other attack data in the MIT university site whose proposal is to test Intrusion Detection Systems .

The Network which was used is as follows :

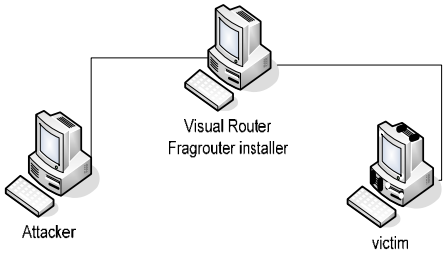

Fig. 5 Attack lab. Network

In simulating rule (1) approximately 14000 different information packets were sent to the target computer which included 10000 Tiny Fragmentation attack and 800 SYN Flood attack and the other normal data which are transferred to and for the network and form the result of simulation shown in figure (a) Tiny Fragmentation attack was approximately detected 100% and SYN Flood was not detected at all.

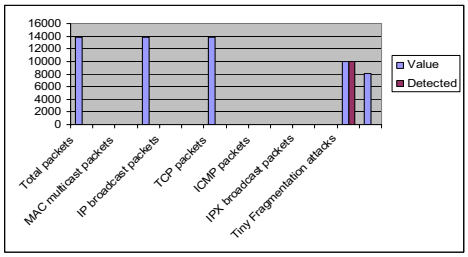

Fig. (a) Tiny fragmentation attack.

and in simulating rule (2) as in rule (1) approximately 11911 information packets were sent to the target computer where 10000 was designated as Overlapping Fragmentation attack and 800 SYN Flood .

The result of simulation as in figure (b) in detected that Overlapping Fragment attack was detected 100% and SYN Flood attack wasn't detected at all.

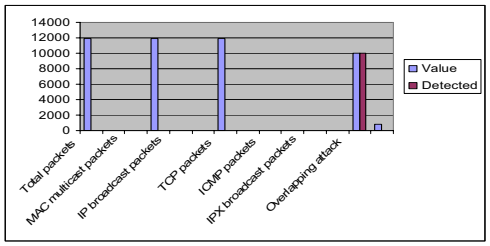

Fig. (b) Overlapping attack.

however, in simulating rule (3) which is especially for manual configuration of information packet in a way that half of the packet is sent and which is no longer normal we sent 33978 Information Packet to the target computer where 10000, are unnamed attacks and 10000 are tiny fragmentation attack, 10000 are overlapping attacks and 800 are information packet attack of SYN Flood, the result shown in figure (d) detected only unnamed attacks and it couldn't detect other attacks .

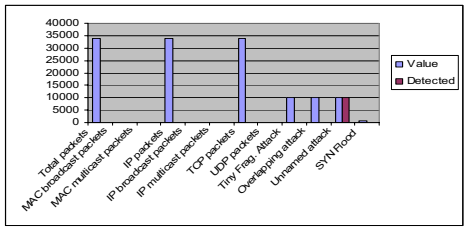

Fig.(d) Rule 3 Unnamed attack.

finally when we synthesized the three rules, we sent the target computer various types of attacks where approximately 32990 information packets was sent which included 10000 Tiny fragmentation attack and 10000 overlapping fragmentation attacks and 10000 unnamed attack and 800 SYN Flood attack .

The result we obtained is illustrated in figure (L) in which approximately all the attacks have been detected 100%.

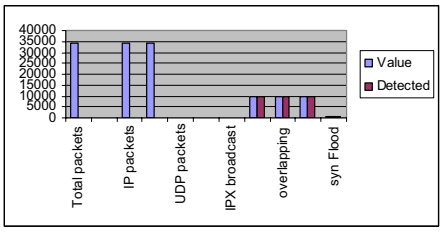

Fig. (L) Synthetic three rules.

TABLE I
COMPARISON OF THE PROPOSED MECHANISM WITH SIMILAR RELATED WORKS

The proposed Detection Mechanism	**Similar Mechanism [19]**
(1)-comparison of rules: Rule (1): they are almost similar. Rule (2): our rule completely detects overlapping attacks. Rule (3): other attacks such unnamed attack are completely detected. (2)- It completely detects synthetic attacks. (3)- detects other attacks like SYN Flood.	**(1)-**comparison of rules: Rule (1): they are almost similar**.** Rule (2): it practically doesn't exist and is limited to setting the router. Rule (3): it doesn't have and it doesn't detect other TCP Fragmentation attacks like Unnamed attack. (2)- it doesn't detect synthetic attacks such as tiny+overlapping . (3)- Its not possible to detect other attacks.

TABLE II
COMPARISON OF PROPOSED MECHANISM WITH NIDS (Snort) MECHANISM

The Proposed Detection Mechanism	**Snort Fragmentation Rules and Reassembling [20,21]**
1- It doesn't require TCP Packet reassembling to detect an attack. 2- It has 100% Fragmentation detection attack. 3- It doesn't detect out of order attacks and there isn't false alarm. 4- The synthetics of the rules which occurs in the module, detects both fragmentation and other attacks.	1- It requires TCP Packet reassembling and since it takes 60 sec. to reassemble it evades the system. 2- Some packet attacks pass through Snort during high network traffic. 3- Some out of order packet get to the target depending on the kind of attack execution. 4- Fragmentation attack rules detect only Fragment attack following reassembling and it is not able to detect other attacks.

V. Conclusion and Future Work

In this paper we investigated the TCP fragmentation attacks which evade the intrusion detection system and a new architecture with our own proposed mechanism (algorithm) was expanded.

The new architecture we presented is a module termed Evasion Detection fitted in to the Intrusion Detection System for further reprocessing of TCP information packet with a view of checking the integrity of the packet itself which currently operates on the TCP Protocol and in future work we will broaden it to other protocol such as UDP and ICMP.

References

[1]- Mark Handley and Vern Paxson ,"Network Intrusion Detection :Evasion Traffic Normalization, and End-to-End Protocol Semantics. In USENIX Security Symposium, Washington,DC August 2001
[2]- InSeon Yoo and Ulrich Ultes-Nitsche,"Towards Run-Time Protocol Anomaly Detection and Verification.2001
[3]- Joel Scambray ,Stuart Mcclure and George Kurtz,"Hacking Exposed:Network Security Secrets &Solutions Second Edition 2002.
[4]-T.H Ptacek and T.N.Newsham. Insersion,evasion,and denial of service:Eluding network intrusion detection. Technical Report T2R-0Y6,secure Netowrk,Inc.,Cagary,al-berta,Canda 1998.
[5]- Jason Anderson,"An Analysis of Fragmentation attacks", March 15, 2001.
[6]- T.H. Ptacek and T.N. Newsham. Custom attack Simulation Language (CASL). Available at www.sockpuppet.org/tqbf/casl.html.
[7]- V.Paxson. Bro: a system for detecting network intruders in real-time. Computer Networks, 31(23/24),December 1999.
[8]- SHai Rubin, Somesh Jha, and Barton P.Miller, "Automatic Generation and Analysis of NIDS Attacks", University of Wisconsin,Madison Computer Sciences Departemnt. 2004
[9]- Ozgur Depren, Murat Topallar, Emin anarim, M.Kemal Ciliz," An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks",Information and Communication Security (BUICS) Lab Bebek ,Istanvul,Turkey 2005.
[10]- Matthew V.Mahoney,"Network Traffic Anomaly Detection Based on Packet Bytes", Florida Instite of Technology,Melbourne, Florida.2002
[11]- Bharat Goyal,Sriranjani Sitaraman,Srinivasan rishnamurthy,"Intrusion detection system: An Overview" Department of Computer Science University of Texas at Dallas.2003
[12]- Network analysis and Porotocl Sniffing .Available at www.networkgeneral.com/Sniffer_Portable_Eval.aspx
[13]- Network sinffer and packet builder available at www.sniff-em.com
[14]-Packet Builder and attack script runner available at http://www.EngageSecurity.com
[15]- IP-tools for attack generator avalible at www.alhacker.com
[16]- Scanning and Fragmentation attack tools available at www.securityfocus.com/download/Nmap/
[17]-D.Song. Fragroute: a TCP/IP Fragmenter, April 2002. Available at www.monkey.org/~dugsong/fragroute.
[18]-MIT University Lab. http://www.ll.mit.edu/IST/ideval/dataset/
[19]- G.Ziemba Alantec ,D.Reed,"Security Consideration For IP Fragment Filtering", Cisco Systems "RFC 1858" October 1995.
[20]-Sumit Siddharth,"Evading NIDS",6-12-2005. available at www.securityfocus.com/infocus/1852.
[21]- Andrew R.Backer ,Brian Caswell ,Mike Poor,"Snort 2.1", Second Edition 2004, Syngress Publisher, Page 248-250.