HONEYMAZE: A HYBRID INTRUSION DETECTION SYSTEM

Divya[1] and Amit Chugh[2]
Department of Computer Science, Lingaya's university, Faridabad, India
Asst. Prof. in Department of Computer Science, Lingaya's university, Faridabad, India

ABSTRACT

In this paper we discussed, a hybrid intrusion detection system using honey pot. Hybrid honeypot is the combination of low and high interaction honeypots. It helps in detecting intrusion attacking on the system. For this, I have proposed the hybrid model of hybrid honeypot. Low interaction honeypot provide enough interaction to attackers to allow honeypot to detect interesting attacks. It also includes the concept of neural network in combination with anomaly detection technique. Attacks against the honeypot are caught, and any incurred state changes are discarded and the alarm is raised. The outcome of processing a request is used to filter future attack instances and could be used to update the anomaly detector and updated in the log table. By using hybrid architecture, we can reduce the cost of deploying honeypots.

KEYWORDS: *IDS, Honeypot, Neural network.*

I. INTRODUCTION

An intrusion detection system (IDS) is a system that is designed to capture intrusion attempts so that measures can be taken to limit damage and prevent future attacks. This is typically accomplished by sending alerts anytime the IDS detect an attack. IDSs can be broken down by where they gather their data and how they check for attacks.

1.1. DETECTION METHODS

A. Anomaly approach: Anomaly detection identifies abnormal behavior. It requires the prior construction of profiles for normal behavior of users, hosts or networks; therefore, historical data are collected over a period of normal operation. IDSs monitor current event data and use a variety of measures to distinguish between abnormal and normal activities. Anomaly detection refers to an approach where a system is trained to learn the "normal behavior" of a network. An alarm is raised .When the network is observed to deviate from this learned definition of normality. This type of system is theoretically capable of detecting unknown attacks, overcoming a clear limitation of the misuse approach. These systems are prone to false alarms, since user's behavior may be inconsistent and threshold levels will remain difficult to fine tune. It is essential that normal data used for characterization are free from attacks.

B. Misuse approach: Misuse detection technique is the most widespread approach used in the commercial world of IDSs. The basic idea is to use the knowledge of known attack patterns and apply this knowledge to identify attacks in various sources of data being monitored.

C. Signature based approach: It works just similar to the existing anti-virus software. In this approach the semantic characteristics of an attack is analyzed and details is used to form attack signatures. The attack signatures are formed in such a way that they can be searched using information in audit data logs produced by computer systems. A database of attack signatures is built

based on well defined known attacks and the detection engine of an ID compares string log data or audit data against the database to detect attack.

1.2. ORGANIZATION

SECTION 2: Description about history of Honeypots.
SECTION 3: Necessary concepts for understanding Honeypot methodology of hybrid model.
SECTION 4: Description about proposed hybrid Honeypot model.
SECTION 5: Details about result of hybrid honeypot.
SECTION 6: A conclusion detailing and Future advancement .

II. RELATED WORK

Omid paper[1] gives the brief about Honeypots provide a system that can catch the attackers and hackers and response to various security frameworks to control the globe and its environment and examine and analysis network activities. We try to employ and develop a honeypot framework to propose a hybrid approach that improves the current security. This paper, we proposed hybrid honeypots based network assuming initiative and enterprise security scheme strategies. The proposed model has more advantages that can response accurately and swiftly to unknown attacks and lifetime safer for the network security.

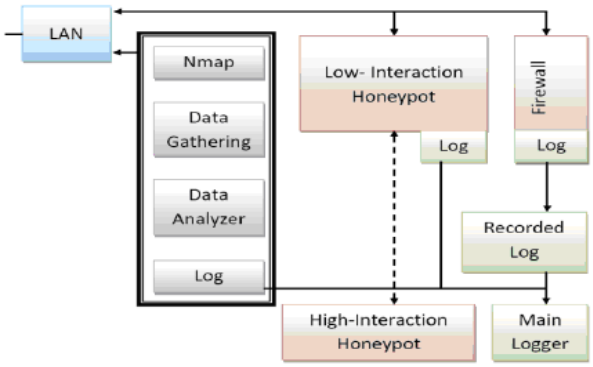

Fig. 1: Functionality of low and high interaction honeypot

Hichem Sedjelmaci and Mohamed Feham[21] proposed Wireless sensor network (WSN) is regularly deployed in unattended and hostile environments. The WSN is vulnerable to security threats and susceptible to physical capture. Thus, it is necessary to use effective mechanisms to protect the network. It is widely known, that the intrusion detection is one of the most efficient security mechanisms to protect the network against malicious attacks or unauthorized access. In this paper, we propose a hybrid intrusion detection system for clustered WSN. Our intrusion framework uses a combination between the Anomaly Detection based on support vector machine (SVM) and the Misuse Detection. Experiments results show that most of routing attacks can be detected with low false alarm. P. KIRAN SREE, Dr I Ramesh Babu, Dr J. V. R. Murty, Dr. R. Ramachandran, N.S.S.S.N Usha Devi, Proposed[22] about Ad hoc wireless network with their changing topology and distributed nature are more prone to intruders. The network monitoring functionality should be in operation as long as the network exists with nil constraints. The efficiency of an Intrusion detection system in the case of an ad hoc network is not only determined by its dynamicity in monitoring but also in its flexibility in utilizing the available power in each of its nodes. In this paper we propose a hybrid intrusion detection system, based on a power level metric for potential ad hoc hosts, which is used to determine the duration for which a particular node can support a network-monitoring node. Power – aware hybrid intrusion detection system focuses on the available power level in each of the nodes and determines the network monitors. Power awareness in the network results in maintaining power for network monitoring, with monitors changing often, since it is an iterative power-optimal solution to identify nodes for distributed agent-based intrusion detection. The advantage that this approach entails is the inherent flexibility it provides, by means of considering only fewer nodes for re-establishing network monitors. The detection of intrusions in the network is done with the help of Cellular

Automata (CA). The CA's classify a packet routed through the network either as normal or an intrusion. The use of CA's enable in the identification of already occurred intrusions as well as new intrusions.

Muna Mhammad [23] proposed in his paper that networks grow both in importance and size, there is an increasing need for effective security monitors such as Network Intrusion Detection System to prevent such illicit accesses. Intrusion Detection Systems technology is an effective approach in dealing with the problems of network security. In this paper, we present an intrusion detection model based on hybrid fuzzy logic and neural network. The key idea is to take advantage of different classification abilities of fuzzy logic and neural network for intrusion detection system. The new model has ability to recognize an attack, to differentiate one attack from another i.e. classifying attack, and the most important, to detect new attacks with high detection rate and low false negative. Training and testing data were obtained from the Defense Advanced Research Projects Agency (DARPA) intrusion detection evaluation data set.

III. HONEYPOT

Honeypots are decoy computer resources set up for the purpose of monitoring and logging the activities of entities that probe, attack or compromise them. Activities on honeypots can be considiered suspicious by definition, as there is no point for benign users to interact with these systems. Honeypots come in many shapes and sizes; examples include dummy items in a database, low-interaction network components.

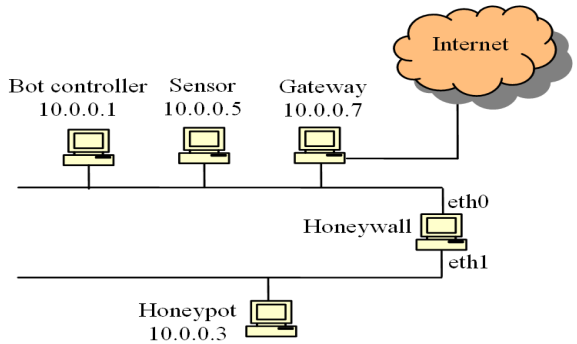

Fig.2: Honeypot

3.1 Type of Honeypots

There are basically 2 ways to classify honeypots. The first classification is based on what the purposes of the honeypots are: production or research purpose. The other way is based on one of the main characteristics of the honeypots: low- or high-interactivity honeypots.

3.1.1 Production / Research

Production honeypots are usually used by commercial organizations to help mitigate risks. This kind of honeypots adds value to the security measures of an organization. They tend to be easy to deploy and maintain and their simplicity keeps the related risks low. Due to their nature and on-purpose lack of flexibility, these honeypots offer very little opportunities for attackers to exploit them in order to perform actual attacks.

Research honeypots are designed to gather information about the attackers. They do not provide any direct value to a specific organization but are used to collect information about what threats organizations may face and therefore better protection methods can be developed and deployed against these threats. They are more complex and involve more risks than the production Honey.

3.1.2 Low / High Interactivity

Low-interactivity honeypots do not implement actual functional services, but provide an emulated environment that can masquerade as a real OS running services to connecting clients. These limited functionalities are often scripts that emulate simple services making the assumption of some predefined behaviour of the attacker. His possibilities to interact with these emulated services are

limited, which make the low-interactivity honeypots less risky than the high-interactivity honeypot. Indeed, there is no real OS or service for the attacker to log on to and therefore the honeypot cannot be used to attack or harm other systems. The primary value of low-interactivity honeypots is detection of scans or unauthorized connection attempts but tend to be not good for finding unknown attacks and unexpected behaviour. Low-interactivity honeypots are often used as production honeypots.
High-interactivity honeypots, do not emulate anything and gives the attacker a real system to interact with where almost nothing is restricted which makes them more risky than the low-interactivity honeypots. These types of honeypots should be placed behind a firewall to limit the risks. They tend to be difficult to deploy and maintain but it is believed that they provide a vast amount of information about attackers allowing the research community to learn more about the blackhat community behaviour and motives. They are usually used as research honeypots
Advantages of Honeypots

(1)Fidelity – Small data sets of high value
(2) Reduced false positives
(3)Reduced false negatives
(4)New tools and tactics
(5)Not resource intensive
(6)Simplicity

Disadvantages of Honeypots

(1) Skill intensive
(2)Limited view
(3)Does not directly protect vulnerable systems
(4) Risks

IV. PROPOSED HYBRID MODEL

A hybrid honeypot model is a combination of low and high interaction honeypot. It also includes anomaly detection technique with combination of neural network. The analyzed data is updated in log and when it caught the intrusion it raises the alarm.

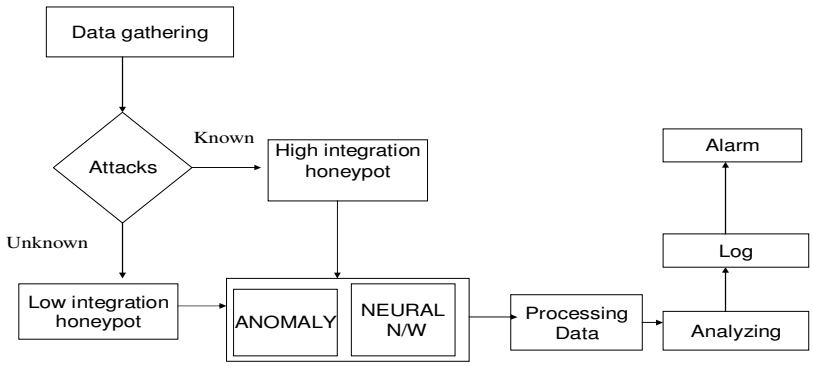

Fig.3: Hybrid Honeypot model

Steps for detecting intrusion in hybrid model:-

Data Gathering: Data is collected over here for detection of intrusion. Data is collected by packet monitoring system. First the packet captured and built some protocols and was able to display them in test program. And then (after getting the source code of it), I used the source code to learn the protocol structures. Now my program supports over 15 protocols. My aim is to add all protocols to my program and to make it available to all. Packet capturing (or packet sniffing) is the process of collecting all packets of data that pass through a given network interface. Capturing network packets in our applications is a powerful capability which lets us write network monitoring, packet analyzers and security tools.

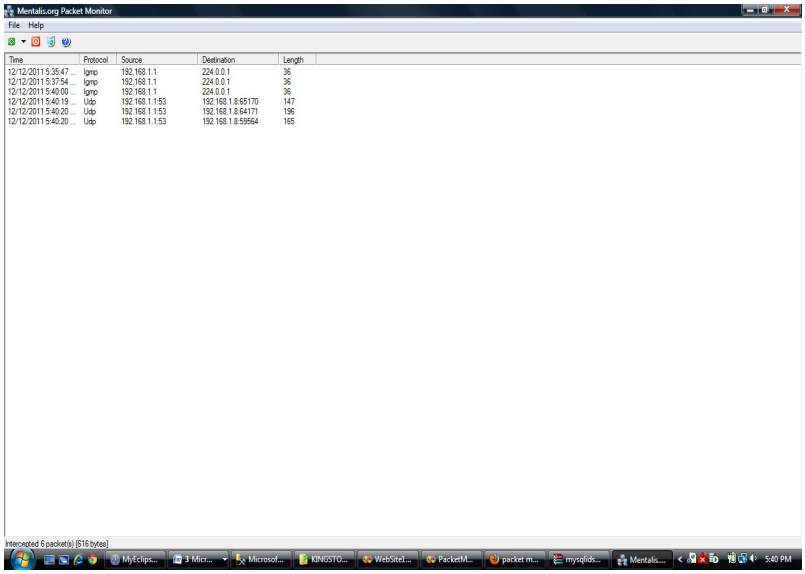

Fig.4: Packet monitoring

For capturing the IP addresses the honeypot is initializing. By starting the monitoring the honeypot start capturing the IP address present in that network. All the activated IP addresses are captured, with their information like time, protocol, source, destination and length. When a new packet arrives the honeypot catches it and display it on the main menu.

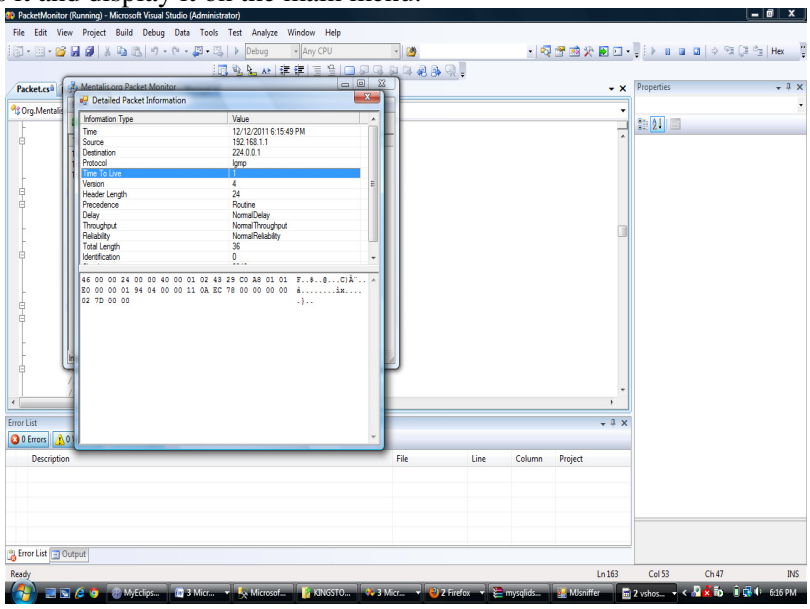

Fig.5: Detailed packet monitoring information.

By clicking on the particular packet(IP address) detailed information can been seen by the user like its time, source, destination, protocol, time to live, version of IP, header length, delay, precedence, reliability, identification etc with its values.

High Interaction/Low interaction Honeypot:-In this data is divided on the basis on known and unknown attack. Known attacks are send to high interaction honeypot and unknown attacks are send to low interaction honeypot. Honeypot is a network security tool written to observe attacks against network services. As a low-interactive honeypot, it collects information regarding known or unknown network-based attacks and uses plug-in for automated analysis.

Anomaly Detection and Neural network:-In this phase anomaly detection techniques and neural network are applied here for detecting intrusions.

Neural network classifier which efficiently and rapidly classifies observed network packets with respect to attack patterns which it has been trained to recognize. This is a feed forward network which uses supervised training, and which:

- can be trained rapidly,
- can be trained incrementally,
- Once trained, can perform fast and accurate classification of its input.

The idea here is to train the neural network to predict a user's next action or command, given the window of 'n' previous actions or commands. The network is trained on a set of representative user commands. After the training period, the network tries to match actual commands with the actual user profile already present in the net.

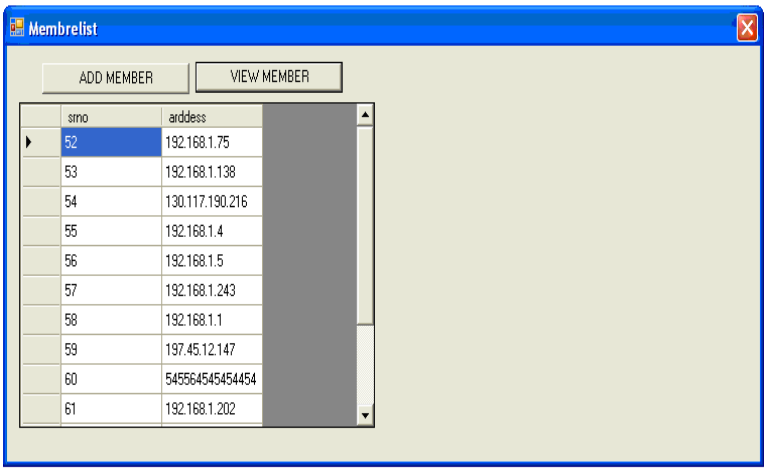

Fig 6: memerlist form

The members added in this list are the authorized user's addresses. System matches with this list when a new IP address enters in network. On the basis of this list Ip address are divided into blacklist and whitelist.
Any incorrectly predicted events actually measure the deviation of the user from the established profile. Advantages:

- They cope well with noisy data.
- Easier to modify for new user communities.
- Their success does not depend on any statistical assumption about the nature of the underlying data. It is used to detect false positive, false negative and detection rate.

Processing Data: - In this data is processed as compared with that stored in backend(database).
Analyzing:-Data in analyzed here and then it send it to the log.
Log: - It is database which consists of three tables.

- First (Blacklist)-It contains the list of IP blocks from the database and generate the output scheme.
- Second (Whitelist)-It consists of IP addresses which should never be added.
- Third(Control list)-It holds the list of valid IP addresses either you own them or because they belong to somebody whom you trust a lot and last time when the data was updated

Table 1: Log table

SR. NO.	IP address	Date
Char(20)	Source address	Time at which it is captured

Alarm:- If honeypot detects an intrusion then it raises an alarm. This is the output may be either an automated response to an intrusion or a suspicious activity alert for a system security officer.

V. RESULT

Performance

The tested performance of the Honeymaze showed significant improvements in the detection accuracy over the single IDS. The improvements were so vast that each and every system trial resulted in a 98% accurate detection at the transition intervals selected within a certain range of deviant node pervasion. The test scenarios varied in the percentage of malicious node pervasion, as well as the number of nodes used in the test.

Table 2: No. of IP addresses captured in 4 weeks

Weeks	No. of IP addresses	Blacklist	Whitelist	False alarm
1	20	4	13	3
2	17	3	11	1
3	14	4	10	1
4	13	4	6	0

These results are based on week's basis. No. of IP addresses are captured by the Honeymaze and then on the basis of memberlist these are categorized in blacklist and in whitelist. These tell about the inside and outside intruders. And the false alarms are also noticed, but they are very less .At the end of week 4 there is no false alarm is raised. So its performance and accuracy is raised.

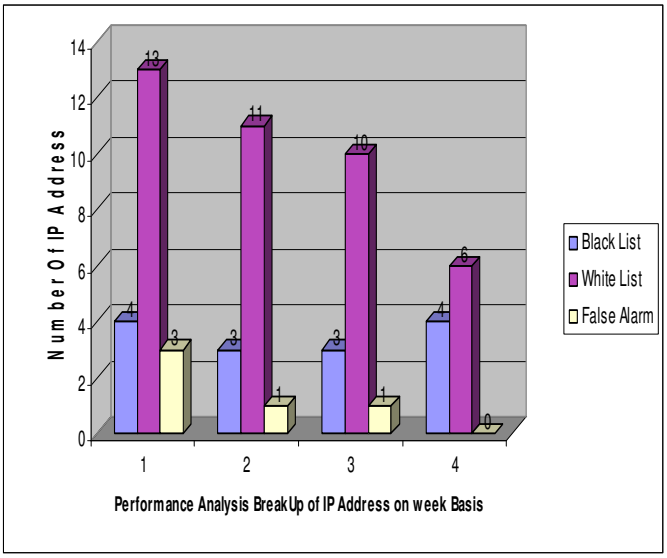

Fig. 7: Performance analysis breakup of ip addresses on week basis

These results show the performance of the honeymaze. It is more accurate then existing honeypots and IDS. It takes less memory and easy to understand. It is highly reliable and flexible. It also detects the viruses. In addition, results indicate that no single architectural parameter alone network IDS capabilities, instead a combination of factors contributes to the sustained performance. In particular, processor speed is not a suitable predictor
Of NIDS performance, as demonstrated by a nominally slower Pentium-3 system Out performing a Pentium-4 system with higher clock frequency. Memory bandwidth and latency is the most significant contributor to the sustainable throughput

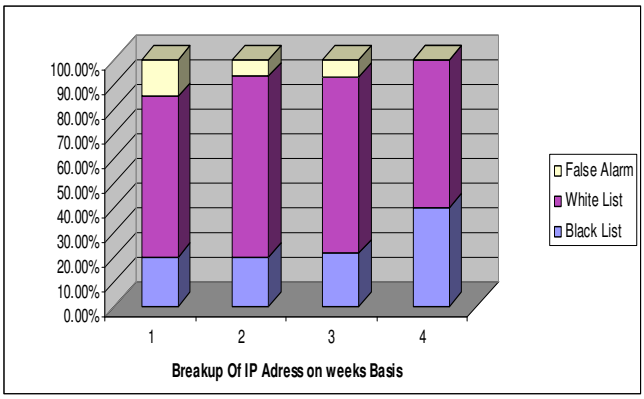

Fig. 8: performance measure

It also detects the viruses present in the system. Firstly it will scan the full system and detects if there are any viruses present in the system and make an alarm and show it with the help of a dialog box. It also tells the path where the virus is detected. This honeypot is very useful in offices etc. It can detect the inside and outside intruders and also detects the viruses. Early honeypot detects only worm, but this honeypot is combination of high and low integration honeypot which is more useful and beneficiary. It also have improved accuracy and performance in detecting intrusions.

VI. CONCLUSION AND FUTURE WORK

The proposed hybrid honeypot architecture system provides a partial protection to the production systems. It fulfills this by decreasing the likelihood of activity of the hacker and is targeting our production systems by employing the lure systems in the network which the hacker cannot come to know about these systems, their status and his fingerprint and consider the fake system as real systems. This cannot complete our goal without employing the redirection capability, and the production system will remain vulnerable to attack for direct assail that do not pass through the conducted honeypot system. In the proposed design, the production honeypot can play only as a passive duty in which they only can log different activities of the attackers, so the system administrator can extract and analyzed them due to data mining. Hybrid honeypots are a highly flexible security tool that can be used in a variety of different deployments. The system detects unauthorized users attempting to enter into a computer system by comparing user behavior to a user profile, detects events that indicate an unauthorized entry and notifies it by raising an alarm. The system also includes a log for storing results. Neural network concept is used to train the system and to reduce false positive, false negative and detection rate. These are a cheap and simple way to add protection to a network and help developing new ways for countering them. In terms of performance, an intrusion detection system becomes more accurate as it detects more attacks and raises fewer false positive alarms.

Future work include the detection of various threats like Dos, worms etc. It performance and detection rate can also be increase. This could play a more active role by analyzing the attacker's activities and decreasing the different attack's type by use of signatures file or a signature database which has the capability of the development and mine the data. As we have shown, the honeypot will be an ability of adding and releasing the warnings, and they can send notice to the administrator, the intruder type and various feasible suggestions to block the attack propagation.

REFERENCES

[1]. Omid Mahdi , Harleen kaur(2011) "An Efficient Hybrid Honeypot Framework for Improving Network Security" Published in (IJCSIS) International Journal of Computer Science and Information Security,Vol. 9, No.2,2011.

[2]. Divya and Amit Chugh(2012), "GHIDS: A Hybrid Honeypot Using Genetic Algorithm Published in IJCTA, Vol. 3. Jan 2012.

[3]. Urjita Thakar, Sudarshan Varma (2005), **"**HoneyAnalyzer – Analysis and Extraction of Intrusion Detection Patterns & Signatures Using Honeypot**"** published in Second International Conference on Innovations in Information Technology.

[4]. Camilo, Viecco(2007) "Improving Honeynet Data Analysis," Information Assurance and Security Workshop, pp. 99.
[5]. Eugene Spafford(1989)."An analysis of the Internet worm" In Proceedings of European Software Engineering Conference, September
[6]. Evan Cooke, Michael Bailey, Z Morley Mao, (2004), *Toward understanding distributed Blackhole placement. In Proceedings of the Second ACM Workshop on Rapid Malcode (WORM), Oct.*
[7]. J. Dike(2001), *"User-mode linux," Proceedings of the 5th annual conference on Linux Showcase & Conference- vol. 5, USENIX Association Berkeley*
[8]. Khattab M, Sangpachatanaruk C,Mosse D, MelhemR,T. (2004)Roaming *honeypots formitigating service-level denial-of-service attacks. In: Proceedings of the IEEE 24th international conference on distributed computing systems March, p. 328–37.*
[9]. Krawetz N(2004). Anti-honeypot technology. *IEEE Security & Privacy Magazine, Vol. 2(1), pp. 76–9.*
[10]. Kreibich C, Crowcroft J(2004)."*Honeycomb: creating intrusion detection signatures using honeypots." ACM SIGCOMM Computer Communication Review ,Vol. 34(1), pp. 51–6.*
[11]. Kuwatly I, Sraj M, Al-Masri Z, Artail H.(2004),"*A Dynamic honeypot design for intrusion detection. In : Proceedings of IEEE/ACS international conference On pervasive services, p. 95–104, July.*
[12]. Lok Kwong Yan. (2005),"*Virtual honeynets revisited," Information Assurance Workshop, pp 232-239.*
[13]. Mark Eichin and Jon A. Rochlis.(1989) *With microscope and tweezers: An analysis of the Internet Virus of November 1988. In Proceedings of the 1989 IEEE Symposium on Security and Privacy.*
[14]. Michael Vrable, Justin Ma, Jay Chen, David Moore, Erik Vandekieft, (2005)"*Scalability, _delity, and Containment in the Potemkin virtual honeyfarm". In Proceedings of the 20th ACM Symposium on Operating Systems Principles (SOSP), October.*
[15]. Omid Mahdi Ebadati E., Harleen Kaur and M. Afshar Alam.*(2010)"A Performance Analysis of Chasing Intruders by Implementing Mobile Agents". Int. Journal of Security (IJS), Vol. 4, No.4, pp 38-45.*
[16]. Omid Mahdi Ebadati E.,Kaur H., Alam A.M.(2010), *"A Secure Confidence Routing Mechanism Using Network-based Intrusion Detection Systems", OLS Journal of Wireless Information Networks &Business Information System, Open Learning Society.*
[17]. P. Barham, B. Dragovic, K. Fraser, S. Hand, T. Harris, A. Ho, (2003)and A. Warfield, *"Xen and the Art of virtualization," ACM SIGOPS Operating Systems Review, vol. 37, pp. 164-177, 2003.*
[18]. Spitzner L.(2002) *Honeypots: tracking hackers. Addison- Wesley,</www.tracking-hackers.com/>.*
[19]. Teo L, Sun A,AhnJ. *Defeating internet attacks using risk awareness and active honeypots(2004). Proceedings of the second IEEE international information assurance workshop, p.p. 155 Virtual PC*
[20]. *"Understanding Intrusion Detection System" by SANS inst. Reading room.*
[21]. Hichem Sedjelmaci and Mohamed Feham(2011), *NOVEL HYBRID INTRUSION DETECTION SYSTEM FOR CLUSTERED WIRELESS SENSOR NETWORK published in International Journal of Network Security & It's Applications (IJNSA), Vol.3, No.4, July 2011.*
[22]. P. KIRAN SREE , Dr I Ramesh Babu, Dr J.V.R.Murty, R.Ramachandran, N.S.S.S.N Usha Devi, *Power-Aware Hybrid Intrusion Detection System (PHIDS) using Cellular Automata in Wireless Ad Hoc Networks* Issue 11, Volume 7, November 2008
[23]. Muna Mhammad T. Jawhar, Monica Mehrotra(2009), *Design Network Intrusion Detection System using hybrid Fuzzy- Neural Network, published in First International Conference on Computational Intelligence, Communication Systems and Networks ; 978-0-7695-3743-6/09*
[24]. Niels Provos(2004), *"A Virtual Honeypot Framework", In Proceedings of the 13th Usenix Security Symposium, San Diego, CA, August 2004, Pp. 1–14.*
[25]. Christian Kreibich, Jon Crowcroft, *"Honeycomb-Creating Intrusion Detection Signatures" Using Honeypot, ACM SIGCOMM Computer Communication Review Archive Volume 34,Issue1 January 2004, Pp. 51 – 56.*
[26]. Erwan Lemonnier, Defcom,*"Protocol Anomaly Detection in Network-based IDSs", http://erwan.lemonnier.free.fr/.*
[27]. Lance Spitzner, *"Honeypots: Simple, Cost-Effective Detection", http://www.securityfocus.com/infocus/1690.*
[28]. Martin Roesch, *"Snort – Lightweight Intrusion Detection for Networks", Proceedings of USENIX 13th System Administration Conference, Nov.99.*
[29]. Yuqing Mai, Radhika Upadrashta and Xiao Su, *J-Honeypot: A Java-Based Network Deception Tool with Monitoring And Intrusion Detection, Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'04) Volume 1 April 05 - 07,2004, Pp. 804-808.*
[30]. Hyang-Ah Kim, Brad Karp, *"Autograph: Toward Automated, Distributed Worm Signature Detection," In Proceedings. of the 13th Usenix Security Symposium San Diego, CA, August 2004. Pp. 271–286*

[31]. Peng Ning, Dingbang Xu,*"Learning Attack Strategies from Intrusion Alerts" in Proceedings of the 10th ACM Conference on Computer and Communications Security, October 2003, Pp 200*
[32]. Peng Ning, Yun Cui, Douglas Reeves, and Dingbang Xu,*"Tools and Techniques for Analyzing Intrusion Alerts," In ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, Pp 273-318.*
[33]. Vinod Yegneswaran, Jonathon T. Giffin, Paul Barford, and Somesh Jha.(2005) *An Architecture for Generating Semantics-Aware Signatures. In 14th USENIX Security Symposium, Baltimore, Maryland, August.*
[34]. V.V. Patriciu, I. Priescu(2003), *"Using Data Mining Techniques for increasing Security in E-mail System Internet- based", in 11th Conference CAIM*.
[35]. V. Paxson(1998), *.Bro: A System for Detecting Network Intruders in Real-Time, Computer Networks (Netherlands: 1999), vol. 31, no. 23, pp. 2435.2463.*
[36]. M. Roesch(1999),*Snort: Lightweight Intrusion Detection for Networks, In Proceedings of the 13th Conference On Systems Administration,1999, pp. 229-238.*
[37]. C. Stoll, *The Cuckoo's Egg. Addison-Wesley, 1986.*
[38]. W. R. Cheswick,*An Evening with Berferd, in which a Cracker is lured,endured And studied, in Proceedings of The 1992 Winter USENIX Conference, 1992.*
[39]. L. Spitzner, *Honeypots: Tracking Hackers. Addison-Wesley, 2003.Available: http://www.tracking-hackers.com/book/*
[40]. N. Provos, *Honeyd - A Virtual Honeypot Daemon in 10th DFN-CERT Workshop, Hamburg, Germany, February 2003.*
[41]. D. Gus_eld, Algorithms on Strings, Trees and Sequences. Cambridge University Press, 1997.
[42]. P. Weiner, *Linear pattern matching algorithms, in Proceedings of the 14th IEEE Symposium on Switching And Automata Theory, 1973, pp. 1.11.*
[43]. E. McCreight, *.A space-economical suf_x-tree construction algorithm,Journal of the ACM, vol 23, pp. 262.272, 1976.*
[44]. E. Ukkonen,*On-line construction of sufIx trees,.Algorithmica,pp. 249.260,1995.*
[45]. S. McCanne and V.Jacobson,tcpdump/libpcap,www.tcpdump.org1994.

Divya has completed her B.Tech in I.T from R.G.E.C, Meerut, U.P (U.P.T.U) and pursuing her M.Tech in CSE from L U, Faridabad, Haryana, India. Currently she has published Research papers in 6 National/ International Journals and Conferences. Her area of interest is system and network security.

Amit Chugh has completed his B.Tech in C.S from B.R.C.M College, Bahal, Haryana (M.D.U) and M.Tech in CSE from ITM College Gurgaon, Haryana, India. Currently he is working in Lingaya's University, Haryana from last two years. He has published Research papers in 6 National/International Journals and Conferences. His area of interest is network security.