Volume 4, Issue 5, May 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Intrusion Detection and Prevention System Using JPCAP/WINPCAP

Archana D Wankhade*
Department of Information Technology
Government College of Engineering,
Amravati,(M.S),India

Dr. P. N.Chatur
Department of Computer Science and Engineering
Government College of Engineering,
Amravati ,(M.S),India

Abstract— Network Intrusion Detection Systems that capture data packets travelling on the network media (cables, wireless) and match them to a database of signatures. Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database. Network Behaviour Analysis (NBA), which examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, certain forms of malware (e.g., worms, backdoors), and policy violations (e.g., a client system providing network services to other systems). NBA systems are most often deployed to monitor flows on an organization's internal networks, and are also sometimes deployed where they can monitor flows between an organization's networks and external networks (e.g., the Internet, business partners' networks). intrusion detection systems and intrusion prevention systems are combined. And network administrator can view the log file generated by the application for viewing the attacks information. Packet logger is also implemented So that to observe the flow that captured packets are stored in the file.

Keywords— TCP, UDP, ICMP, IPSpoofing, NBA

I. INTRODUCTION

Introduction for implementation of Intrusion Detection and Prevention System Using Jpcap/Winpcap. An Intrusion Detection System (abbreviated as IDS) is a defence system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including data collection phases that involve for example, port scans. Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. one key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and block a suspected connection. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the thread posed by hackers)[1]. Intrusion is a series of concatenated activities that pose threat to the safety of IT resources from unauthorized access to a specific computer or address domain. Incident is a violation of the system security policy rules that may be identified as a successful intrusion. Attack is a failed attempt to enter the system (no violation committed). Modelling of intrusions is a time-based modelling of activities that compose an intrusion. The intruder starts his attack with an introductory action followed by auxiliary ones to proceed to successful access; in practice, any attempts undertaken during the attack by any person, for example by the IT resource manager can be identified as a threat. An intrusion can be defined (Heady et al., 1990) as "any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource", for example, illegally gaining super user privileges, attacking and rendering a system out of service (i.e., denial-of-service), etc. Intrusion Prevention System IPS technologies are differentiated from IDS technologies by one characteristic: IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. Intrusion prevention techniques, such as user authentication (e.g. using passwords or biometrics), avoiding programming errors, and information protection (e.g., encryption) have been used to protect computer systems as a first line of defence [2]. Motivation: Due to a growing number of intrusions and since the Internet and local networks have become so ubiquitous, organizations increasingly implementing various systems that monitor IT security breaches. Intrusion Detection Systems (IDS) are those that have recently gained a considerable amount of interest. It gives an overview of several types of detectable attacks, symptoms that help in intrusion detection, describes IDS tasks, different architectures and concepts in this field. An Intrusion Detection System (abbreviated as IDS) is a defence system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including data collection phases that involve for example, port scans. One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. According to Amoroso, intrusion detection is "a process of identifying and responding to malicious activity targeted at computing and networking resources". In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the thread posed by hackers).

Objective: Since now a days almost all the work is done through the internet communication. Whenever there is a large network or small network. Its security is the big problem. So to provide the network security as well as the individual host security different attack detection and prevention tools are used. There are many attacks possible on the network. Form that attacks some are known attacks and some are new to the system. Since intrusion detection systems deal with hacking breaches. There are many dangerous activities can going on the network. The data which is important for an enterprise should be kept securely.

Theme: Design and implementation of Robust Campus Wide Network Defender (RCWND) is the system uses hybrid approach for detection and prevention of the Network attacks. It uses signature based and anomaly based approach. Mainly Network attacks are DoS Denial of Service attack, Syn-flood attack, TCP packet attacks, UDP packet attacks, ICMP packet attacks.

II. PERFORMANCE ANALYSIS

This chapter deals with the setting up the environment for implementing the system. User Interface screen shows how the user will interact with the system and the data entry forms required to gather data for the system. The screen shots are also shown in this chapter. To give the reality of the design we have done for the proposed system, we have implemented it using Java, specifically we used JPCAP. Implementing the system involves, writing the code in specific programming language for generating the Graphical User Interface, authorizing the user, gathering the data from user, creating tables required to store the data, inserting the data into the tables, retrieving the required data from the tables. This chapter mainly deals with the user interface design as the user is the main acting entity for the system. The user interface design creates an effective communication medium between a human and a computer. The user interface design process encompasses the four distinct framework activities: User, task and environment analysis, Interface design, Interface construction and Interface validation. Each of the tasks can occur more than once with each occurrence representing additional elaboration of requirements and the resultant design. The implementation activity normally begins with the creation of a prototype that enables usage scenarios to be evaluated. As an iterative design process continues, a user interface tool kit may be used to complete the construction of the interface. Validation is also a part of the implementation. The validation focuses on: The ability of the interface to implement every task correctly, to accommodate all task variations and to achieve all general user requirements The degree to which the interface is easy to use and easy to learn The users' acceptance of the interface as a useful tool in their work.

Computational Analysis: The Robust Campus Wide Network Defender System contains three modules ,Packet Display GUI module, Detection module, Prevention module .Packet Display GUI module :This module gives the graphical user interface for interacting with the system. The captured packets are displayed in the table format within the frame. To implement the packetDisplayGUI in table JTable is used from java swing. Packet DisplayGUI unit ask user to select the interface and mode for capturing the packets. Mode Selection module: There are two modes available Promiscuous Mode, Inline mode, It allow user to select the mode.

Packet Filter Module: The packet Filter module allow user to select the filter for capturing the packets. This module captures the specified packets only if other that 1st option is selected. If the 1st option is selected then all type of packets are captured by the System.

Detection module: The detection module uses the algorithms which are explained above in the designing of RCWND system. Using that algorithm it checks the incoming and outgoing packets for attack.

Prevention module:The prevention module execute the rules for dropping the packets which are malicious. The system requires to run on windows. The rules which should be executed on detection of attack are explained above in design of the system. So it uses the WIPFW that is windows ipfw is based on ipfw of BSD. This firewall is same as the IPTABLE which runs on Linux, UNIX.

III. EXPERIMENTAL ANALYSIS: EXECUTION OUTPUT

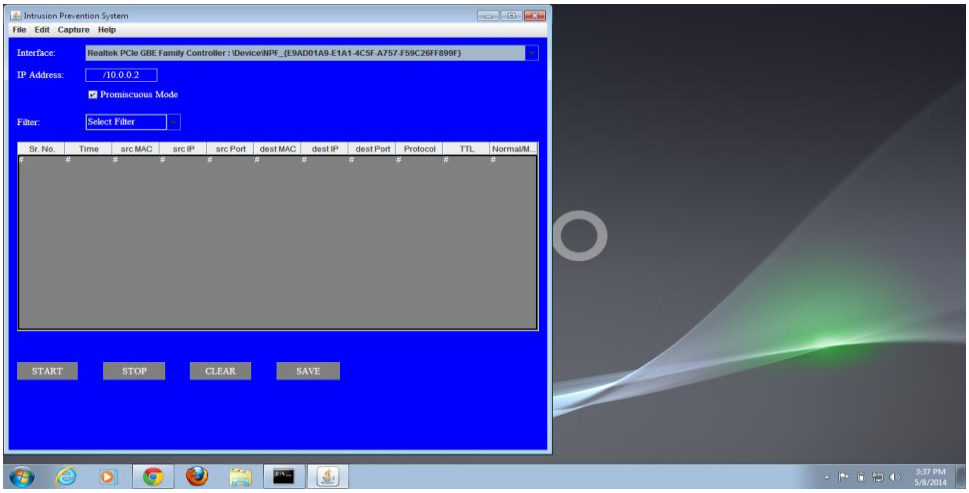

Figure 3.1 Screen shot for Intrusion Protection System

Figure shows the result after analysing the packets by IDS and IPS components. Here in the above figure the user select the interface. IP address of that interface is shown in IP address field. Next the user selects the mode (Promiscuous mode/inline mode). After specifying the mode for capturing the packet application open the interface and set the filter for capturing the packets and starts capturing packets. Here all the captured packets are Normal. The Start button allows user to start monitoring the packet flow. The stop button Stops capturing packets. The clear button allows user to clear the table contents. The Save button allows user to save all the captured packets in the file.

Experimental Results for different examples

Screen Shot for TCP Traffic

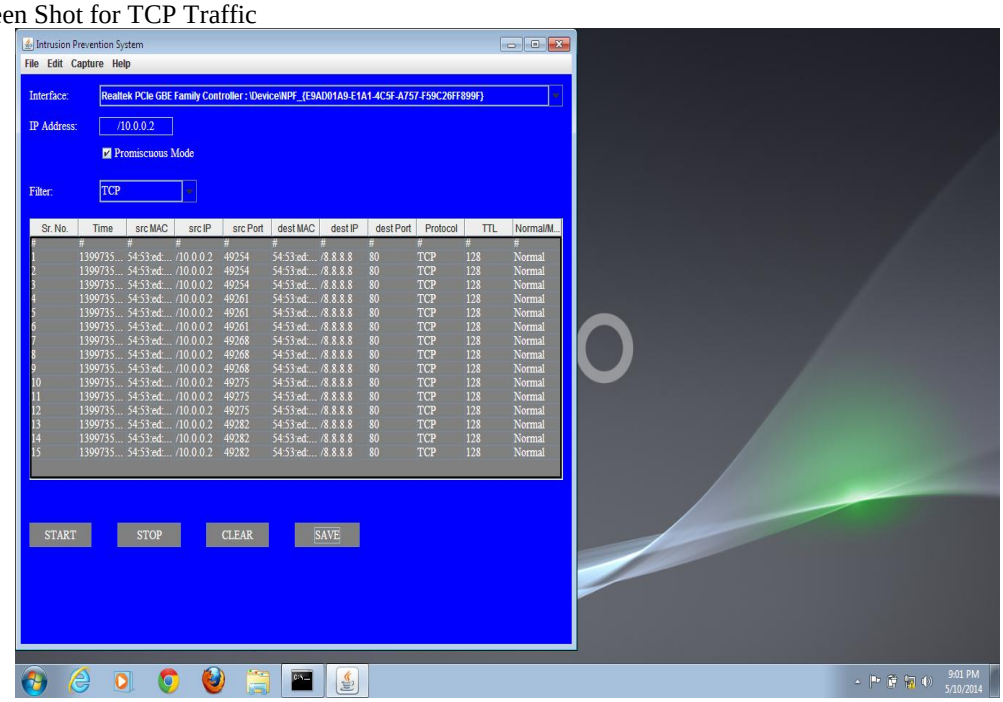

Figure 3.2 Screen shots for TCP traffic

In the above figure the normal packets for TCP traffic are captured. The last column shows packet status. That is captured packets are Normal or Malicious.

Screen Shot for UDP Traffic

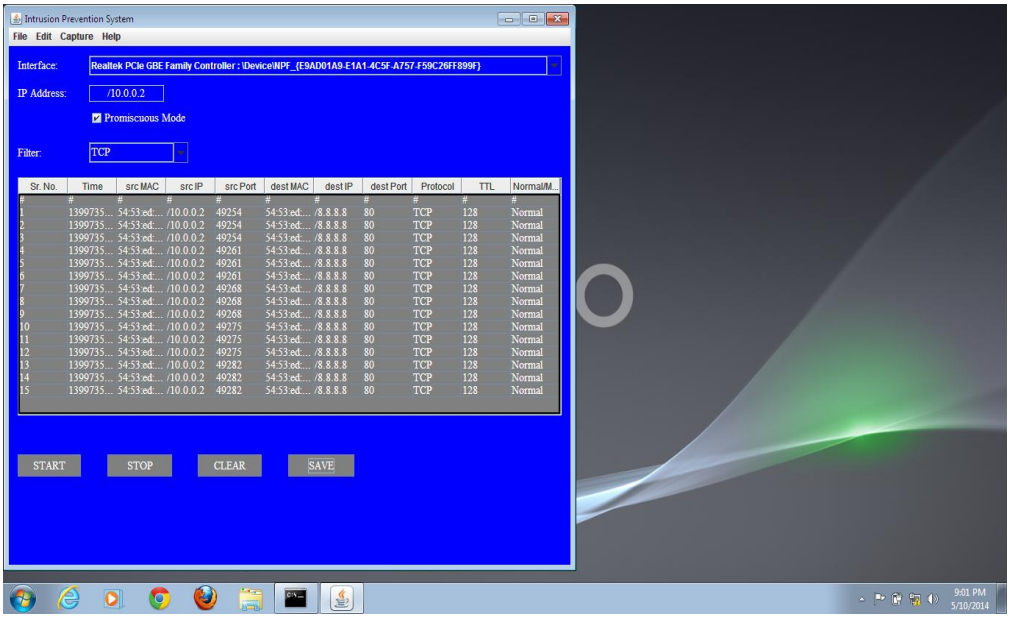

Figure 3.3 Screen Shot for UDP traffic

In the above figure the normal packets for UDP traffic are captured. The last column shows packet status. That is captured packets are Normal or Malicious.

Comparison between Computational and Experimental Analysis

Testing for Performance

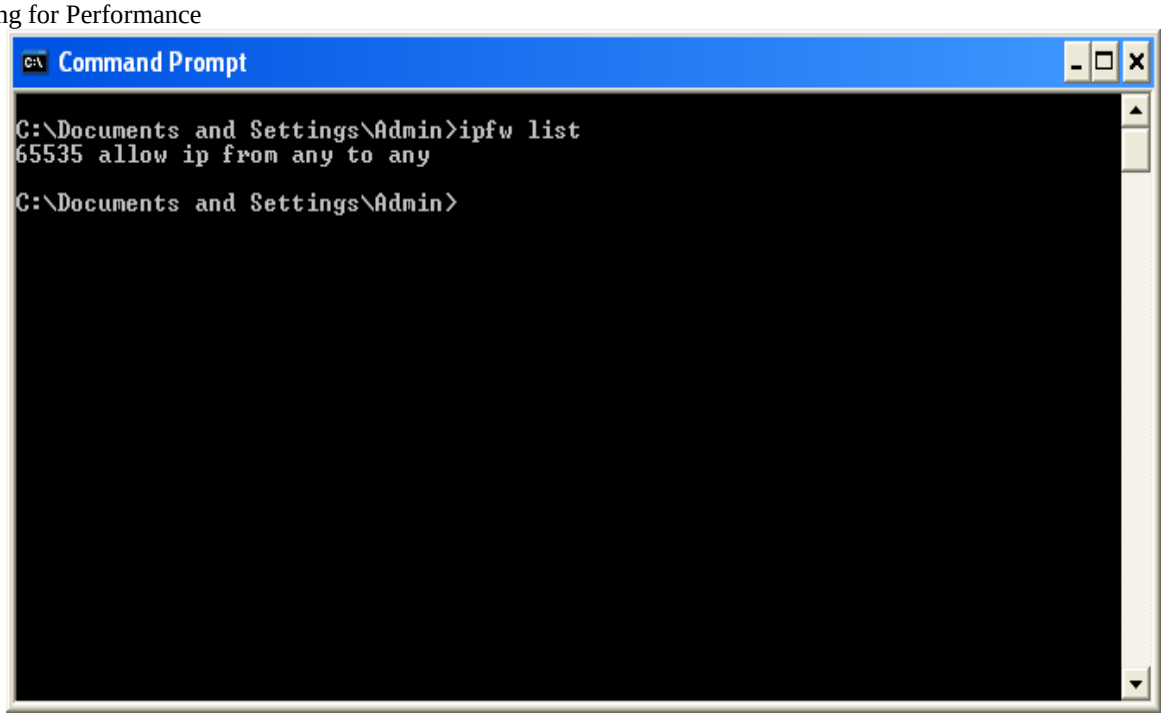

Figure 3.4 IPFW rule Table before updating

Figure shows the list of rules present in the ipfw rule table. *Ipfw list* command gives the list of rules added in the rule table.

Comparison of Results

UDP fraggle attack detection

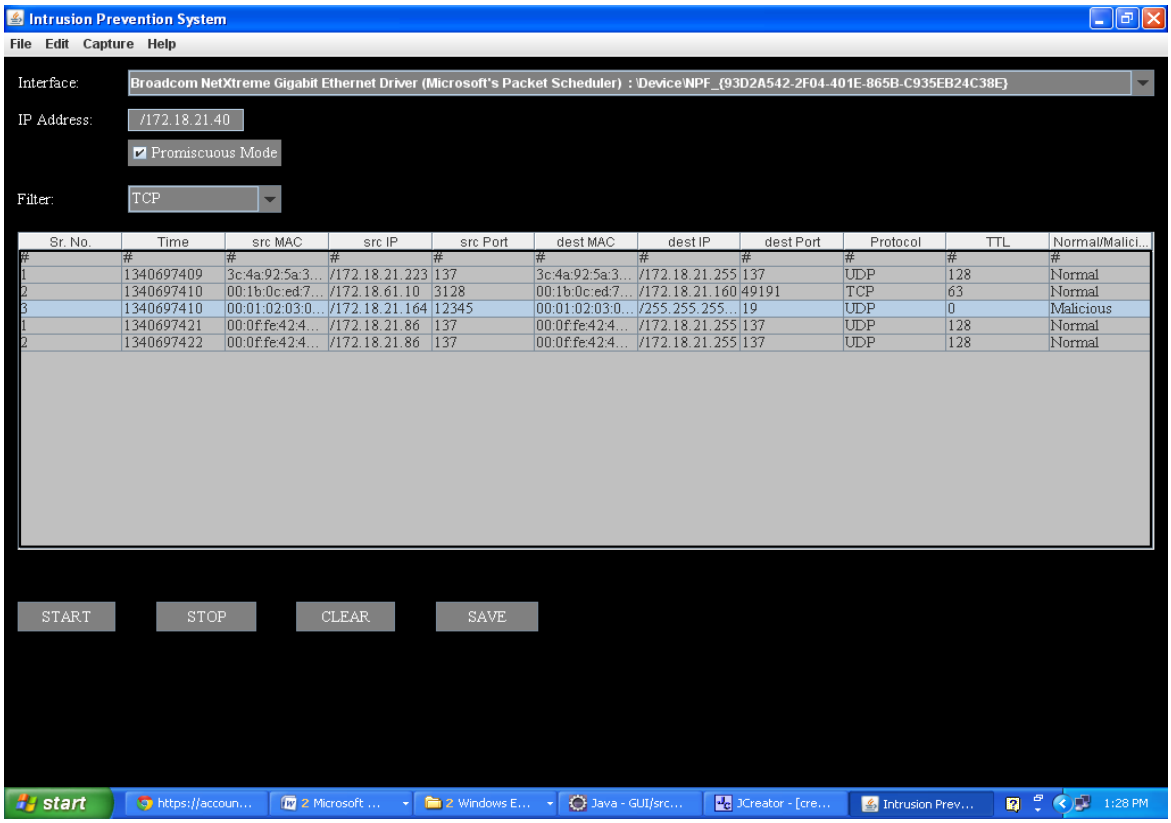

Figure 3.5 Screen shot for fraggle attack

Figure shows the output of UDP fraggle attack detection.The highlighted row shows the UDP packet Dest_address is 255.255.255.255. IDS checks the UDP dst_address and port. If the dest_address is broadcast address and the port is 7 or 19 then UDP echo fraggle attack is detected and IPS executes the rule prevent the packet filtering of those attacks.

Updated Ipfw rules table for UDP fraggle attack

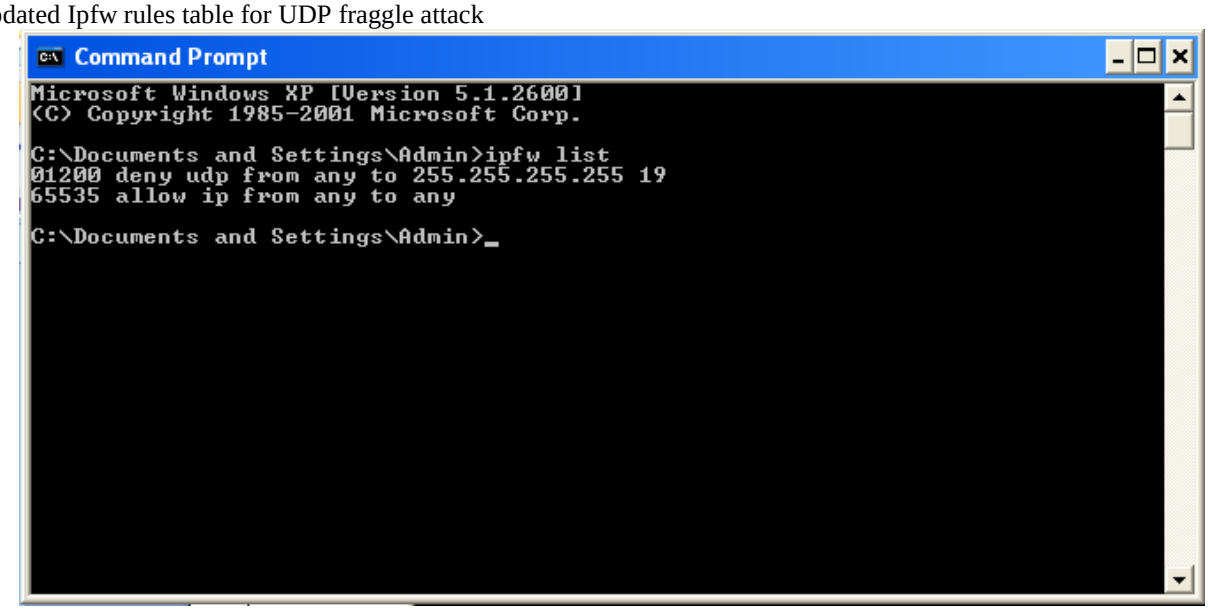

Figure 3.6 After adding rules in IPFW rules table

The above figure shows list of ipfw rules. When the UDP fraggle attack is detected the IDS component returns true. If the result of IDS unit is true then IPS unit performs the action on it. The IPS unit executes the command which add the rule in to ipfw rule table.

Generated log file for UDP packet

1340697237703##---Retrieving Blacklist---

1340697237734##Total No of blacklisted IPs : 3
1340697237734##BlackList:-
1340697237734##IP : 10.0.0.1 Added at : 1338360524156
1340697237734##IP : 10.0.0.2Added at : 1338360524156
1340697237734##IP : 10.0.0.1 Added at : 1338801651093
1340697237734##Blacklist retrieved successfully
1340697241515##-----start capturing the from-----
1340697418328##-----start capturing the from-----

The log file output is as shown above. Above circled part in the log file shows when the attack is detected and IP address in that packet also IPS action taken on that attack. The network administrator gets the blacklistedIP addresses from BlacklistedIP.XML file. Justification: A ruleset is a group of IPFW rules coded to allow or deny packets based on the values contained in the packet. The bi-directional exchange of packets between hosts comprises a session conversation. The firewall ruleset processes both the packets arriving from the public Internet, as well as the packets originating from the system as a response to them. Each TCP/IP service (i.e.: telnet, www, mail, etc.) is predefined by its protocol and privileged (listening) port. Packets destined for a specific service, originate from the source address using an unprivileged (high order) port and target the specific service port on the destination address. All the above parameters (i.e., ports and addresses) can be used as selection criteria to create rules which will pass or block services. When a packet enters the firewall it is compared against the first rule in the ruleset and progresses one rule at a time moving from top to bottom of the set in ascending rule number sequence order. When the packet matches the selection parameters of a rule, the rules' action field value is executed and the search of the ruleset terminates for that packet. This is referred to as "the first match wins" search method. If the packet does not match any of the rules, it gets caught by the mandatory IPFW default rule, number 65535 which denies all packets and discards them without any reply back to the originating destination.

IV. CONCLUSIONS

The intrusion detection and prevention systems is multilayer system. In the system for IP spoofing TTL value is used to detect the spoofed IP in the packet. . For IP spoofing we use hope count parameter for detection because it is difficult to change TTL value. DDOS attacks are quite advanced methods of attacking a network system to make it unusable to legitimate network users. These attacks are an annoyance at a minimum, and if they are against a critical system, they can be severely damaging. Loss of network resources costs money, delays work, and cuts off communication between network users. IP spoofing is use for hiding information, so host think that packets are coming from a legitimate user whereas it comes from attacker. When both attack taken place together than it is difficult to detect as well as prevent from this attacks. The negative effects of DDOS and IP Spoofing attack make it important that solutions and security measures be developed to prevent these types of attacks.

Future Scope: This application is just a small step towards tackling the attack and a lot more needs to be done. Some of the features that may be added to this application in order to make it more useful are: Deep Packet Inspection can be implemented So that if the packet contains any malicious code or data then that can be identified. Statistics of the

received, dropped packets, blocked ip addresses, types of attacks, number of attacks etc can be shown.Statistical information can be shown in graphical format by using graph. Like in SAX-2 all the packet information Statistical data is shown using graphs. Various trace back methodologies can be implemented. Various trace back techniques like messaging, packet marking, and logging can be used. The system can be extended by incorporating Data Mining.The present system only prevents the known attacks. This can be extended by incorporating Intelligence into it in order to gain knowledge by itself by analysing the growing traffic and learning new Intrusion patterns. Techniques to analyse the information in the log records which may help in efficient decision making.

Applications: In enterprise networks it work as a defence mechanism. Network-based approaches can defend the machine against attack, as detection occurs before the data arrive at the machine. In enterprise networks , network-based approaches can detect the so-called "distributed" intrusions over the whole network and thus lighten the burden on each individual host machine for detecting intrusions.

References

1. Carl Endorf,Eugene Schultz and Jim Mellander,"Intrusion Detection and Prevention", McGraw-Hill,2004.
2. W.Li,"A Generic Algorithm Approach to Network Intrusion Detection",SANS Institute,USA,2004.
3. Atul Kahate, "Cryptography and Network Security" ,Second Edition ,Tata,McGraw Hill Education Pvt Ltd. In 2012.
4. Bernard Menezes, "Network Security and Cryptography",Cengage Learning India Pvt.Ltd.2010.
5. Behrouz A.Forouzan,"TCP/IP Protocal Suite",Tata McGraw-Hill Publishing Company Limited,2000.
6. D.Chapman and E. Zwicky,"Building Internet Firewalls" ,Second Edition,Orielly and Association Inc.,2000.
7. B.Khan,K.K. Muhammad,M.Maqsood and A.S. Khaled, "Security Analysis of Firewall Rule Sets in Computer Networks,",2010.
8. H.Hazem and E.Adel,"On Dynamic Optimization of Packet Matching in High-Speed Firewalls" ,in 2006.
9. William R. Cheswick,Steven M. Bellovin,Aviel D. Rubin"Firewalls and Internet Security",Second Edition ,Pearson Education.
10. Koch.R..Face of Computer Science University under Bundeswehr Munchen,Neubiberg,Germany, "Architecture for Evaluating and correlating NIDS in real World networks" ,June 2013,ISSN:2325-5366 ,pp1-20.
11. Indraneel Mukhopadhyay,Mohuya Chakraborty,Satyajit Chkrabati,"A Comparative Study of Related Technologies of Intrusion Detection and Prevetion System" ,Journal of Information Security ,Scientific Research,January-,2011,pp28-38.
12. Deris Stiawan,Abdul Hana Abdullah,Mohod.Tazid Idris " Characterizing Network Intrusion Prevention System" International Journal of Computer Application",ISSN:0975-8887,January 2011,pp.11-18.
13. Z.D.Elizabeth,C.Simon and C.Brent,Building Internet Firewalls,http://www.oreilly.com,Ed.O'Reilly and Associates,2000.
14. JPCAP online tutorial
15. Java online Tutorial

