DOI: http://dx.doi.org/10.26483/ijarcs.v9i4.6176

ISSN No. 0976-5697

Volume 9, No. 4, July – August 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

INTRUSION DETECTION& PREVENTION USING HONEYPOT

Vivekanand Rajbhar
M.Sc. (CS), (Department Of Computer Science)
Thakur College of Science & Commerce
Mumbai, Maharashtra, India

Abstract: Computers & information technology (IT) revolutionized the world & growing day by day.Computer networks enable us to communicate with remote computer network and access resources effectively & efficiently. But these networks are not secure it's prone to intrusion, threats and attacks. Now a days industries use Intrusion detection system (IDS) & Intrusion prevention system (IPS) to monitor the system or a network for attacks, intrusion or threats& prevent the system or network from such vulnerabilities. However IDS/IPS is very expensive & complex to be implemented on your IT systems. It is not viable for small scale industries to implement such systems,thus a model of advanced decoy based technology called honeypot is proposed as a solution for small scale industries. Today honeypot is widely used by such industries beside that honeypot is also useful for large scale industries in improving their intrusion and prevention systems.But traditionally honeypot is viewed as deception system&not as a intrusion detection or prevention technology also most of the honeypot is built for Linux/Unix based operating systems because of the fact that these operating systems are open sourced systems.Most of the time honeypots are used in the virtualized environment & they usually stimulate fake system to capture network packets which are used later toanalyze them offline for any threats and intrusions.This paper proposes new framework &methodology that implements IDS & IPS within the honeypot withreal time network packet capturing &intrusions detection along with embedded firewall for intrusion prevention,which make the proposed honeypotmore effective and efficient than existing honeypots. The goal of this paper is to propose and design a portable java based real time packet capturing with intrusion detection & preventionhoneypot for windows based operating system. This honeypot is designed keeping Research honeypots in mind but it can be used in virtualized environment also.

Keywords: Intrusion detection system, Intrusion prevention system,Honeypot, Firewall, Security.
General Terms: Jnetpcap, Jderby,Winpcap,Powershell, Firewall.

I. INTODUCTION

A honeypot is a program, machine, or system put on a network as bait for attackers[3].The sole idea of honeypot is to deceive the attacker by making the honeypot seem like a legitimate system.
Honeypots are typically virtual machines that emulate real machines by feigning runningservices and open ports, services which one might find on a typical machine on a network,These running services are meant to attract the attention of attackers so that they spend valuable timeand resources will be used to try to exploit the machine while the attacker is being monitored & recorded by the honeypot [3].
The idea behind these systems is to provide systems or services that deceive the intruder. Such systems help in learning the methods that intruders use and they also can be viewed as a decoy to distract hackers from the real systems and services.
Honeypots is used as a decoy based deception system for information gathering,monitoring & preventing the real system from attacks.Today honeypots are mainly used by the small corporate companies to secure their networks from the hackers and unauthorized users.But traditionally honeypots is not be viewed as a solution to network security. There is vast types of honeypot are available in market especially for Linux/Unix systems though there is few honeypot designed for windows operating systems.Most of them store data of captured packets in TCPdump file for later analysis of threats and intrusions. Thus it mainly acts as a decoy (virtualization) & records the activity of attacker. However it does directly implement intrusion detection &prevention system.
In this thesis we look at the new framework and methodology which is proposed for honeypot.The proposed honeypot is designed for windows 64 bit operating system which has IDS & IPS in it which makes this honeypot more effective & efficient than traditional honeypots.

II. LITERATURE REVIEW

Honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems.
Honeypot is a decoy based deception system, used todeceive the attacker and monitor the activities of attackers on a system. In network security,honeypots are used to detect attack techniques of the attackers,these information which is gained from honeypotare used to modify and develop their IT system accordingly for better security. Thus the loop holes of the network security can be covered with the help of information provided by honeypots.

Honeypots are classified into following categories by their use:

Research honeypots: These are customized honeypots which is used to acquire information and knowledge of the hacker society. The knowledge gained by the experts are used for the early warnings, judgment of attacks, enhance the

intrusion detection systems and designing better tools for security.[1]

Production honeypots:These are the honeypots derived by the industries as a part of network security backbone. These honeypots works as early warning systems. The objectives of these honeypots are to remove the threats in industries. It provides the information to the administrator before the actual attack.[1]

Honeypots can also be classified on the basis of level of interaction as:

Low level interaction:These honeypots emulates some of the services of the operating system.Theyare typically processes running on a system. These are simplest honeypot to design & implement. Experienced hackers can easily detect these type of honeypot but has low risk of system being compromised.

High level interaction: High level interaction honeypots are real machines with realoperating systems and services which possess potential risk of being compromised from attackers. These type of honeypot allowuser to capture the information of attacker and record their activities and actions.

However IDS and IPS are different from honeypot [2][4].

Intrusion Detection System:An intrusion detection system (IDS) is a security system which inspects all your network traffic for any suspicious or malicious packets/patterns based on set of defined rules & alert about the intrusions in real time which might be a potential security breach, attack or threats that can compromise your system or its security.

Intrusion Prevention System: An intrusion preventionsystem (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.The IPS often sits directly behind the firewall and provides a complementary layer of analysis that negatively selects for dangerous content. Unlike its predecessor the Intrusion Detection System (IDS) - which is a passive system that scans traffic and reports back on threats.

Firewall:A firewall is a network security system that monitors and controls over all your incoming and outgoing network traffic based on advanced and a defined set of security rules.

It acts like a filter between two systems .It monitors all packets of your system & protect your system form any security breach, attacks, unauthorized access, viruses, and worms that try to reach your computer from the Internet.

Both IPS & IDS can implemented forrules based, signature based or anomaly based security systems.

III.SECURITY ISSUES WITH TRADITIONALHONEYPOTS*:*

- ✓ *Honeypots that fake or simulate:*These honeypot emulates services of a systemwhich mimics to be real services of a system to the attacker or hackers in order to deceive them. These type of honeypot can be easily detected by experienced hackers,thus there is potential threat to your system for being compromised.

- ✓ *High level interaction or Research based honeypot:* These type of system are real system are a put into use to deceive the attacker and monitor their activities.In this approach full access is given to attacker to access the system and intended to get information from attacks.But this system is always at risk to be compromised and after you got the information from one source you usually want to restrict the access to that source.

- ✓ *Honeypot stores data for later analysis:* Most of the honeypot are Linux/Unix based and usesTCP dump file to store data of intrusions and attacks which is used for later analysis of threats and intrusions that has occurred in a system. As the analysis is done offline, intrusion or threat detection is not done in real time.

- ✓ *Honeypot as a decoy:* Typically honeypot are is as a decoy based deception technology, hence it does not implement IPS directly. It usually used in virtualized environment as a decoy to prevent attacks to real production systems.

Thus the above mentioned problems can be improved by implementing real time intrusion detection & prevention system (using firewall)within honeypot.

IV. PROPOSED FRAMEWORK

The proposed framework of honeypot implements IDS & IPS within itself .While honeypot is installed between gateway of the network.

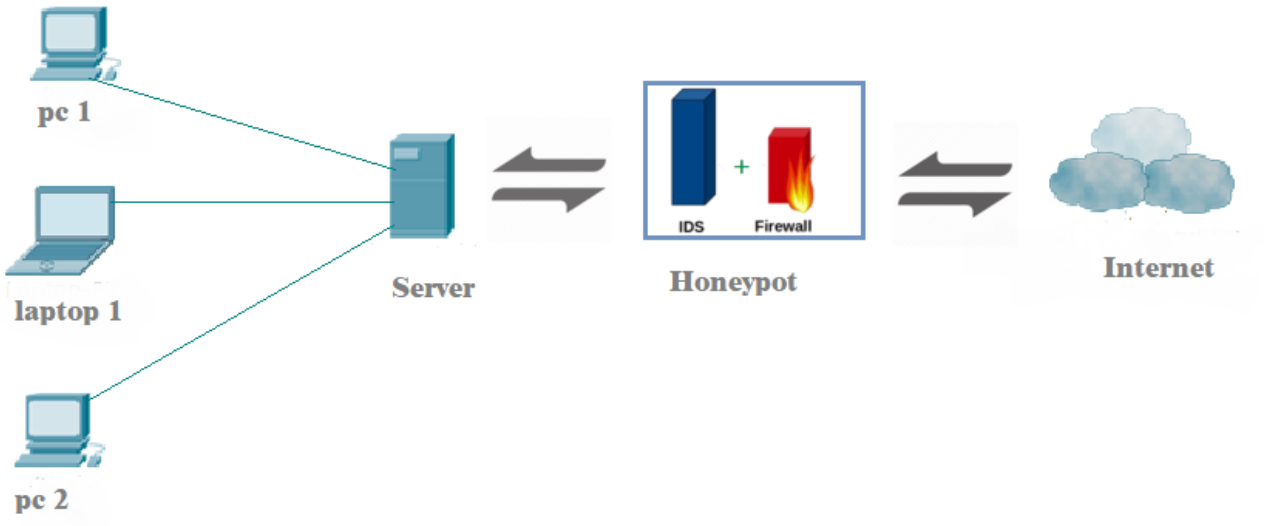

Fig 1: The conceptual view of proposed frame work for Honeypot.

The proposed honeypot filters all the traffic and check for intrusions using IDS rules & algorithms while intrusionsare prevented using IPS rulesand default firewall of operating system which is embedded in honeypot itself.

V. METHODOLOGY & IMPLEMENTATION

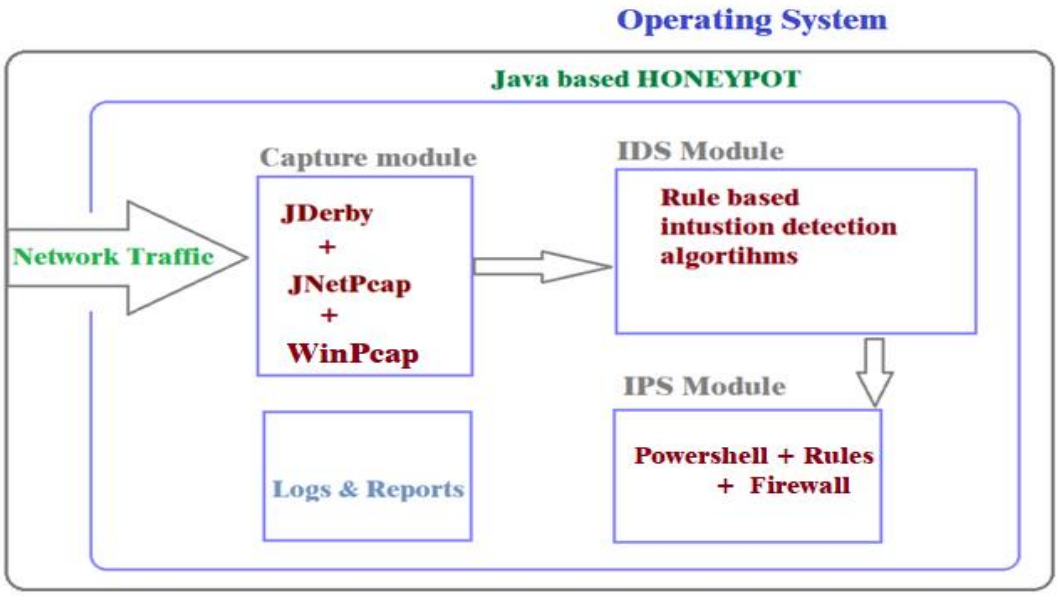

Fig 2: The conceptual view of methodology used to implement proposed Honeypot.

The proposed framework of honeypot is designed for windows 64 bit operating system .The idea is to develop a java based portable honeypot that has IDS & IPS embedded within itself.Proposed honeypot captures packets in real time using Jnetpcap,Winpcap&Jpowershelllibraries andstores all the packets data in to embeddedJderby database.Real time IDS is implemented in honeypot by using Jpowershell, IDSrules and algorithms. While IPS is implemented by usingJpowershell, custom rules& windows defaultfirewall.

In conventional honeypot usually packet is captured by packet sniffer tool like Wireshark and this sniffed/captured packet information is stored in TCP dump file. Therefore this TCP dump file is later used and applied with rules and algorithms in order to detect intrusions, attacks and any breach of security.

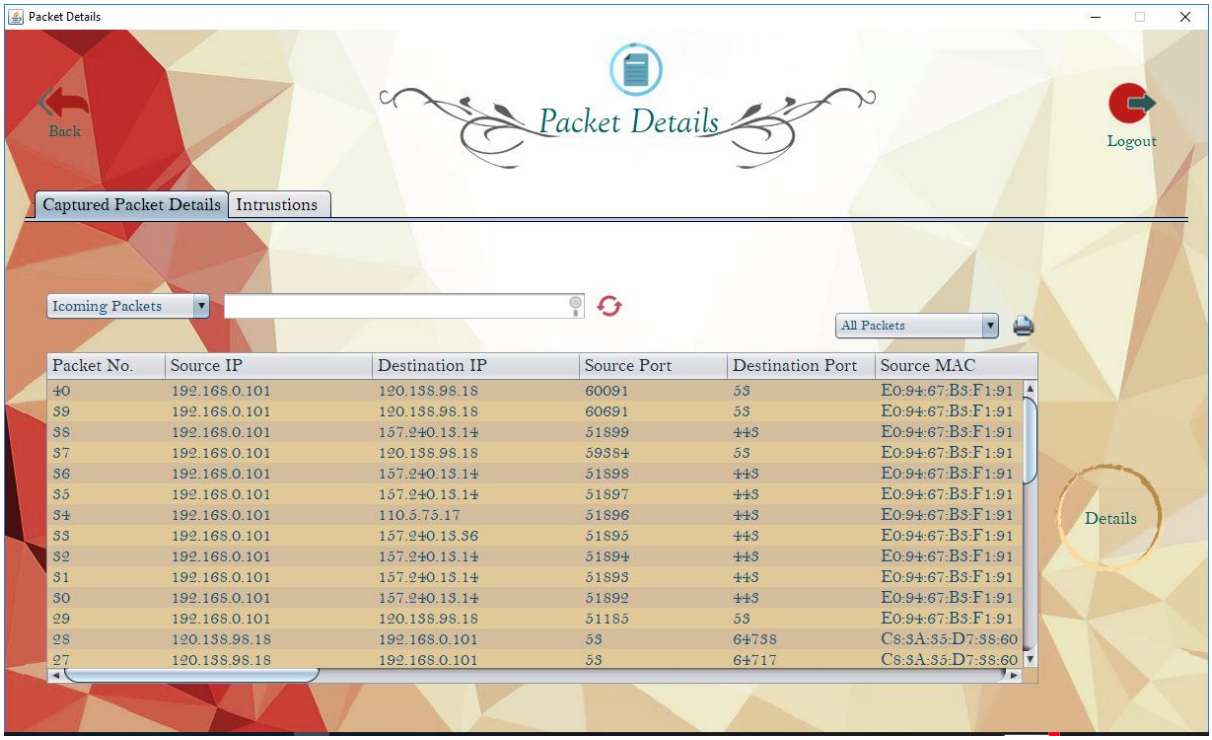

Fig 3: Details of packets which is being captured.

The proposed system differs from traditional honeypots it is a single instance multithreaded java based portable honeypotwhich uses custom JnetpcapAPI with Winpcap andJpowershell to capture &fetch packets information. But instead of creating TCP dump file it uses a embedded Jderby database to store all the packet information, which enables this honeypot to implement a real time intrusiondetectionsystem within it.

.

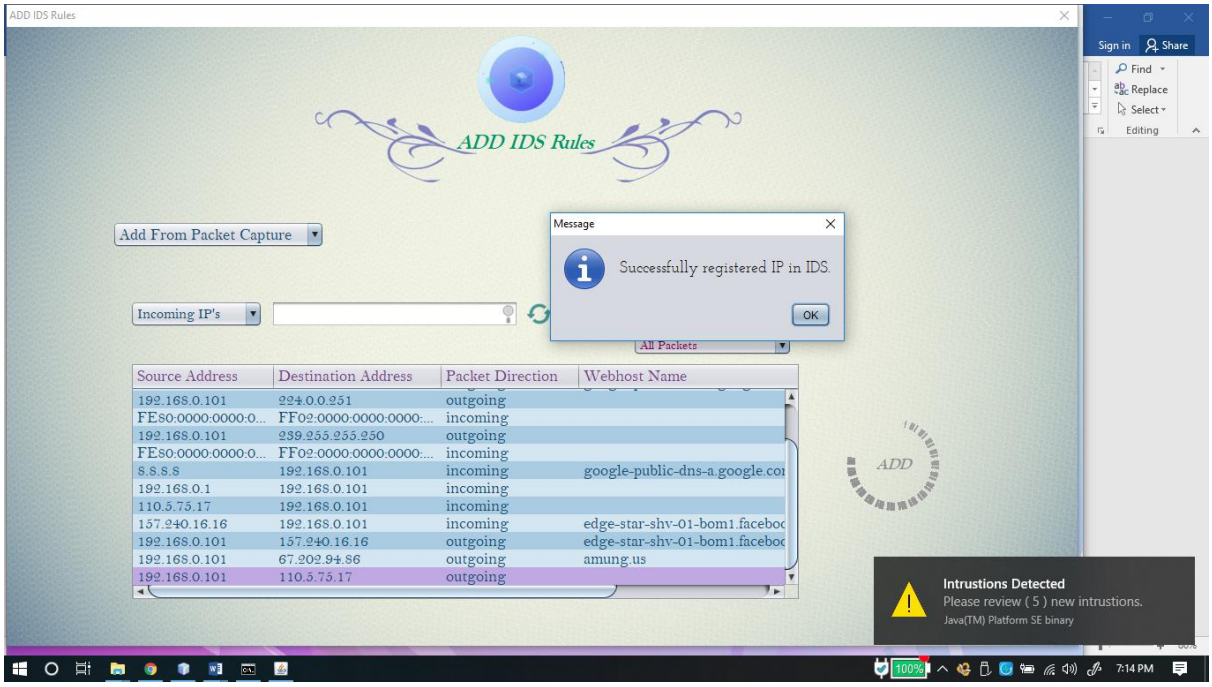

Fig 4: IDS rules is added and intrusion alert is shown as a desktop notification.

During the time of packet capture honeypot checks the packets for any intrusions happened. When packet is arrived,IDS rules & algorithms is applied on it to detect intrusions. If any intrusion is detected,honeypot will immediately alert the user about the detected intrusion.

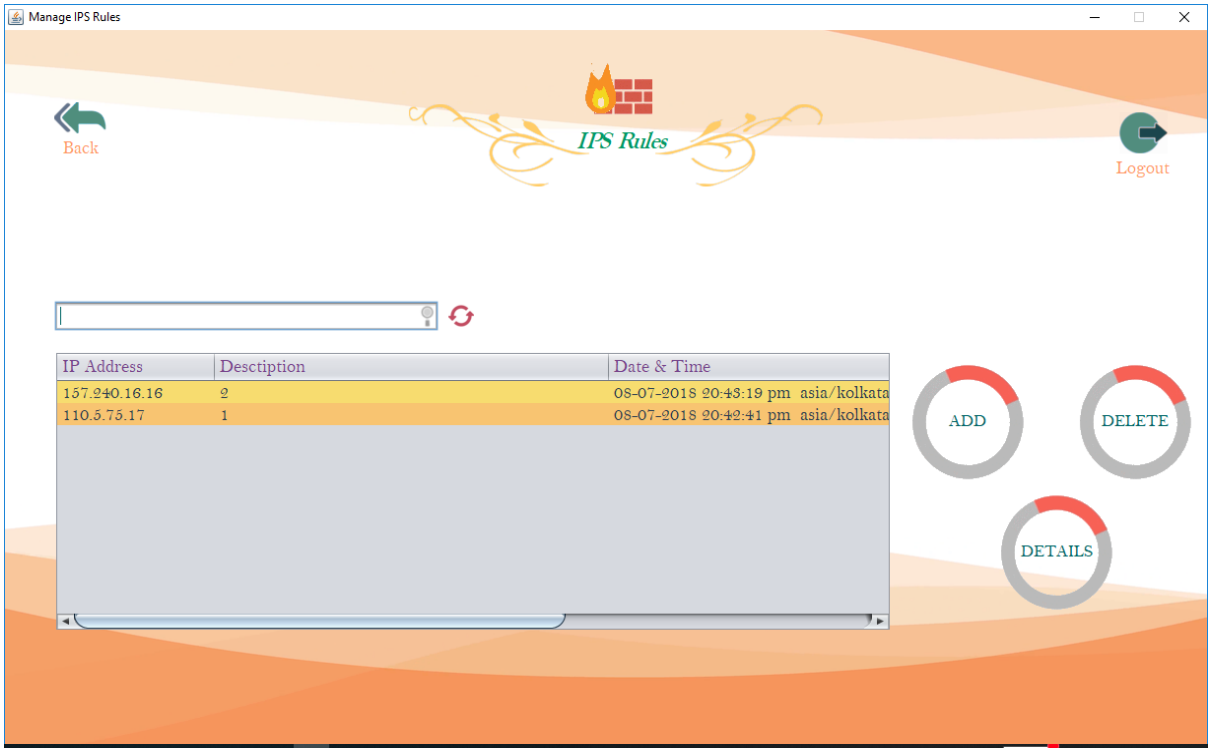

Fig 5: IPS rules is added.

While IPSis implemented using set of rules, Jpowershell, &a default firewall.As windows is not open source operating system, we cannot access the default operating systems firewall directly from java based honeypot thus we use Powershell runtime instance to access firewall.Honeypot passes firewall commands to Jpowershell e to add and remove rules in firewall to block or unlock IP address.

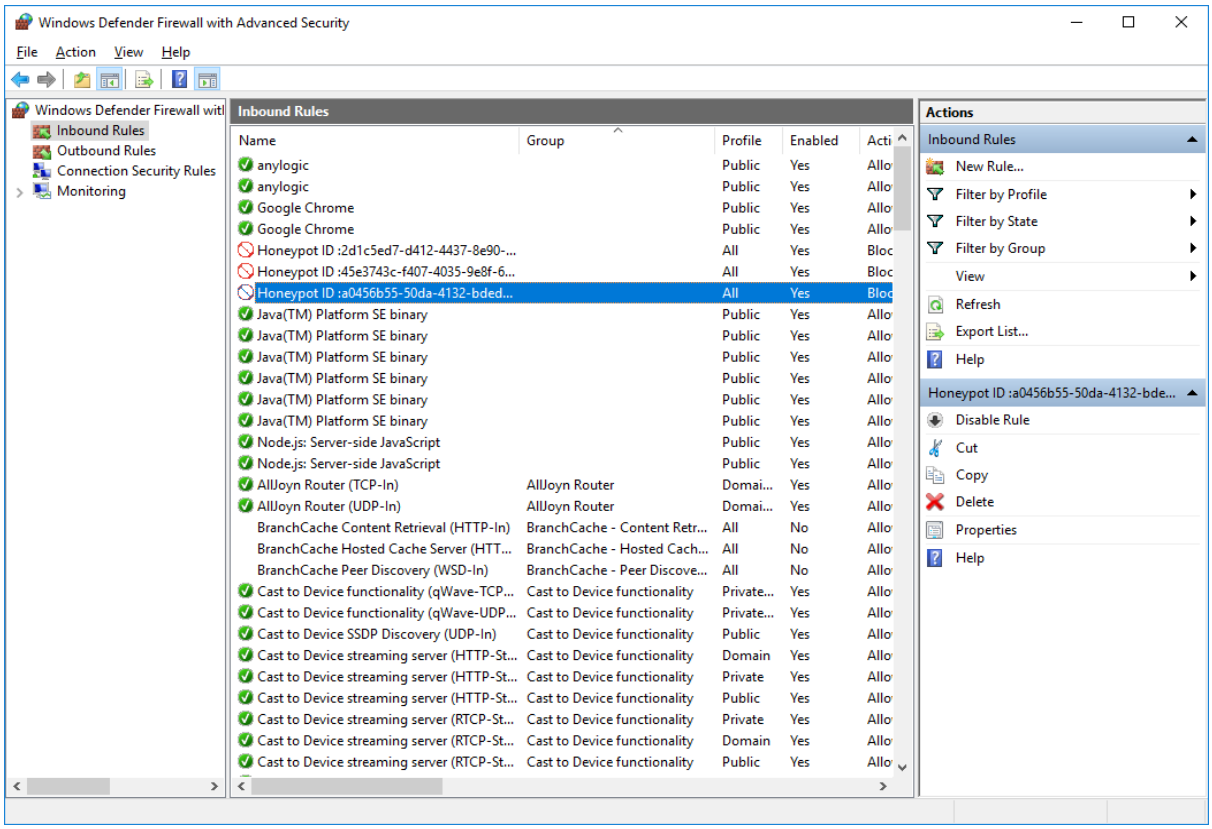

Fig 6: Added IPS rules from honeypot is generates rules in firewall.

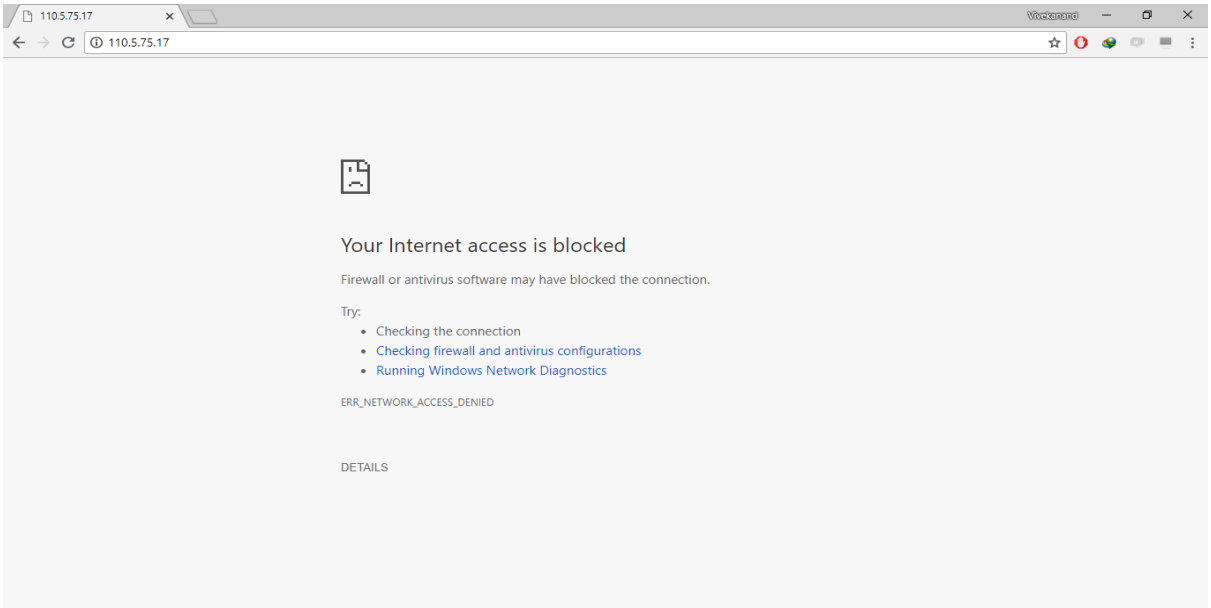

Fig 7: Firewall blocks all the packets of IP's that are present in IPS of honeypot.

When intrusions happens administrator can blacklist it to prevent any further intrusions from the same source.
As soon as admin adds IPS rules in honeypot a new rules is automatically generated in firewall which immediately starts preventing intrusions from network.
Logs and reports are also generatedfrom whole processwhich stored in database for further analysis.Thus this honeypot implements real time IDS &IPS which improves effectiveness of honeypot in network security.

.

VI.RESULT AND ANALYSIS

This honeypot implements real time rule based intrusion detection and prevention system, thus the accuracy of this honeypot for intrusion detection and prevention is 100%. But if signature based intrusion detection system or intrusion prevention system will be implemented on this proposed honeypot framework the accuracy of intrusion detection & prevention will vary according to ability of the signature based algorithm to detect false positive and false negative.

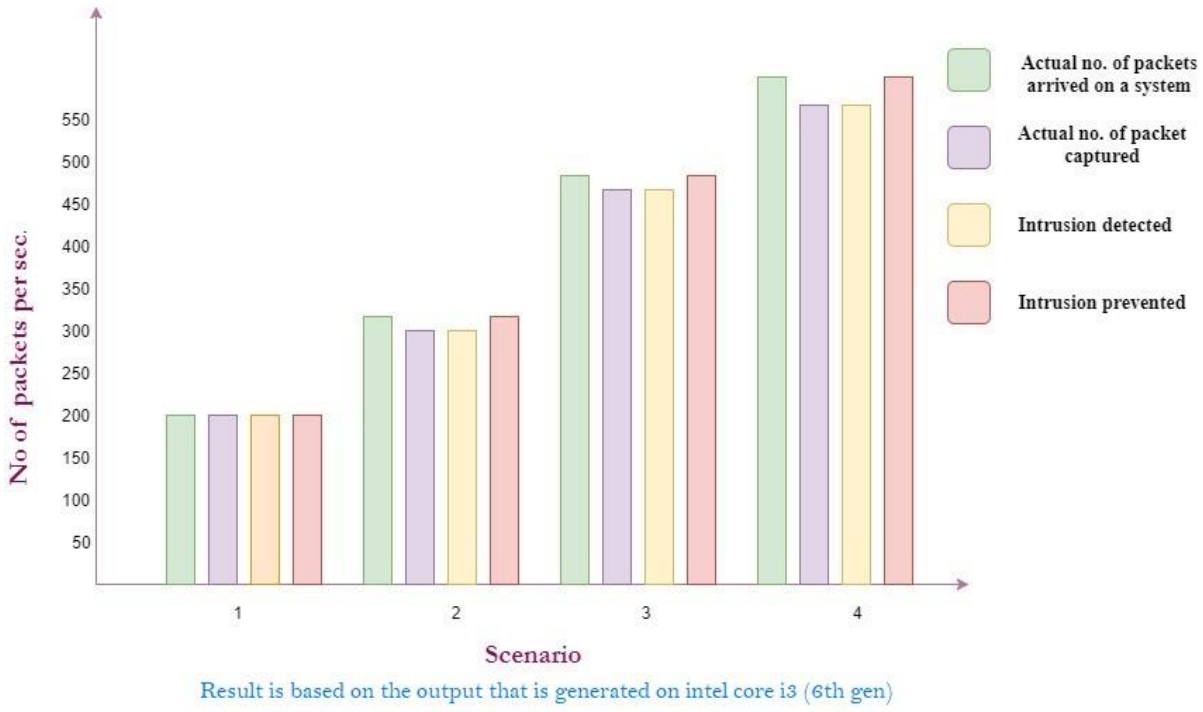

Fig 8:Performance graph of honeypot.

Performance of this system also depends upon the processing power of CPU.Because this honeypot implements real time IDS & IPS, it requires lot of computation. Therefore high processing power is need in the

case of higher bandwidth network, to process the current packet and switch to next packet quickly.

As you can see in above graph as the number of packets increases per sec the computation time also increase due to that some packet will be missed by honeypot but whatever packet is captured by honeypot, it detects intrusions for packets with 100% accuracy.

While this honeypot embeds OS default firewall to provide rule based IPS, thus it blocks all the packets ofspecified IP's entering the system at OS level.

Thereforeas result suggest, this proposed framework of honeypot more effective, secure and efficient.

VII.ADVANTAGES OF PROPOSED HONEYPOT:

- ✓ There are many honeypots available in the market there are only few honeypot for windows operating system most of them are based of Linux/Unixsystem.
- ✓ This system is java based portable honeypot with real time IDS &IPS that not only detected intrusions or but also prevent it using firewall.
- ✓ This type of honeypot can be very effective in research based & high interaction honeypot as it can be used with virtual machines or with real time systems
- ✓ It monitors all incoming and outgoing network traffic to your machine and gives alert to administrator when intrusion happens.
- ✓ It uses portable embedded Jderby database to store all information about packets, logs.
- ✓ It is more secure than traditional honeypots & can be used in non-virtual environment also.
- ✓ Economically viable as it uses minimal amount of resources.

VIII.LIMITATIONS OF PROPOSED HONEYPOT:

As there are several important advantages of using honeypots, there are also some disadvantages of them as well. You can only capture data when the hacker is attacking the system actively. If he does not attack the system, it is not possible to catch information. If there is an attack occurring in another system, the honeypot will not be able to identify it. So, attacks not towards the honeypot system may damage other systems and cause big problems.

Currently rule based IDPS is used in this honeypot and uses window operating system's default firewall to demonstrate proposed framework.

IX. CONCLUSION

Honeypot is a good decoy based deception tool mainly used by small scale industries, however is not a complete a solution to network security. Implementing IDSwith firewall within inHoneypot provides new way to attacks prevention, detection and reaction, it makes system more secure & effective. Honeypot can serve as a good deception tool for prevention of production system because of its ability of trapping attacker to a decoy system. Experts should focus to make honeypot easier to deploy, more difficult to detect& to add more functionality to it.Researchers should focus on developing new generation of honeypots that can incorporatenew security systemswhichis created using artificial intelligence and other latest technologies.Constant research development and innovation is needed in security domain inorder to keep out systems secure in future.

X. FUTURE WORK

In the future, attempt can be made to add implementationof signature & anomaly based intrusion detection and prevention system. Custom firewalls can be embedded with honeypot. In order to make it more effective and more robust.Furthermore this java based honeypot can be designed for various operating systems also more functionality can be added to it.

XI.REFERENCES

[1] Abhishek Sharma, "HONEYPOTS IN NETWORK SECURITY", Lovely Professional University (Punjab), India, (IJTRA) - Volume 1, Issue 5 (Nov-Dec 2013).

[2] Aaditya Jain, Dr. BalaBuksh, "ADVANCE TRENDS IN NETWORK SECURITY WITH HONEYPOT AND ITS COMPARATIVE STUDY WITH OTHER TECHNIQUES", M.tech(CS&E), Professor(CS&E) R.N. Modi Engineering College, Kota,Rajasthan,India, (IJETT) – Volume 29 - No. 26 (Nov 2015).

[3] Yogendra Kumar Jain, Surabhi Singh, "HONEYPOT BASED SECURE NETWORK SYSTEM",Computer Science & Engineering Samrat Ashok Technological Institute Vidisha, M.P ,India, (IJCSE) – Volume. 3 - No. 2 (Feb 2011).

[4] Aye AyeThu, " INTEGRATED INTRUSION DETECTION AND PREVENTION SYSTEM WITH HONEYPOT ON CLOUD COMPUTING ENVIRONMENT",University of Computer Studies (Yangon), Myanmar, (IJCA)- Volume 67– No.4,(April 2013).

[5] DenizAkkaya – Fabien Thalgott, "HONEYPOTS IN NETWORK SECURITY",Linnaeus University, 29th Feb 2010.