ISSN: 2321-8169
805 – 810

Network Based Intrusion Detection Using Honey pot Deception

Dr.K.V.Kulhalli, S.R.Khot

Department of Electronics and Communication Engineering
D.Y.Patil College of Engg.& technology, Kolhapur ,Maharashtra ,India.
kvkulhalli@gmail.com , srkhot08@gmail.com

Abstract- The Main purpose of this paper is to design, implement and evaluate a strong Intrusion Detection System (IDS) using Honey pot Deception, which is a Network based IDS (NBIDS). The system is deployed on the point of (server) network, from where it can monitor all the incoming traffic. It works as IDS for all the clients that are connected to the server. This IDS detects both types of attacks like Anomaly based Intrusion Detection and Rule based Intrusion Detection system. First of all the System captures the packets from incoming traffic analyzes it and collects the information about the packet. Once the Intruder is detected it is sent to honey pot. Honey pot blocks the attacker from the network without knowing the Intruder. It collects the information about the Intruder and study the attacking patterns of the intruder The modules of Anomaly based intrusion detection and Rule based intrusion detection are implemented and results are discussed.

***Keywords** - Intrusion Detection, Honey Pot, Packet Analyzer, Legitimate Traffic, Attack patterns.*

*****

I. Introduction

Advances in computer and communications technology have made the network ubiquitous, and have rendered networked systems vulnerable to malicious attacks orchestrated from a distance. The growing number of computer security incidents on the Internet has reflected that the computer systems are vulnerable to attacks. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

Network Based Intrusion Detection System (NBIDS) is an independent platform that identifies intrusions by examining network traffic and monitors multiple hosts. NIDS gain access to network traffic by connecting to a network hub. Host-based intrusion detection system (HIDS) consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability databases, Access control lists, etc.) and other host activities .Stack-based intrusion detection system (SIDS) consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode. This fact makes its implementation to be dependent on the Operating System that is being used.

Anomaly Based IDS detects computer intrusions and its misuse by monitoring system activity and classifies it as either normal or anomalous, based on heuristics or rules, rather than patterns or signatures. This will detect any type of misuse that falls out of normal system operation. This is as opposed to signature based systems which can only detect attacks for which a signature has previously been created. The Artificial Neural Networks can efficiently and effectively used to recognize what attack traffic is and normal system activity. Also another method known as strict anomaly detection is used to define the normal usage of the system, by using a strict mathematical model, and the flag to indicate any deviation.

Rule Based IDS detects intrusions on a network by storing signature profiles and identifying patterns associated with network intrusions in a signature database and then generating classification rules based on the signature profiles. Data packets transmitted on the network and having corresponding classification rules are classified according to generated classification rules. Classified packets are forwarded to a signature engine for comparison with signature profiles. Signature based IDS monitors' packets in the Network and compares with pre-configured and pre-determined attack patterns known as signatures. The issue is that there will be lag between the new threat discovered and Signature being applied in IDS for detecting the threat. During this lag time your IDS will be unable to identify the threat.

A honeypot is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. It consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. Honeypot can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypot may be classified as, Production Honey Pot (PHP) and Research Honey Pot (RHP)

PHP are easy to use, capture only limited information, and are used primarily by companies or corporations. These are placed inside the production network with other production servers in an organization to improve their overall state of security. Normally, PHP are low-interaction honeypot, which are easier to deploy. They give less information about the attacks or attackers than research honeypot do. The purpose of a PHP is to help mitigate risk in an organization. The honeypot adds value to the security measures of an organization.

RHP is run by a volunteer, non-profit research organization or an educational institution to gather information about the motives and tactics of the Black hat community targeting different networks. These honeypot do not add direct value to a specific organization instead, they are used to research the threats of an organizations face and to learn how to better protect against those threats. RHP is complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

The goal of this paper is to develop a user friendly, cost effective system with features such as to detect intrusions in the system using specified rules and some anomalies, it should run continuously with minimal human supervision, it also should impose a minimal overhead on the network where it is running to distinguish the difference between normal and abnormal traffic. The Use of honeypot deception is considered so that attacker should not know he is being traced and his attack has failed.

II *System Working*

2.1 Schematic of NBIIDS System

Fig1 indicates Network Based Integrated Intrusion Detection System (NBIIDS) which is designed and implemented .The goal is to create a system which is capable of interactively detect the attacks and turn them into the honeypot. This system can detect both the Anomaly based attacks and rule based attacks. The server of the LAN keeps watch on entire network and it detects the intrusion throughout the network, if server finds any intruder it blocks the intruder from remaining network and turns it into the honeypot without knowing the intruder. Honeypot will collect all the information about the intruder.

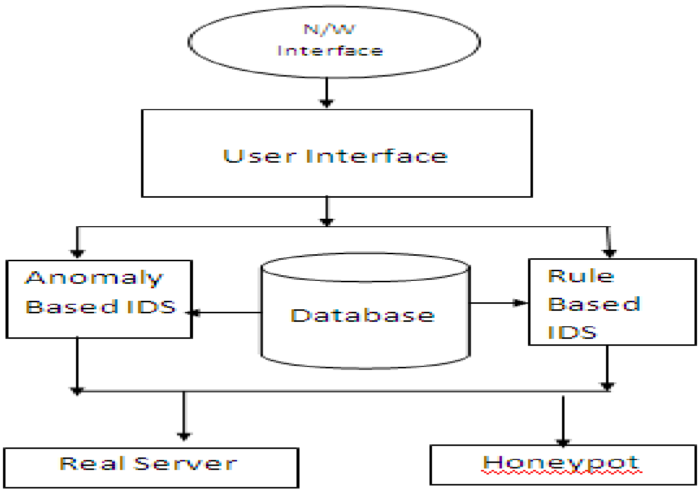


Fig1 Block Schematic of the NBIIDS system

The 10/100 MBPs Ethernet, modems, or Wireless network connection can be used as network interface to the system. The user interface shows dropdown list to select the input and gives two buttons to start or stop the intrusion detection, it also gives the facility to do Conference chat with LAN users..

In NBIDS the user interface creates the socket and listen continuously for the incoming data after selecting the particular network interface it passes the object to Jpcap.captor(), Jpcap.captor() captures the packet and send it to Packet Analyzer(PA). PA opens the packet and collects information about packet. It collects information about Source IP address, Source Port, Destination IP address, Destination port, Packet type, Packet length, Packet data, Packet analyzer and sends this information to intrusion detection module, where it classifies the packets into packet type and stores the information into database..Anomaly based detection module and rule based detection module retrieves this data from database and detects the Intruder.

Once the intrusion is detected the intruders IP is blocked and turned into the Honeypot then honeypot collects the information about Intruder.

2.2 Anomaly-based Detection Module (ABDM)

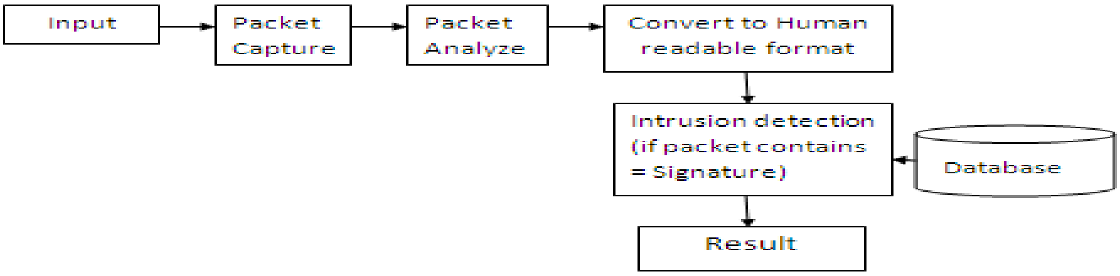

Input
Packet Capture
Packet Analyze
Convert to Human readable format
Intrusion detection (if packet contains = Signature)
Database
Result

Fig2 Anomaly-based Detection Module

In ABDS packets are captured when the data packets cross a computer network. Deep packet capture (DPC) is the act of capturing, at full network speed, complete network packets (header and payload) crossing a network with a high traffic rate. Once captured and stored, either in short-term memory or long-term storage, software tools can perform Deep packet inspection (DPI) to review network packet data, perform forensics analysis to uncover the root cause of network problems, identify security threats, and ensure data communications and network usage complies with outlined policy. Some DPCs can be coupled with DPI and can as a result manage, inspect, and analyze all network traffic in real-time at wire speeds while keeping a historical archive of all network traffic for further analysis

2.1 Rule based Detection Module

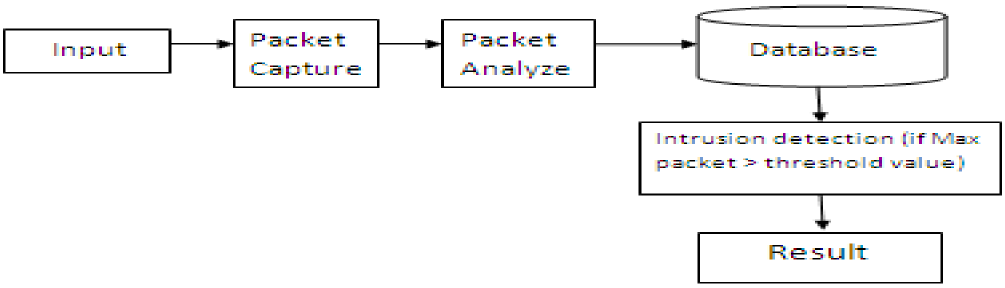


Fig 3 Rule based Detection Module

From the output of network interface the every packet that crosses the network segment is captured. After capturing the packets they are analyzed using packet analyzer (also known as a network analyzer, protocol analyzer, or sniffer, or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network . There are viruses which have particular pattern in their data field. These patterns are matched with data contents of the packets.

III System Design and Implementation

The presented NBIIDS uses Rule-based and Anomaly-based intrusion detection technique. The Honeypot deception technique is implemented in this ID, so as to detect the intrusion, without the knowledge of the attacker who will still keep on attacking thinking that his attack is successful but actually he will not be able to penetrate into actual system. In this way enough time is available to detect the attacker and his activities. The system is designed in this presented work is such that it is very fast because of the less access time, it is cost effective and user friendly. This system detects the attacks like Anomaly-based-attacks such as TCP flooding, UDP flooding. ICMP flooding attacks and Signature-based- attacks such as Shutdown virus, Snow-White Trojan attacks.

The network interface i.e. LAN is selected and packets come through the network interface of server to the user interface. Each packet is analyzed and goes through the Rule-based or Anomaly-based detection technique. The contents of packet are checked with the database where we have already stored typical attack patterns. If the content of packet is matched with the attack patterns then packet coming from this host are blocked and forwarded to honeypot. The honeypot actually blocks the packets. At the same time the IP address and attack type are added to database called Intruder List. If packets are sent by a legitimate user then they are forwarded to clients attached in network through real server.

3.1 *Interface selection*

Figure 4 displays the dropdown list through which the Input interface such as Realtek, Ethernet, Bluetooth, and Wireless LAN is selected is illustrated in fig.4.

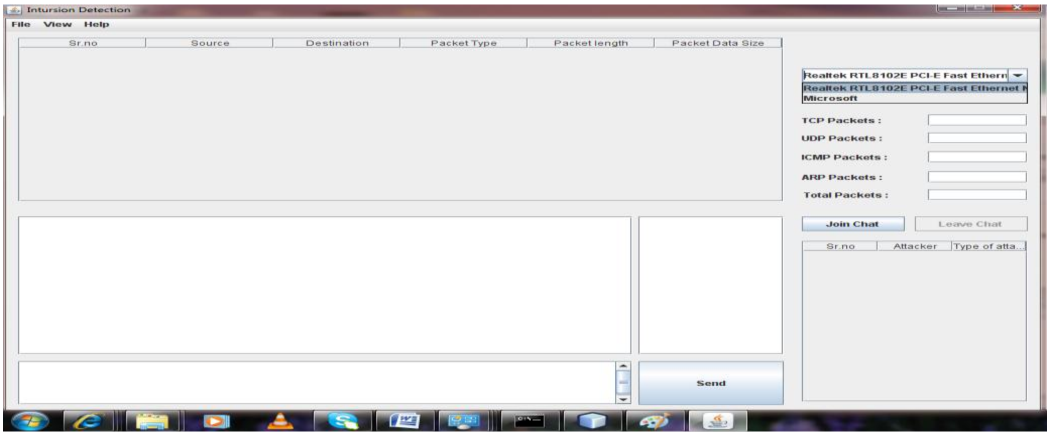
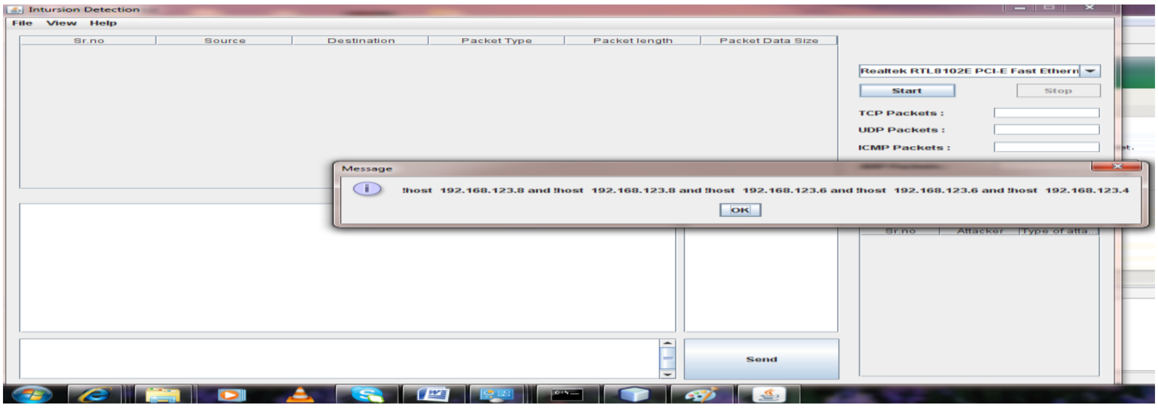


Fig4 GUI of Interface selection process

3.2 *Already Blocked Intruder*

Figure 5 shows the already blocked Intruders after the intrusion detection of the selected Interface starts. It retrieves the Intruders list from the Intruder table and displays it to user that this IP addresses are already blocked.

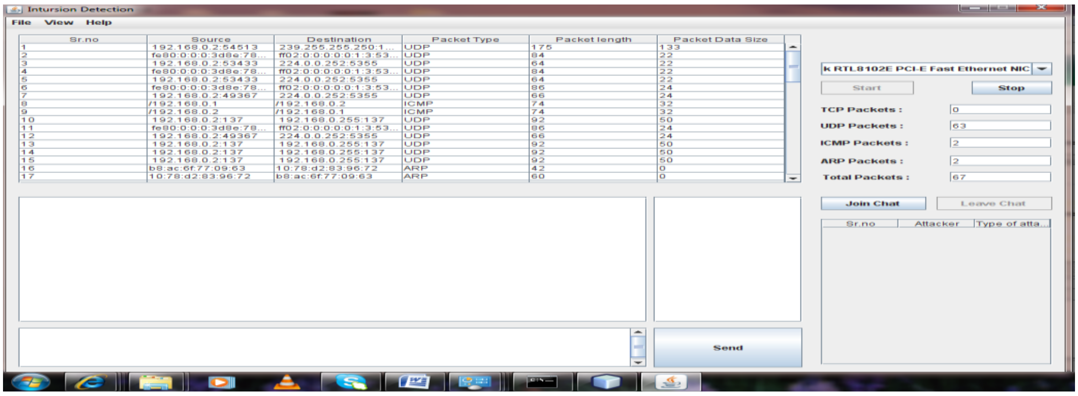


!host 192.168.123.8 and !host 192.168.123.8 and !host 192.168.123.6 and !host 192.168.123.6 and !host 192.168.123.4

Fig 5 List of already blocked intruders

3.3 *Packet Capturing*

A detail of the captured packets is illustrated in Fig.6. The packet is opened and various fields like source IP address, IP address of destination, type of packet, packet data length, packet size is observed.



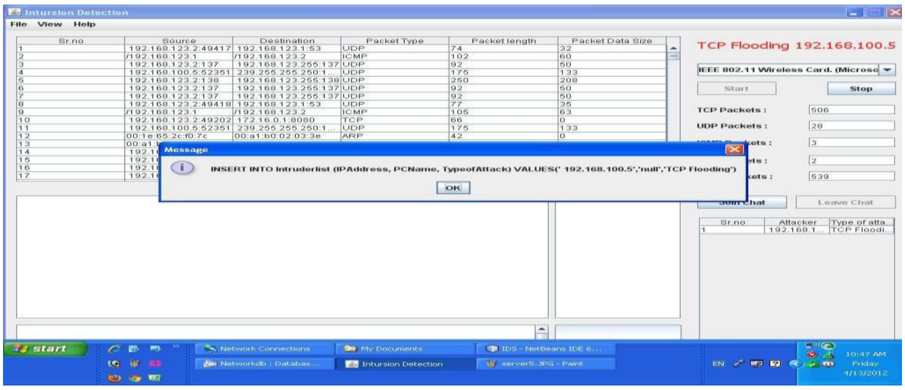
Sr.no	Source	Destination	Packet Type	Packet length	Packet Data Size
1	192.168.0.2:54513	239.255.255.250:1...	UDP	175	133
2	fe80:0:0:0:3d8e:78...	ff02:0:0:0:0:0:1:3:53...	UDP	84	22
3	192.168.0.2:53433	224.0.0.252:5355	UDP	64	22
4	fe80:0:0:0:3d8e:78...	ff02:0:0:0:0:0:1:3:53...	UDP	84	22
5	192.168.0.2:53433	224.0.0.252:5355	UDP	64	22
6	fe80:0:0:0:3d8e:78...	ff02:0:0:0:0:0:1:3:53...	UDP	86	24
7	192.168.0.2:49367	224.0.0.252:5355	UDP	66	24
8	/192.168.0.1	/192.168.0.2	ICMP	74	32
9	/192.168.0.2	/192.168.0.1	ICMP	74	32
10	192.168.0.2:137	192.168.0.255:137	UDP	92	50
11	fe80:0:0:0:3d8e:78...	ff02:0:0:0:0:0:1:3:53...	UDP	86	24
12	192.168.0.2:49367	224.0.0.252:5355	UDP	66	24
13	192.168.0.2:137	192.168.0.255:137	UDP	92	50
14	192.168.0.2:137	192.168.0.255:137	UDP	92	50
15	192.168.0.2:137	192.168.0.255:137	UDP	92	50
16	b8:ac:6f:77:09:63	10:78:d2:83:96:72	ARP	42	0
17	10:78:d2:83:96:72	b8:ac:6f:77:09:63	ARP	60	0

TCP Packets : 0
UDP Packets : 63
ICMP Packets : 2
ARP Packets : 2
Total Packets : 67

Fig 6 Details of captured packet

3.4 TCP-Flooding Attack

Figure 6 shows the TCP flooding attack and the IP address of the attacker.



Sr.no	Source	Destination	Packet Type	Packet length	Packet Data Size
1	192.168.123.2:49417	192.168.123.1:53	UDP	74	32
2	/192.168.123.1	/192.168.123.2	ICMP	102	60
3	192.168.123.2:137	192.168.123.255:137	UDP	92	50
4	192.168.100.5:52351	239.255.255.250:1...	UDP	175	133
5	192.168.123.2:138	192.168.123.255:138	UDP	250	208
6	192.168.123.2:137	192.168.123.255:137	UDP	92	50
7	192.168.123.2:137	192.168.123.255:137	UDP	92	50
8	192.168.123.2:49418	192.168.123.1:53	UDP	77	35
9	/192.168.123.1	/192.168.123.2	ICMP	105	63
10	192.168.123.2:49202	172.16.0.1:8080	TCP	66	0
11	192.168.100.5:52351	239.255.255.250:1...	UDP	175	133
12	00:1e:65:2c:f0:7c	00:a1:b0:02:03:3e	ARP	42	0
13	00:a1:				
14	192.1				
15	192.1				
16	192.1				
17	192.1				

INSERT INTO Intruderlist (IPAddress, PCName, TypeofAttack) VALUES(' 192.168.100.5','null','TCP Flooding')

TCP Flooding 192.168.100.5

IEEE 802.11 Wireless Card. (Microso

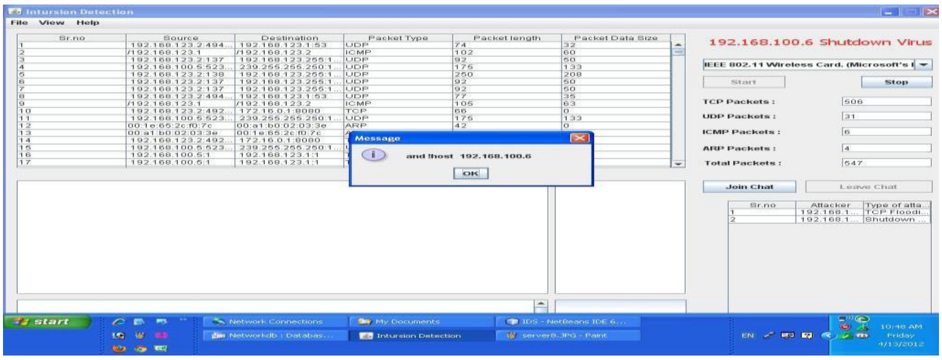
TCP Packets : 506
UDP Packets : 28
kets : 3
ts : 2
kets : 539

Sr.no	Attacker	Type of atta...
1	192.168.1...	TCP Floodi...

Fig 6 Details of TCP-Flooding attack

3.5 Shut down Virus

Figure 7 shows the Shut down Virus attack and shows the IP address of the attacker



Sr.no	Source	Destination	Packet Type	Packet length	Packet Data Size
1	192.168.123.2:494...	192.168.123.1:53	UDP	74	32
2	/192.168.123.1	/192.168.123.2	ICMP	102	60
3	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
4	192.168.100.5:523...	239.255.255.250:1...	UDP	175	133
5	192.168.123.2:138	192.168.123.255:1...	UDP	250	208
6	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
7	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
8	192.168.123.2:494...	192.168.123.1:53	UDP	77	35
9	/192.168.123.1	/192.168.123.2	ICMP	105	63
10	192.168.123.2:492...	172.16.0.1:8080	TCP	66	0
11	192.168.100.5:523...	239.255.255.250:1...	UDP	175	133
12	00:1e:65:2c:f0:7c	00:a1:b0:02:03:3e	ARP	42	0
13	00:a1:b0:02:03:3e	00:1e:65:2c:f0:7c	A		
14	192.168.123.2:492...	172.16.0.1:8080	T		
15	192.168.100.5:523...	239.255.255.250:1...	U		
16	192.168.100.5:1	192.168.123.1:1	T		
17	192.168.100.5:1	192.168.123.1:1	T		

and !host 192.168.100.6

192.168.100.6 Shutdown Virus

IEEE 802.11 Wireless Card. (Microsoft's I

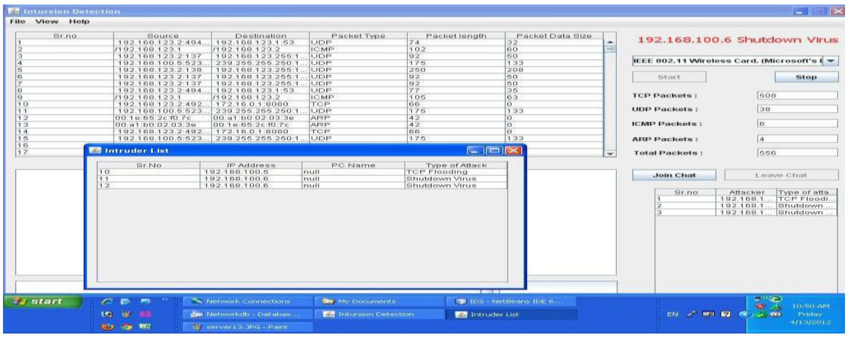
TCP Packets : 506
UDP Packets : 31
ICMP Packets : 6
ARP Packets : 4
Total Packets : 547

Sr.no	Attacker	Type of atta...
1	192.168.1...	TCP Floodi...
2	192.168.1...	Shutdown ...

Fig 7 Details of Shut down virus attack

3.6 Intruder list

The details of the Intruder list is in view menu and contains the IP address of attacker, PC name and type of attack is shown in Fig.8.



Sr.no	Source	Destination	Packet Type	Packet length	Packet Data Size
1	192.168.123.2:494...	192.168.123.1:53	UDP	74	32
2	/192.168.123.1	/192.168.123.2	ICMP	102	60
3	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
4	192.168.100.5:523...	239.255.255.250:1...	UDP	175	133
5	192.168.123.2:138	192.168.123.255:1...	UDP	250	208
6	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
7	192.168.123.2:137	192.168.123.255:1...	UDP	92	50
8	192.168.123.2:494...	192.168.123.1:53	UDP	77	35
9	/192.168.123.1	/192.168.123.2	ICMP	105	63
10	192.168.123.2:492...	172.16.0.1:8080	TCP	66	0
11	192.168.100.5:523...	239.255.255.250:1...	UDP	175	133
12	00:1e:65:2c:f0:7c	00:a1:b0:02:03:3e	ARP	42	0
13	00:a1:b0:02:03:3e	00:1e:65:2c:f0:7c	ARP	42	0
14	192.168.123.2:492...	172.16.0.1:8080	TCP	66	0
15	192.168.100.5:523...	239.255.255.250:1...	UDP	175	133
16					
17					

Sr.No	IP Address	PC Name	Type of Attack
10	192.168.100.5	null	TCP Flooding
11	192.168.100.6	null	Shutdown Virus
12	192.168.100.6	null	Shutdown Virus

192.168.100.6 Shutdown Virus

IEEE 802.11 Wireless Card. (Microsoft's I

TCP Packets : 508
UDP Packets : 38
ICMP Packets : 6
ARP Packets : 4
Total Packets : 556

Sr.no	Attacker	Type of atta...
1	192.168.1...	TCP Floodi...
2	192.168.1...	Shutdown ...
3	192.168.1...	Shutdown ...

Fig 8 Details of Intruder list

IV. Conclusion

The designed NBIIDS system is successfully implemented and tested, that uses both Anomaly Detection and Rule-based detection techniques. Honey pot deception technique is proved to be very useful to trace the attacker along with preventing him from penetrating into actual system. The system imposes very less overhead on the performance of server machine and client. Response time is quite satisfactory and processing time is fast. The NBIIDS designed is very user friendly. System can also be deployed on Wireless Networks. Honeypot designed in this paper can be enhanced to capture all packets of attacker even after blocking him. New attack patterns can be added to database so that the system detects new attacks. The designed system gives satisfactory results.

References

1. Ram Kumar Singh, Prof. T. Ramanujam, “Intrusion Detection System using Advanced Honeypot”, International Journal on Computer Science and Engineering (IJCSE),Vol.2, issue 1, 2012.
2. Network vs. Host-based Intrusion Detection: A guide to Intrusion Detection Technology. 2010
3. Karen Scarfone ,Peter Mell,Guide to Intrusion Detection and Prevention Systems , Special Publication pp.800-94.2012
4. Robert Graham ,Network Intrusion Detection Systems. 2009
5. Akshay Kulkarni et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (1) , 2012.
6. Jammi Ashok et. al. / International Journal of Engineering Science and Technology,Vol. 2,issue 10, pp 5689-5696,2010.