DOI: http://dx.doi.org/10.26483/ijarcs.v10i5.6478

ISSN No. 0976-5697

Volume 10, No. 5, September-October 2019

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# SECURING NETWORK THROUGH HONEYPOT AND ITS IMPLEMENTATION

Shubham Kumar
Assistant Professor
Galgotias University ,Greater Noida,U.P. India

***Abstract:*** Distributed systems and technology reformed the world and developing day by day. Computer systems empower us to speak with remote PC system and access assets successfully and productively. Yet, these systems are not verify it's inclined to interruption, dangers and assaults. Presently a days ventures use Intrusion Detection System (IDS) and Instrusion Prevention System (IPS) to screen the framework or a system for assaults, interruption or threats& keep the framework or system from such vulnerabilities. Anyway IDS/IPS is over the top expensive and complex to be executed on your IT frameworks. It isn't feasible for little scale enterprises to actualize such systems, thus a model of cutting edge imitation based innovation called honeypot is proposed as an answer for little scale ventures. Today honeypot is broadly utilized by such ventures close to that honeypot is likewise valuable for huge scale enterprises in improving their interruption and aversion systems. But customarily honeypot is seen as trickiness system & not as an interruption location or avoidance innovation additionally a large portion of the honeypot is worked for Linux/Unix based working frameworks on account of the way that these working frameworks are publicly released systems. Most of the time honeypots are utilized in the virtualized condition and they normally invigorate counterfeit framework to catch organize bundles which are utilized later to analyze them disconnected for any dangers and intrusions. This paper proposes new structure &methodology that actualizes IDS and IPS inside the honeypot with real time arrange parcel catching &intrusions recognition alongside implanted firewall for interruption prevention, which makes the proposed honeypot more successful and effective than existing honeypots. The objective of this paper is to propose and structure a convenient java based continuous bundle catching with interruption identification and prevention honeypot for windows based working framework. This honeypot is planned remembering Research honeypots however it very well may be utilized in virtualized condition moreover.

***Keywords:*** Intrusion detection system, Intrusion prevention system, Honeypot, Firewall, Security.

## INTODUCTION

A honeypot is a program, machine, or framework put on a system as trap for attackers[3].The sole thought of honeypot is to bamboozle the assailant by causing the honeypot to appear to be an authentic framework.

Honeypots are normally virtual machines that imitate genuine machines by pretending running services and open ports, administrations which one may discover on an ordinary machine on a network, These running administrations are intended to draw in the consideration of assailants with the goal that they spend important time and assets will be utilized to attempt to abuse the machine while the aggressor is being checked and recorded by the honeypot [3]. The thought behind these frameworks is to give frameworks or administrations that misdirect the interloper. Such frameworks help in learning the techniques that gatecrashers use and they likewise can be seen as a fake to occupy programmers from the genuine frameworks and administrations.

Honeypots is utilized as an imitation based trickiness framework for data gathering, monitoring and keeping the genuine framework from attacks. Today honeypots are for the most part utilized by the little corporate organizations to verify their systems from the programmers and unapproved users. But generally honeypots isn't being seen as an answer for system security. There is huge kinds of honeypot are accessible in market particularly for Linux/Unix frameworks however there is not many honeypot intended for windows working systems. Most of them store information of caught parcels in TCP dump document for later investigation of dangers and interruptions. Along these lines it basically goes about as an imitation (virtualization) and records the action of assailant. Anyway it does straightforwardly execute interruption discovery &prevention framework.

In this proposition we take a gander at the new structure and philosophy which is proposed for honeypot. The proposed honeypot is intended for windows 64 piece working framework which has IDS and IPS in it which makes this honeypot more successful and productive than conventional honeypots.

## LITERATUREREVIEW

Honeypot is a PC security component set to recognize, divert, or, in some way, balance endeavors at unapproved utilization of data frameworks. Honeypot is a distraction based duplicity framework, utilized to deceive the assailant and screen the exercises of aggressors on a framework. In system security, honeypots are utilized to recognize assault methods of the attackers, these data which is picked up from honeypot are used to alter and build up their IT framework in like manner for better security. Along these lines the escape clauses of the system security can be secured with the assistance of data given by honeypots.

Honeypots are ordered into following classifications by their utilization:

1. **Research honeypots:**

These are altered honeypots which is utilized to secure data and learning of the programmer society. The learning picked up by the specialists are utilized for the early alerts,

© 2015-19, IJARCS All Rights Reserved

judgment of assaults, improve the interruption recognition frameworks and planning better instruments for security.[1]

***2.* Production honeypots*:***

These are the honeypots determined by the businesses as a piece of system security spine. These honeypots fills in as early cautioning frameworks. The goals of these honeypots are to evacuate the dangers in businesses. It gives the data to the executive before the real attack.[1]

Honeypots can likewise be arranged based on level of association as:

**1. Low level interaction:**

These honeypots copies a portion of the administrations of the working system.Theyare commonly procedures running on a framework. These are least complex honeypot to structure and actualize. Experienced programmers can without much of a stretch distinguish these kind of honeypot however has generally safe of framework being undermined.

**2. High level interaction:**

High level connection honeypots are genuine machines with realoperating frameworks and administrations which have potential danger of being undermined from aggressors. These sort of honeypot allowuser to catch the data of aggressor and record their exercises and activities.

Anyway IDS and IPS are unique in relation to honeypot [2][4].

**Intrusion Detection System:**

An interruption identification framework (IDS) is a security framework which examines all your system traffic for any suspicious or noxious parcels/designs dependent on set of characterized rules and caution about the interruptions continuously which may be a potential security rupture, assault or dangers that can bargain your framework or its security.

**Intrusion Prevention System:**

An interruption preventionsystem (IPS) is a system security/risk aversion innovation that looks at system traffic streams to recognize and avoid helplessness exploits.The IPS frequently sits straightforwardly behind the firewall and gives a corresponding layer of examination that adversely chooses for hazardous substance. Not at all like its ancestor the Intrusion Detection System (IDS) – which is an inactive framework that outputs traffic and reports back on dangers.

**Firewall:**

A firewall is a system security framework that screens and powers over the entirety of your approaching and active system traffic dependent on cutting edge and a characterized set of security rules. It acts like a channel between two frameworks .It screens all parcels of your framework and ensure your framework structure any security rupture, assaults, unapproved get to, infections, and worms that attempt to arrive at your PC from the Internet.

The two IPS and IDS can actualized forrules based, signature based or inconsistency based security frameworks.

**SECURITY ISSUES WITH TRADITIONALHONEYPOTS*:***

- Honeypots that phony or simulate:These honeypot imitates administrations of a systemwhich emulates to be genuine administrations of a framework to the aggressor or programmers so as to bamboozle them. These kind of honeypot can be effectively identified by experienced hackers,thus there is potential danger to your framework for being undermined.
- High level cooperation or Research based honeypot: These sort of framework are genuine framework are a placed into utilization to delude the assailant and screen their activities.In this methodology full access is given to aggressor to get to the framework and proposed to get data from attacks.But this framework is consistently in danger to be undermined and after you got the data from one source you more often than not have any desire to limit the entrance to that source.
- Honeypot stores information for later examination: Most of the honeypot are Linux/Unix based and usesTCP dump record to store information of interruptions and assaults which is utilized for later investigation of dangers and interruptions that has happened in a framework. As the investigation is done disconnected, interruption or risk location isn't done continuously.
- Honeypot as an imitation: Typically honeypot are is as a bait based duplicity innovation, subsequently it doesn't execute IPS straightforwardly. It normally utilized in virtualized condition as a bait to counteract assaults to genuine generation frameworks.

In this manner the previously mentioned issues can be improved by executing constant interruption location and counteractive action framework (utilizing firewall)within honeypot.

**PROPOSEDFRAMEWORK**

The proposed system of honeypot executes IDS and IPS inside itself .While honeypot is introduced between entryway of the system.

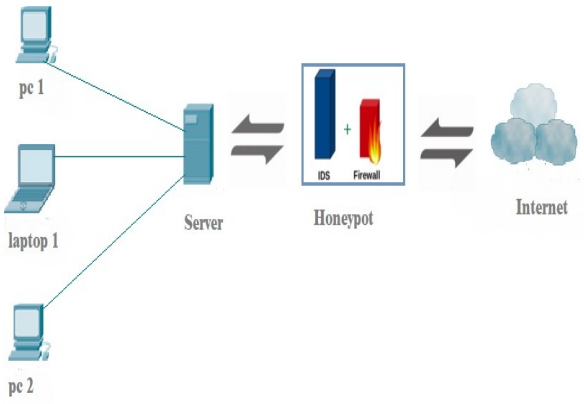


**Fig 1: The conceptual view of proposed frame work for Honeypot.**

The proposed honeypot channels all the traffic and check for interruptions utilizing IDS rules and calculations while interruptions are avoided utilizing IPS rulesand default firewall of working framework which is implanted in honeypot itself.

© 2015-19, IJARCS All Rights Reserved

## METHODOLOGY &IMPLEMENTATION

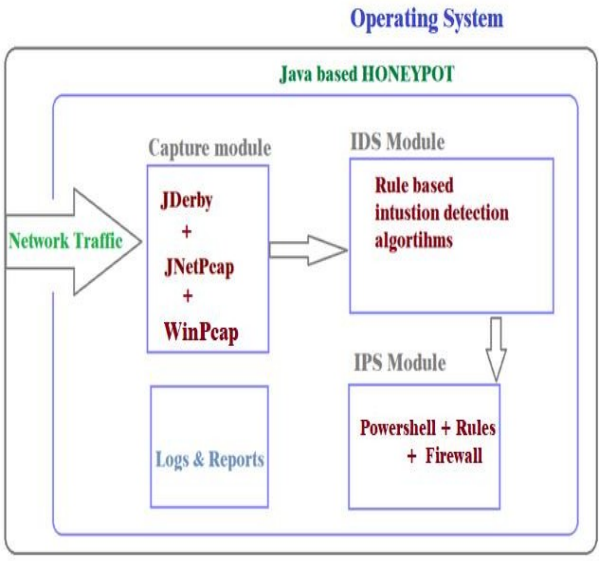


**Fig 2: The conceptual view of methodology used to implement proposed Honeypot**.

The proposed structure of honeypot is intended for windows 64 piece working framework .The thought is to build up a java based versatile honeypot that has IDS and IPS inserted inside itself.Proposed honeypot catches parcels progressively utilizing Jnetpcap,Winpcap&Jpowershelllibraries andstores every one of the bundles information in to embeddedJderby database.Real time IDS is actualized in honeypot by utilizing Jpowershell, IDSrules and calculations. While IPS is actualized by usingJpowershell, custom rules& windows defaultfirewall.

In ordinary honeypot more often than not parcel is caught by bundle sniffer device like Wireshark and this sniffed/caught bundle data is put away in TCP dump record. In this way this TCP dump document is later utilized and applied with guidelines and calculations so as to recognize interruptions, assaults and any rupture of security.

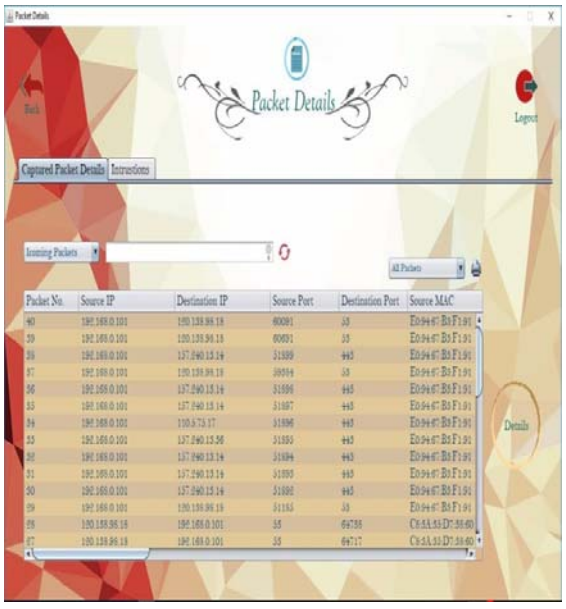


**Fig 3: Details of packets which is being captured.**

The proposed framework contrasts from conventional honeypots it is a solitary example multithreaded java based versatile honeypot which uses custom Jnetpcap API with Winpcap and Jpowershell to catch &fetch parcels data. Be that as it may, rather than making TCP dump document it utilizes an installed Jderby database to store all the parcel data, which empowers this honeypot to execute an ongoing interruption recognition framework inside it.

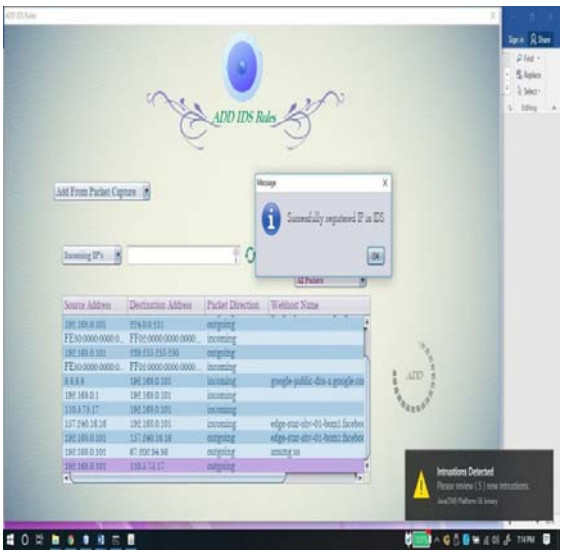


**Fig 4: IDS rules is added and intrusion alert is shown as a desktop notification.**

During the hour of bundle catch honeypot checks the parcels for any interruptions occurred. At the point when parcel is arrived,IDS rules and calculations is applied on it to identify interruptions. On the off chance that any interruption is detected,honeypot will quickly alarm the client about the recognized interruption.

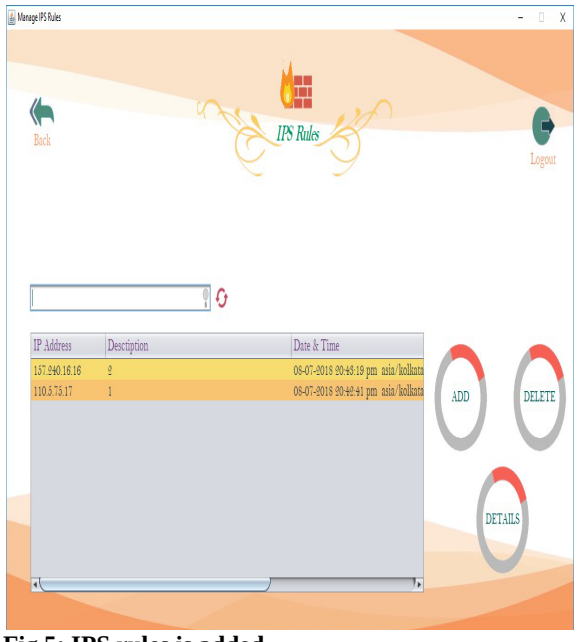


**Fig 5: IPS rules is added.**

© 2015-19, IJARCS All Rights Reserved

While IPSis executed utilizing set of standards, Jpowershell, &a default firewall.Aswindows isn't open source working framework, we can't get to the default working frameworks firewall legitimately from java based honeypot along these lines we use Powershell runtime case to get to firewall.Honeypot passes firewall directions to Jpowershell e to include and expel controls in firewall to square or open IP address.

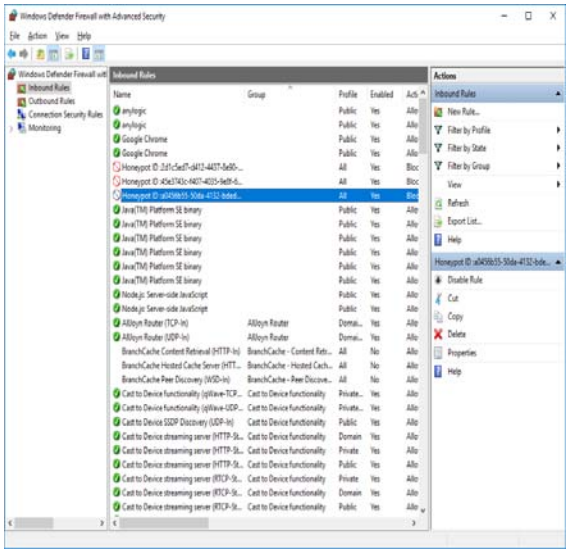

**Fig 6: Added IPS rules from honeypot is generates rules in firewall.**

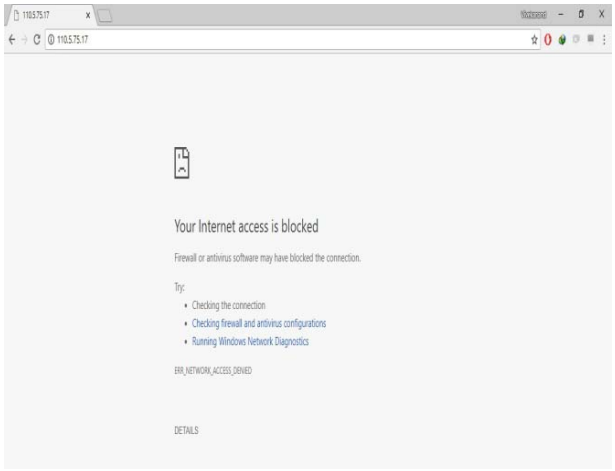


**Fig 7: Firewall blocks all the packets of IP's that are present in IPS of honeypot.**

At the point when interruptions happens head can boycott it to keep any further interruptions from a similar source. When administrator includes IPS governs in honeypot another guidelines is naturally produced in firewall which quickly starts keeping interruptions from system. Logs and reports are likewise generatedfrom entire processwhich put away in database for further analysis.Thus this honeypot executes ongoing IDS &IPS which improves viability of honeypot in system security.

**RESULT ANDANALYSIS**

This honeypot actualizes ongoing standard based interruption identification and aversion framework, subsequently the exactness of this honeypot for interruption discovery and avoidance is 100%. Be that as it may, if mark based interruption discovery framework or interruption counteractive action framework will be actualized on this proposed honeypot system the precision of interruption recognition and avoidance will fluctuate as indicated by capacity of the mark based calculation to identify false positive and false negative.

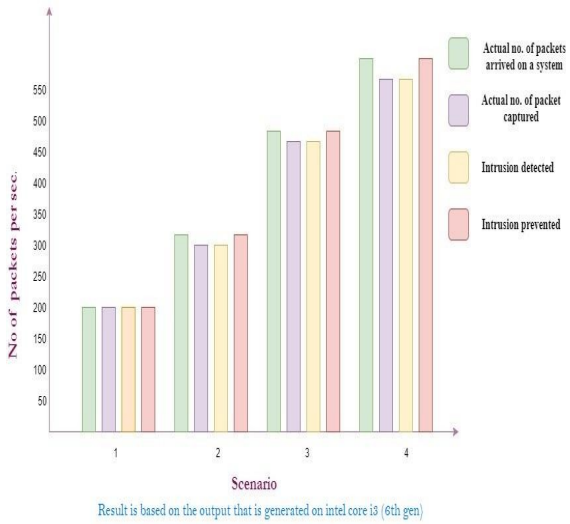


**Fig 8:Performance graph of honeypot.**

Execution of this framework likewise relies on the processing power of CPU. Because this honeypot actualizes continuous IDS and IPS, it requires parcel of calculation. Accordingly high preparing force is need on account of higher transmission capacity organize, to process the present bundle and change to next parcel rapidly.

As should be obvious in above diagram as the quantity of bundles increments per sec the calculation time additionally increment because of that some parcel will be remembered fondly by honeypot however whatever parcel is caught by honeypot, it recognizes interruptions for bundles with 100% precision.

While this honeypot installs OS default firewall to give guideline based IPS, in this manner it obstructs every one of the bundles ofspecified IP's entering the framework at OS level.

Thereforeas result recommend, this proposed system of honeypot increasingly successful, secure and productive.

**ADVANTAGES OF PROPOSEDHONEYPOT:**

- There are numerous honeypots accessible in the market there are just couple of honeypot for windows working framework the majority of them are based of Linux/Unixsystem.
- This framework is java based compact honeypot with

© 2015-19, IJARCS All Rights Reserved

continuous IDS &IPS that distinguished interruptions or as well as counteract it utilizing firewall.

- This sort of honeypot can be extremely viable in research based and high cooperation honeypot as it very well may be utilized with virtual machines or with constant frameworks
- It screens all approaching and active system traffic to your machine and offers alarm to head when interruption occurs.
- It utilizes convenient implanted Jderby database to store all data about bundles, logs.
- It is more secure than conventional honeypots and can be utilized in non-virtual condition too.
- Economically reasonable as it utilizes insignificant measure of assets.

**LIMITATIONS OF PROPOSEDHONEYPOT:**

As there are a few significant points of interest of utilizing honeypots, there are a few impediments of them too. You can possibly catch information when the programmer is assaulting the framework effectively. On the off chance that he doesn't assault the framework, it is preposterous to expect to get data. In the event that there is an assault happening in another framework, the honeypot won't have the option to distinguish it. In this way, assaults not towards the honeypot framework may harm different frameworks and cause enormous issues. Right now principle based IDPS is utilized in this honeypot and utilizations window working framework's default firewall to show proposed system.

**CONCLUSION**

Honeypot is a decent distraction based double dealing instrument predominantly utilized by little scale enterprises, anyway is certifiably not a total an answer for system security. Actualizing IDSwith firewall inside inHoneypot gives better approach to assaults anticipation, recognition and response, it makes framework increasingly secure and compelling. Honeypot can fill in as a decent duplicity device for counteractive action of creation framework in light of its capacity of catching assailant to an imitation framework. Specialists should center to make honeypot simpler to convey, progressively hard to detect& to add greater usefulness to it.Researchers should concentrate on growing new age of honeypots that can incorporatenew security systemswhichis made utilizing man-made reasoning and other most recent technologies.Constant examine improvement and advancement is required in security space inorder to keep out frameworks secure in future.

**FUTUREWORK**

Later on, endeavor can be made to include implementationof signature and inconsistency based interruption location and aversion framework. Custom firewalls can be inserted with honeypot. So as to make it increasingly powerful and more robust.Furthermore this java based honeypot can be intended for different working frameworks likewise greater usefulness can be added to it.

**REFERENCES**

[1] Abhishek Sharma, “HONEYPOTS IN NETWORK SECURITY”, Lovely Professional University (Punjab), India, (IJTRA) - Volume 1, Issue 5 (Nov- Dec2013).

[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 (Nov2015).

[3] YogendraKumar 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] AyeAyeThu, ” INTEGRATED INTRUSION DETECTION AND PREVENTION SYSTEM WITH HONEYPOT ON CLOUD COMPUTING ENVIRONMENT”,University of ComputerStudies (Yangon), Myanmar, (IJCA)- Volume 67– No.4,( April2013).

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

© 2015-19, IJARCS All Rights Reserved 