ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

A Novel Approach to Identify the Intruders in the Network with Snort and Honey Pot

K.Meghana[1], B.Naseeba[2]

M. Tech Student, Department of CSE, Vizag Institute of Technology, Dakamarri, Visakhapatnam, Andhra Pradesh, India[1]

Assistant Professor, Department of CSE, Vizag Institute of Technology, Dakamarri, Visakhapatnam, Andhra Pradesh, India[2]

ABSTRACT: Now a day's the usage of the internet and electronic gadgets are increased. Identification of Authorized users and intruders in the network is became problem. Intrusion detection system is used for detect the intruders in the network. SNORT is an intrusion detection system to identify the intruders, in this paper we used SNORT. Honey pot is helpful to identify the un authorized users in the network, here we used Nmap to identify the au authorized users in the network. We identified the intruders and un authorized users and the results are shown.

KEYWORDS: SNORT, Nmap, Intruders, Honey pot.

I. INTRODUCTION

Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level. Intruders have signatures, like computer viruses, that can be detected using software. You try to find data packets that contain any known intrusion-related signatures or anomalies related to Internet protocols. Based upon a set of signatures and rules, the detection system is able to find and log suspicious activity and generate alerts. Usually an intrusion detection system captures data from the network and applies its rules to that data or detects anomalies in it. Snort is primarily a rule-based IDS, however input plug-ins are present to detect anomalies in protocol headers.

Authentication is any process by which you verify that someone is who they claim they are. Authorization is any process by which someone is allowed to be where they want to go, or to have information that they want to have. we identified three factors that are used in positive authentication of a user[2]. We also pointed out in the previous section that while these factors are in themselves good, there are items in some that suffer from vulnerabilities.

A. AUTHENTICATION METHODS

Different authentication methods are used based on different authentication algorithms. These authentication methods can be combined or used separately, depending on the level of functionality and security needed. Among such methods are: password authentication, public-key authentication, Anonymous authentication, remote and certificate-based authentication.

i. Password Authentication

The password authentication methods are the oldest and the easiest to implement. They are usually set up by default in many systems. Sometimes, these methods can be interactive using the newer keyboard-interactive authentication. Password authentication includes reusable passwords, one-time passwords, challenge response passwords, and combined approach passwords.

ii. Secure Socket Layer (SSL) Authentication

Secure Socket Layer (SSL) Authentication is an industry standard protocol designed by Netscape Communications Corporation for securing network connections. SSL provides authentication encryption and data integrity using public key infrastructure (PKI). SSL authentication being cryptographic based uses a public / private

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

key pair that must be generated before the process can begin. Communicating elements acquire verifications certificate for a certificate Authority (CA).

A certificate authority is a trusted third party, between any two communicating elements such as network servers, that certifies that the order two or more entities involved in the intercommunication, including individual users, databases, administrators, clients, servers, are who they say they are. The certificate authority certifies each user by verifying each users identity and grants a certificate, signing it with the certificate authorities private key. Up on the verification, the certificate authority then publishes its own certificate which includes its public key. Each network entity, server, database and others gets a list of certificates from all the trusted CAs and it consults this list every time there is a communicating user entity that needs authentication. With the CA's issued certificate, the CA guarantees that anything digitally signed using that certificate is legal. Sometimes it is possible to also get a private key along with certificate, if the user does not want to generate the corresponding private key from the certificate. As e-commerce picks up momentum, there is an increasing need for a number of creditable companies to sign up as CA's. And indeed many are signing up. If the trend continues, it is likely that the use of digital certificates issued and verified by CA as part of a public key infrastructure (PKI) is likely to become a standard for future e-commerce.

B. HONEY POTS

A honey pot is a trap set to detect, analyze, or in some manner counteract attempts of unauthorized use of information systems. Generally, it consists of a computer, data, or network site which seems to contain information or resources of value to attackers, but is actually isolated, protected, and monitored.

i. Variations of Honey pots According to Their Interaction Level

There are two main categories of honey pots: Low-interaction and high interaction. Low-interaction honey pots are passive, and cyber attackers are limited to Emulated services instead of actual operating systems[4]. They are generally easier to deploy and pose minimal risk to the administrators. Examples of low interaction honey pots are Honeyd, LaBrea Tarpit, BackOfficer Friendly, Specter, and KFSensor.

High-interaction honey pots provide working operating systems and applications for attackers to interact with. They are more complex and serve as better intelligence-collection tools. However, they pose a higher level of risk to the administrator due to their potential of being compromised by cyber attackers, as for instance, with the use of compromised honey pots to propagate other attacks. Examples are the Symantec Decoy Server (formerly ManTrap) and honey nets as an architecture (as opposed to a product or software).

Table 1. Honey pots according to interaction level

Low-interaction	High-interaction
Honeypot emulates operating systems, services and network stack.	Full operating systems, applications, and services are provided.
Easy to install and deploy. Usually requires simply installing and configuring software on a computer.	Can be complex to install and deploy (although commercial versions tend to be simpler).
Captures limited amount of information, mainly transactional data and some limited interaction.	Can capture far more information, including new tools, communications, and attacker keystrokes.
Minimal risk of compromise, as the emulated services control what attackers can and cannot do.	Increased risk of compromise, as attackers are provided with real operating systems with which to interact.

ii. Types of Honey pots According to Their Purpose

Honey pots can be deployed as production or research systems. When deployed as production systems, typically in an enterprise or military network, honey pots can serve to prevent, detect, bait, and respond to attacks. When deployed as research systems, typically in a university or institute, they serve to collect information on threats for analysis, study, and security enhancement.

iii. Types of Honey pots According to Their Implementation

Another distinction exists between physical and virtual honey pots. Physical means that the honey pot is running on a real machine, suggesting that it could be high-interaction and able to be compromised completely. Physical honey pots are expensive to maintain and install, making them impractical to deploy for large address spaces.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Virtual honey pots use one real machine to run one or more virtual machines that act as honey pots. This allows for easier maintenance and lower physical requirements.

While reducing hardware requirements for the administrators, virtual honeypots give cyber attackers the perspective of independent systems in networks. This reduces the cost of management of the honeypots for production and research, compared to physical honeypots. There are, however, disadvantages. The use of the virtual machines is limited by the hardware virtualization software and the host operating system. The secure management of the host operating system and virtualization software has to be thoroughly planned and executed in order to prevent attackers from seizing control of the host system, and eventually the entire honeynet. It is also easier to fingerprint a virtual honeynet, as opposed to honeynets deployed with real hardware, by the presence of virtualization software and signatures of the virtual hardware emulated by the virtualization software. Cyber attackers may potentially identify these signatures and avoid these machines, thereby defeating the purpose of deploying the honeynet.

iv. Types of Honeypots According to Their Side

The last distinction is between server-side and client-side honeypots. Traditional, server-side honeypots are servers which wait passively to be attacked, possibly offering bait. Client honeypots, by contrast, are active devices in search of malicious servers or other dangerous clients[6]. The client honeypot appears to be a normal client as it interacts with a suspicious server and then examines whether an attack has occurred. The main target of client honeypots is Web browsers, but any client that interacts with servers can be part of a client honeypot, including SSH, FTP, and SMTP.Examples of client honeypots are HoneyC, HoneyMonkey, HoneyWare, and HoneyClient.

v. Honey Nets

The value of honeypots can be increased by building them into a network; two or more honeypots on a network form a honeynet [2]. Integrating honeypots into networks can provide cyber attackers a realistic network of systems to interact with, and permits defenders a better analysis of distributed attacks.

vi. Monitoring Tools in a Honeypot

Honeypots typically contain a set of standard tools, including a component to monitor, log, collect, and report the intruder's activity inside the honeypot. The goal is to capture enough data to accurately recreate the events of the honeypot.

Data collection can be done in many ways, the most important of which are:

- Honeypot log files
- Packet sniffing (network sniffing or intrusion detection systems)
- Keystroke logging (or keylogging)
- Snapshot software
- Firewall logs

As part of the defense-in-depth approach to information security (multiple layers of security controls), and a critical part of honeypot architecture, intrusion detection systems are deployed to detect potential incoming threats based on signature sets or anomalies[8]. Although they are passive, they can overwhelm administrators with alerts instead of responses or actions against detected attacks. To address this problem, intrusion prevention systems can be used with higher thresholds for alerts; they extend the detection capability of IDS to include automated controls in response to cyber-attacks. For instance, they can ignore, block, or modify packets, preventing the success of the exploit. This active capability, however, comes at a cost to the performance of protected networks or systems. Snort is probably the most popular and well-known intrusion-detection system. It is useful in disabling attacks on a honeypot and for later analysis of the data, with the goal of detecting and understanding cyber-attacks against honeypots.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Table II Characteristics of some honeypots and ways to detect them

Honeypot / Honeynet	Typical Characteristics	Methods for Detecting the Honeypot
Back officer Friendly	Restricted emulation of services and responses	Send different requests and verify the consistency of responses for different services.
LaBrea Tarpit	TCP window size 0; bogus MAC address	Check persistent TCP window size 0 and MAC address (0:0:0:f:ff:ff)
Honeyd	Signature based responses same clock for every host	Send a mixture of legitimate and illegitimate traffic, with common signatures recognized by targeted honey pots. Analyze timestamps of the hosts.
Snort IPS	Modification actions; suspicious packets could be dropped or modified.	Send different packets and verify the existence and integrity of response packets.
Virtual Honey net (VMware)	Virtualization and system files	Detect virtual hardware by name and VMware MAC address. Probe for existence of VMware.
Active tcpdump session or sebek	Logging processes	Scan for active logging process or increased round trip time (for instance, due to read() in sebek- based honeypots.

We will describe the applications used in the implementation, with a quick analysis of the methods to detect them, some countermeasures, and finally the software used to analyze the results.

II. RELATED WORK

Helen and Richard in 2010 presented a paper on Internet security and intrusion detection which highlights the principal attack techniques that are used in the Internet today and possible countermeasures. In particular, intrusion detection techniques are analyzed in detail[1]. This paper mixes a practical character with a discussion of the current research in the field.

In 2009, Srinivas and Ramakrishna suggested the use of neural networks and support vector machines in intrusion detection[3]. Their paper on Intrusion detection using neural networks and support vector machines describes these approaches to intrusion detection and also compares the two methods.

In 2008, Chen and Sung incorporates soft computing techniques into a probabilistic intrusion detection system. There are a lot of industrial applications that can be solved competitively by hard computing, while still requiring the tolerance for imprecision and uncertainty that can be exploited by soft computing[5]. This paper presents a novel intrusion detection system (IDS) that models normal behaviors with hidden Markov models and attempts to detect intrusions by noting significant deviations from the models. At almost the same time, Abouzakhar and Nasser came up with An intelligent approach to prevent distributedsystems attacks. This paper proposes an innovative way to counteract distributed protocols attacks such as distributed denial of service (DDoS) attacks using intelligent fuzzy agents. Cansian and Adriano in the paper An attack signature model to computer security intrusion detection mention internal and external computer network attacks or security threats occur according to standards and follow a set of subsequent steps, allowing to establish profiles or patterns. This well-known behavior is the basis of signature analysis intrusion detection systems. This work presents a new attack signature model to be applied on network-based intrusion detection systems engines.

In 2009, Xiang and Daxin in their paper Generating IDS attack pattern automatically based on attack tree illustrate the generation of attack pattern automatically based on attack tree[7]. The extending definition of attack tree is proposed and the algorithm of generating attack tree is presented. The method of generating attack pattern automatically based on attack tree is shown, which is tested by concrete attack instances. The results show that the algorithm is effective and efficient. The efficiency of generating attack pattern is improved and the attack trees can be reused.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

III. PRESENTATION OF THE MAIN CONTRIBUTION OF THE PAPER

Every week, we made a quick analysis of all the information available, using some programs and tools to assist us. At the end of the study, we made a more detailed review. As we learned what worked and what did not, we used different logs, scripts, tools, and software to better analyze the information captured. This approach required some changes in the methodology and log formats, and as a result, there was a significant difference in the amount of work and information available between the first and last weeks. We noticed that some of the default formats of the logs are not easy to order or parse for analysis, such as the text alert logs created by Snort.

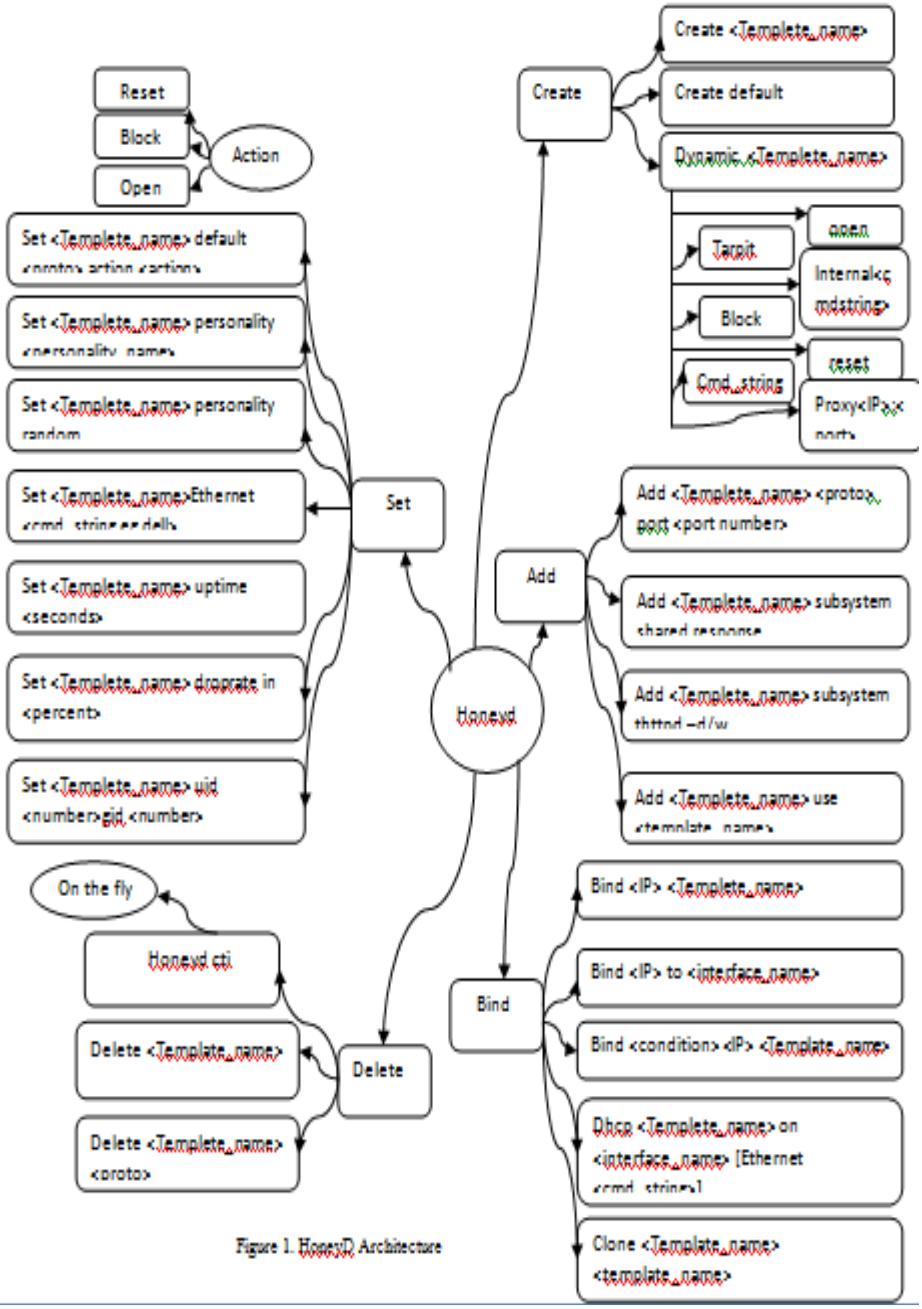

Figure 1. HoneyD Architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

The procedure of the honeyd is first create the template then set the template after set it add the template then bind the template to a particular IP Address. Here we created some shell scripts which are used to identify the attacker in the honeypot.

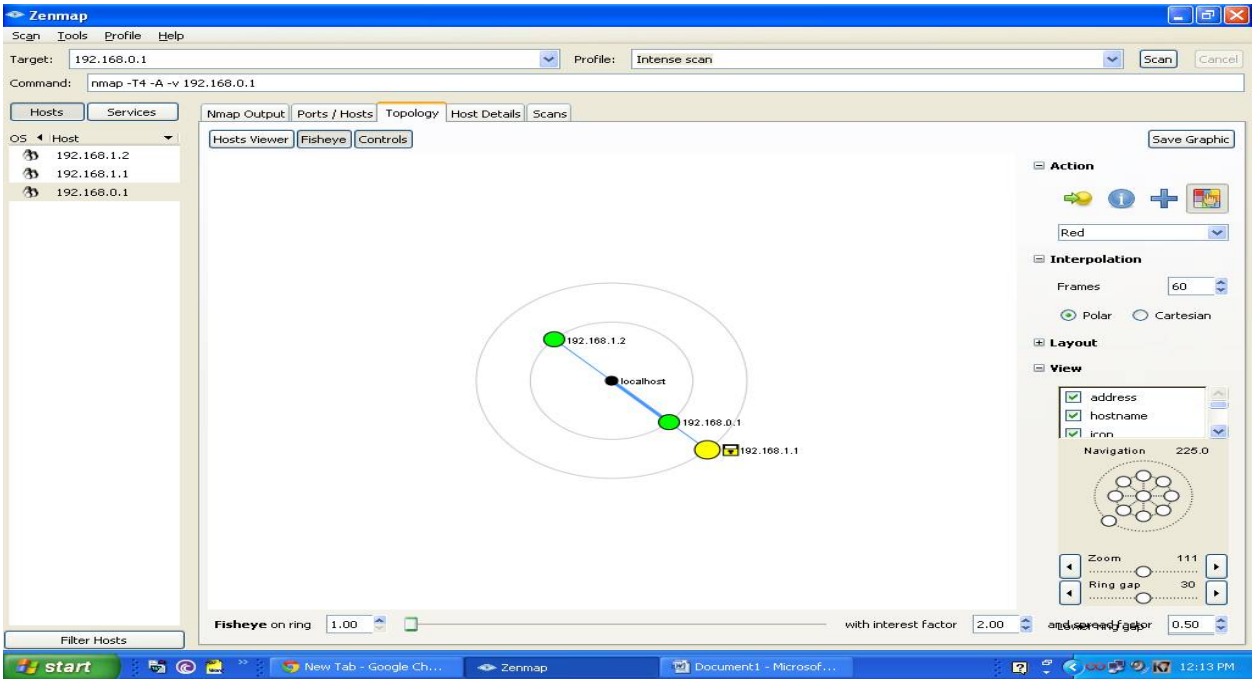

Fig 2. My Honey Pot Topology

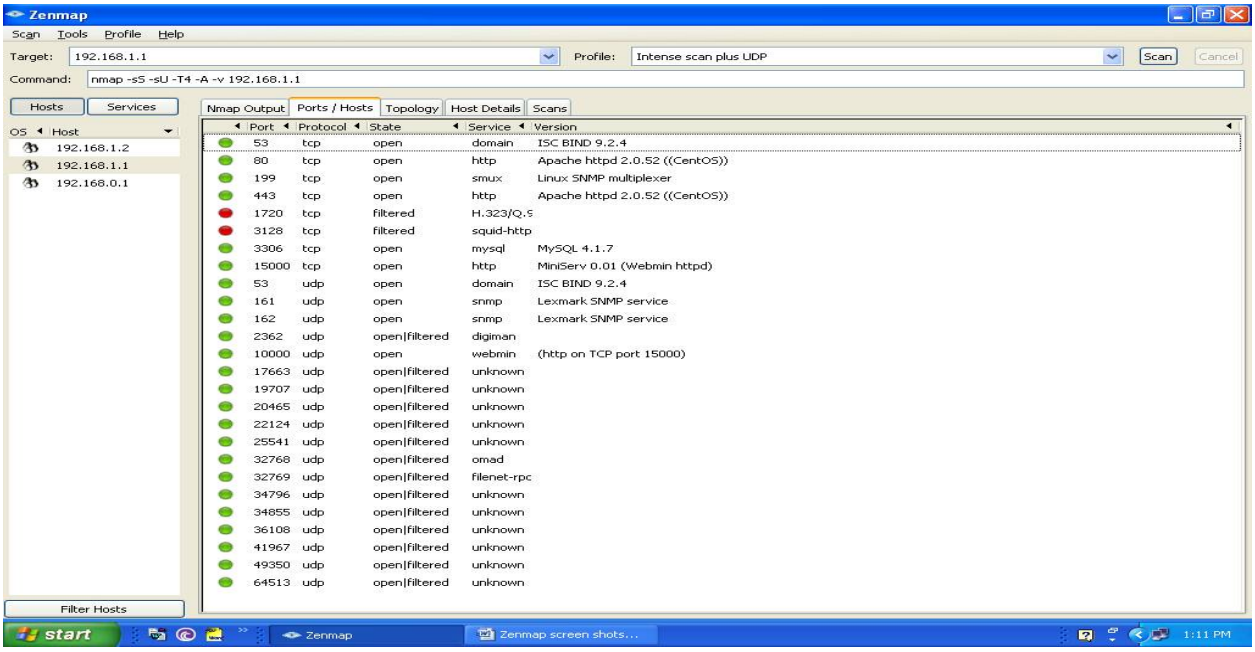

Fig 3. Host Details in the Topology

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

IV. CONCLUSIONS

This paper explains how to identify the intruders and un authorized authors in the network. The results and screen shots are shown in the above section with the results we can identify the intruders. The Nmap and Snort are used in this paper to detect the intruders and un authorized users. The snort rules are very helpful to detect the user behavior, and based the user behavior we segregate the authentication of the users. We established the lab and continuously thirty days we observed the users and their behavior to identify the intruders in the network.

REFERENCES

1. F Richard Yu, Helen Tang, "Distributed node selection for threshold key management with intrusion detection in mobile ad hoc networks", International Journal of Wireless Networks, pp.787-794, 2010.
2. Dr. R.China Appala Naidu, K. Meghana, P.S.Avadhani and I. Uma Maheswara rao, " New Approach of Authentication Method based on Profiles", Proceedings of the 2016 IEEE 3rd International Conference on Recent Advances in Information Technology (RAIT-2016), Indian School of Mines(ISM), Dhanbad, Jharkhand, India, ISBN No. 978-1-4799-8578-4, pp. 347-351, March 2016.
3. Sivakumar Ramakrishna, Sujatha Srinivasan, "Intelligent agent based artificial immune system for computer security", International Journal of Artificial Intelligence Review, pp.13-43, October 2009.
4. M. Divya Sai , Dr.R.China Appala Naidu, Sudha Rani.V M.SaiKrishna Murthy and K.Meghana, " An Advanced Authentication system for multi server environment With Snort" IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI-2016), 20-25 Sep 2016.
5. Pei Te Chen, Chi Sung Laih, "an intrusion detection system with identification capability", International Journal of information Security, pp.185-197, 2008.
6. R.China Appala Naidu, A.Prakash, Vinod P.K and Sreenivasa Rao.T " An Efficient Approach to Identify the Information Loss with Snort in Wireless Technology" International Journal of Advanced Research in Computer Science and Software Engineering ISSN : 2277-128X, Volume 5, Issue 2, Pp.862-866, February 2015.
7. Daxin Tian,Yanherng Liu,Yang Xiang, "Large scale network intrusion detection based on distributed learning algorithm", International Journal of information Security, Vol.8(1), pp.25-35, 2009.
8. R.China Appala Naidu and P.S.Avadhani "An Effective Evolution of Packet Loss With SNORT" InternatIonal Journal of Computer Science and Technology(IJCST) ISSN : 0976-8491 (Online) | ISSN : 2229-4333 (Print), IJCST Vol. 4, Issue 3, July - Sept 2013.

BIOGRAPHY

K.Meghana doing M.Tech in Computer science and Engineering at Vizag Institute of Technology, Dakamarri,Vishakapatnam, under JNTU Kakainada . She received B.Tech degree in 2014 at GMR Institute of Technology, JNTU Kakainada. Areas of interest are information security and wireless networks.

B.Naseeba, Assistant professor in Computer science and Engineering at Vizag Institute of Technology, Dakamarri,Vishakapatnam, under JNTU Kakinada. She received B.Tech from GITAM University in 2008 and M.Tech from Samskruthi college of Engineering and Technology, under JNTU Hyderabad in 2014. Her Areas of interest are information security, Ad hoc networks and Data ware Housing & Data Mining.