ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

Network Intrusion Detection System

Niharika Sangani [1], Pravin Nawale[2], Kalpesh Jethwa[3], Chirag Gosalia[4]

Student, BE Computers, K. J. Somaiya College of Engineering, Mumbai, India [1,2,3,4]

Abstract: Network Intrusion Detection is an important technology in business sector as well as in high security zones such as research. It is an effective weapon that provides information security. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take appropriate action. Computers that form networked distributed systems, may span multiple buildings sometimes located thousands of miles apart. The network of such a system is a pathway for communication between the computers in the distributed system. The network is also a pathway for intrusion. This system is designed to detect some common attacks (i.e. SYN Flooding and IP spoofing in this case) on network systems. It follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a signatures or attributes from known malicious threats. It has been implemented in Java with help of JPcap Library. In this system the attack log displays the list of attacks to the administrator for evasive action. This system works as an alert device in the event of attacks directed towards an entire network.

Keywords: NIDS, malicious, legitimate, attacks, signature, SYN flood, IP Spoofing.

I. INTRODUCTION

Since the evolution of the internet, there has been an increasing need for security systems. One important type of security software has been emerged since the evolution of the internet is Intrusion Detection Systems (IDSs). Intrusion detection is defined as the processes to identify the internal or external users who intend to do something unauthorized against the computer system. Intrusion detection also identifies the legal connected users who intend to misuse their privileges. Intrusion detection systems (IDS) are based on the principle that malicious behaviors on computer or network systems will be noticeably different from normal behaviors. IDS can also perform the following tasks.

- Keep an eye on the system and user activities.
- Verification of the system errors.
- Evaluating the integrity of systems and data files.
- Note down any abnormal behavior make statically records.
- Recognition activity model mapping known attacks and alerts.

The main objective of the paper is to focus on Network based Intrusion Detection System. The goal of a Network Intrusion Detection System (NIDS) is to alert a system administrator each time an intruder tries to penetrate the network.

II. NEED

In today’s world, everyone is increasingly dependent on the ability to have instant access to information. The explosion of internet, along with wireless and broadband technologies, allows companies and individuals, unprecedented”Real Time” access to vast amount of information [1]. Network security has been an issue almost since the computers have been networked together.

So in order to provide security at its best we require a system which can detect malicious content and take proper decision. The security is utmost required in banking and insurance sector and the corporate sector where the confidential data needs to be communicated via network.

III. LITERATURE SURVEY

Attacks on the network infrastructures are the big problem of the networks of today’s world, with the swiftly growing illegal activities in the networking world; the network security becomes a big challenge which is neither hopeless nor solved. In early days firewall was sufficient to provide the security to the network but now a days due to tremendous growth of different attacks there is a need of an extra layer of protection besides firewall.

A. Various threat to network security

A Network is defined as a threat, intrusion, denial of service or other attack on a network infrastructure that will analyze the target network and gain information to eventually cause the network to crash or to become corrupted. Unmonitored network devices are the main source of information leakage in organizations. If the attacker is able to "own" the network devices, then they "own" the entire network [6]. Network attacks cut across all categories of software and platform type. There are at least five types of network attacks.

- Spoofing.
- Sniffing.
- Trojans.
- DoS and DDoS.
- Social engineering.

This paper concentrates on two most important attack i.e. Spoofing and SYN flooding which is a part of DoS attack.

B. Types of Intrusion Detection Systems

There are broadly two types of Intrusion Detection systems.

a) Host based Intrusion Detection System (HIDS).
b) Network based Intrusion Detection System (NIDS).

NIDS monitor the whole traffic of the network from which the hosts are connected, it obtains data from them and make their decisions. NIDS is cost effective and gives immediate real time detection of the network attacks so it reduces and decreases the chance of the damages of the network because of the intrusion activities in figure1. Network based sensors apply predefined attack signatures to each frame to identify hostile traffic. If it finds a match against any signature, it notifies the management console.

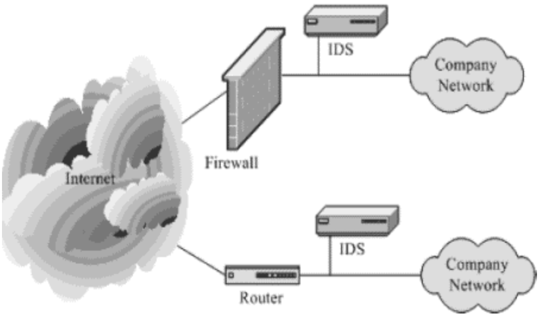


Figure1: IDS setup in a network.

C. Methods and Techniques in Intrusion Detection

Intrusion Detection Systems (IDS) refers to a program used to detect an intrusion when it happens and to prevent a system from being compromised.

- *Anomaly Based Methodology*

Anomaly based methodology works by comparing observed activity against a baseline profile [6]. The baseline profile is the learned normal behavior of the monitored system and is developed during the learning period were the IDS learns the environment and develops a normal profile of the monitored system. The profile can be fixed or dynamic. Anomaly intrusion detection methodology uses three general techniques for detecting anomalies and these are the statistical anomaly detection, Knowledge/data-mining, and machine learning based [6].

- *Signature Based Methodology:*

Signature based methodology works by comparing observed signatures to the signatures on file. This file can be database or a list of known attack signatures. Any signature observed on the monitored environment that matches the signatures on file is flagged as a violation of the security policy or as an attack. The signature based IDPS has little overhead since it does not inspect every activity or network traffic on the monitored environment [6].

- *Stateful Protocol Analysis Based Methodology:*

The Stateful protocol analysis methodology works by comparing established profiles of how protocols should behave against the observed behavior [9]. The established protocol profiles are designed and established by vendors. Unlike the signature based methodology which only compares observed behavior against a list, Stateful protocol analysis has a deep understanding of how the protocols and applications should interact/work.

- *Hybrid Based Methodology:*

The hybrid based methodology works by combining two or more of the other methodologies [9]. The result is a better methodology that takes advantage of the strengths of the combined methodologies [6].

Comparing all the above methodologies, this paper proposes signature based method due to its number of advantages over other such as it has high accuracy rate, scalability, low maintenance, easy to configure and it also has protection against new attacks.

IV. PROPOSED SYSTEM

Paper focuses on the Spoofing and SYN flooding attack and suggests the counter measures to detect them.

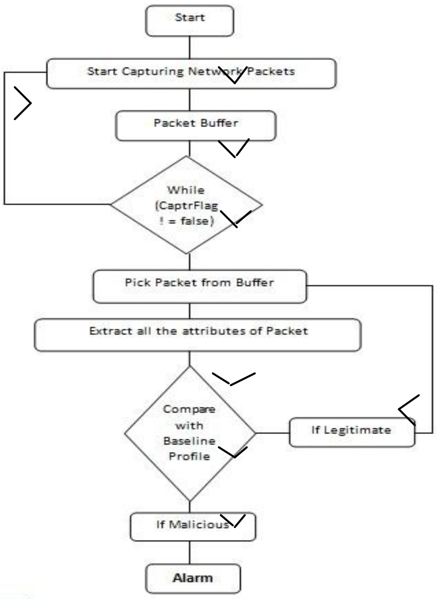

Start
Start Capturing Network Packets
Packet Buffer
While (CaptrFlag ! = false)
Pick Packet from Buffer
Extract all the attributes of Packet
Compare with Baseline Profile
If Legitimate
If Malicious
Alarm

Figure2: Flowchart of NIDS execution.

As shown in figure2 the execution initially starts capturing packets that are coming from the network. It stores all these packets in packet buffer. The system continues capturing the upcoming packets until the process is stopped. It goes in an infinite loop if not stopped. Once the packet capturing is stopped, it analysis each and every packet in the buffer and access all the attributes of packet. Then these attributes are compared with the baseline profile to determine whether the signature is available in database, if the attributes of incoming packet and stored signature is matched it is a malicious packet and thus the user must be alarmed. If it is legitimate analyze other packet queued in buffer.

D. IP Spoofing

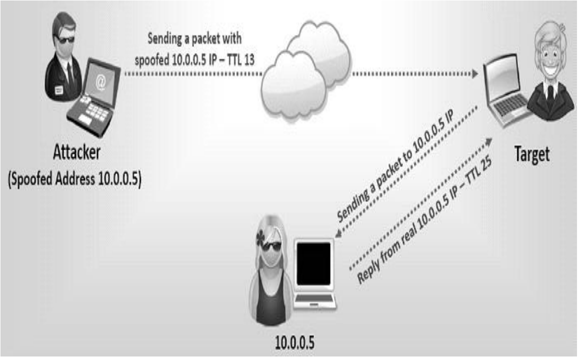

Sending a packet with spoofed 10.0.0.5 IP – TTL 13
Attacker
(Spoofed Address 10.0.0.5)
Target
Sending a packet to 10.0.0.5 IP
Reply from real 10.0.0.5 IP – TTL 25
10.0.0.5

Figure3: IP Spoofing attack

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

Any internet connected device necessarily sends IP datagram's into the network. Such internet data packets carry the sender's IP address as well as application-layer data. If the attacker obtains control over the software running on a network device, they can then easily modify the device's protocols to place an arbitrary IP address into the data packet's source address field. This is known as IP spoofing, which makes any payload appear to come from any source [4]. With a spoofed source IP address on a datagram, it is difficult to find the host that actually sent the datagram.

The countermeasure for spoofing is ingress filtering. Routers usually perform this. Routers that perform ingress filtering check the IP address of incoming datagrams and determine whether the source addresses that are known to be reachable via that interface. If the source addresses that are known to be reachable via that interface. If the source address is not in the valid range, then such packets will be discarded.

- ***IP Spoofing Detection Algorithm***

The IP spoofing detection mechanism which will first identify if the packet is malicious or not and if found malicious it will then try to identify the true source of the IP packet from where the packet has originated. IP packet header fields – the TTL and the ID field of the packet will be used to help find the attack source. The TTL of an IP header is a record of how many routers the packet has traversed and the ID is a serial number that is used in de-fragmentation.

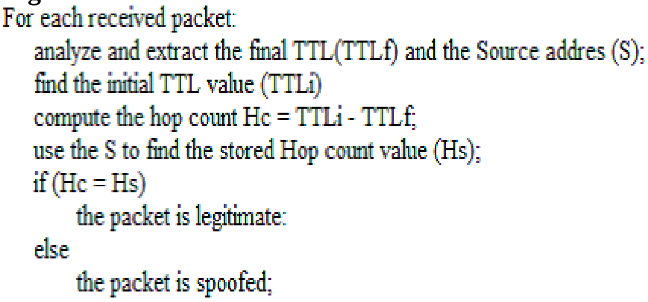
Detection Mechanism based on TTL

One most common attack based on IP spoofing is DDoS attack. Such attack is initiated when the attacker compromise various botnets using some malicious way [4]. These compromised hosts then spoof the attack packet by inserting some random IP address in the source address field of the IP packet. This detection mechanism keeps track of the packet flow information embedded in the IP header. TTL is a 8 bit field in IP header determines the maximum lifespan of an IP packet. As the IP packet transit through the network each intermediate node decrements the TTL value by one before forwarding it to the next node. Hence, this mechanism uses the number of Hop the packet travelled to detect if the packet is legitimate or not. This information is obtained by subtracting the final TTL with the initial TTL value. This hop count value is then compared with the stored hop count corresponding to the source address. In Static Approach the hop count for particular IP is stored in the form of HOP COUNT required to reach the same IP. If both the values (stored hop count and calculated hop count) are same then the packet is legitimate or the packet is malicious. But this method has some limitations that it requires pre knowledge of hop count for any IP. So this method is not that much efficient. In Dynamic Approach the actual hop count for any IP is calculated by using trace route mechanism and then it is compared with the HOP COUNT received with IP. This received HOP COUNT is calculated as,

Hop Count = (Basic TTL - TTL Value of IP)

Here Basic TTL value is predefined for the particular Operating system. If both the values (Hop Count and Actual Hop count) are same then the packet is legitimate or the packet is malicious.

Algorithm



```
For each received packet:
    analyze and extract the final TTL(TTLf) and the Source addres (S);
    find the initial TTL value (TTLi)
    compute the hop count Hc = TTLi - TTLf;
    use the S to find the stored Hop count value (Hs);
    if (Hc = Hs)
        the packet is legitimate:
    else
        the packet is spoofed;
```

E. SYN Floods

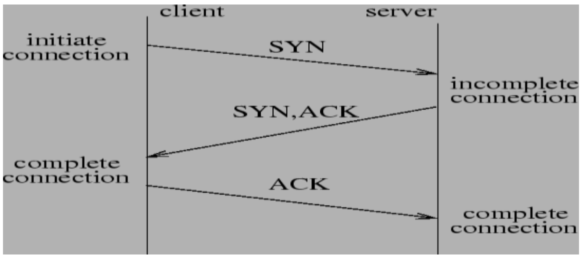


Figure 4: 3 way handshake protocol.

When a computer wants to make a TCP/IP connection to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer, sends a TCP/SYN packet which asks the server if it can connect. If the server is ready, it sends a TCP/SYN-ACK packet back to the client to say "Yes, you may connect" and reserves a space for the connection, waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client is often forged so that when the server sends a TCP/SYN-ACK packet back to the client, the message is never received from client because the client either doesn't exist or wasn't expecting the packet and subsequently ignores it. This leaves the server with a dead connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which keeps legitimate clients from making connections.

- ***SYN flooding single feature detection***

The proposed system maintains the state information of clients in network. It keeps track of the TCP SYN request packet [10]. And increments counter whenever there is SYN request. When connection is successfully established that is 3-way handshake is completed it decrements the counter value. SYN request packets are buffered for some time in system.

Buffer Threshold value:

Windows System	150
Linux	120
Unix	130

The timeout period for pending SYN request is 0.5 in windows system. When pending request counter exceeds this threshold value within this timeout period it indicates flooding attack. The system will alarm the victim system.

V. ADVANTAGES

- The system will detect the TCP SYN flooding and IP spoofing attack.
- It will alarm the user when attack is detected.
- It will capture incoming packet and display the content for analyses.
- It is efficient and less resource hungry.

VI. DISADVANTAGES

- The system requires more computation power.
- IP Spoofing algorithm is unable to detect internal network threat.
- It is not learning system.

VII. CONCLUSION

The proposed system can be used in sector where there is intensive need for security. NIDS are becoming the logical next step for many organizations after deploying firewall technology at the network perimeter. NIDS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. Some points are very important to always keep in mind. If all of these points are not adhered to, NIDS implementation along with a firewall alone cannot make a highly secured infrastructure.

ACKNOWLEDGMENT

The proposed system would not have been possible without the guidance of Prof. Swati Mali. Her inputs during the period of research and project development were highly valuable and helpful.

REFERENCES

[1] “Intrusion Detection System for detecting network threats and vulnerabilities,” paper published in 2004 by LEE YEW LOON

[2] Efficient Computer Network Anomaly Detection by change point detection methods. Alexander G. Tartakovsky, Senior member, IEEE, Aleksey S. Polunchenko, and Grigory Sokoloy.

[3] Analysis and Application of Wireshark in TCP/IP Protocol Teaching 2010 International Conference on E- Health Networking, Digital Ecosystems and Technologies.

[4] Intrusion Detection System with Packet Filtering for IP Spoofing. Manusankar, Karthik, Rajendran. Proceedings of the International Conference on Communication and Computational Intelligence – 2010, Kongu Engineering College, Perundurai Erode, T.N.India 27-29 December,2010.pp.563-567

[5] SACK2: effective SYN flood detection against skillful spoofs. C. Sun1 C. Hu2 B. Liu3 1IBM China Research Lab, Beijing, People’s Republic of China 2MOE KLINNS Laboratory, School of Electronic and Information Engineering, Xi’an Jiaotong University, Xi’an, Shaanxi People’s Republic of China 3Department of Computer Science and Technology, Tsinghua University, Beijing, People’s Republic of China

[6] NETWORK INTRUSION DETECTION AND PREVENTION ATTACKS Harpreet Kaur C.Sc. Dept. S.R.Govt. College (W), Amritsar, June 2012

[7] Bottleneck Analysis of Traffic Monitoring using Wireshark. Abes Dabir Ashraf Matrawy Department of Systems and Computer Engineering, Carleton University, Canada fadabir, amatrawy @sce. carleton.ca

[8] An Accurate Sampling Scheme for Detecting SYN Flooding Attacks and Port scans. Maciej Korczy´nski∗ Lucjan Janowski† and Andrzej Duda Grenoble Informatics Laboratory, Grenoble Institute of Technology, Grenoble, France AGH University of Science and Technology, Cracow, Poland IEEE ICC 2011.

[9] A study of Methodologies used in Intrusion Detection and Prevention Systems (IDPS), IEEE 2012.

[10] A Comparison of SYN Flood Detection Algorithms.