MONITORING WEB TRAFFIC AND TRACKING ATTACKER ACTIVITIES USING HONEYPOTS
S.Vignesh¹, D.Revathi²

¹ B.Tech-IT -IV Year, Srizidya College of Engineering & Technology, Tamilnadu, India
² Asst.Prof/IT, Srividya College of Engineering & Technology, Tamilnadu, India
Vignesh.sinfect@gmail.com¹, revathi.durairaj11@gmail.com²

ABSTRACT
A honeypot is an intrusion prevention system that are use to maintain the internet web traffic through monitoring the network and tracking the attackers activities using log files generation the file can go larger in size and might be difficult to handle so dynamic allocation of the log file should be processed. The data being monitored using some of the applications using firewall, snort, port scanners ,vurnability scanners etc….the result shows minimizing the log file and identifying the attacker through his ip address output of this experiment will shown in the form of the graph.

I. INTRODUCTION
Due to the improvement in the technology internet usage have being more since after the network technology have under gone a step to make the world a small planet, so that hackers are skilled enough to break into system to steal data from industries which they do not belong too. Currently firewall and IDS systems are used to have defense towards this illegal activities .

Intrusion Detection System (IDS)
The system holds the key information on data that are monitored by the application like firewall and malware detecting software .if a system is being targeted by a network attack there are two types of (IDS);host based (HIDS)and networkbased(NIDS) each of those technique has advantage and disadvantage .Host based IDSs examine the individual computer that serves as the host Examples of hostbased IDS windows NT2000 security logs on the other hand network based IDS are used to analyze the original data ,they are compared with well defined patterns that are already set. SNORT is a open source (NIDS) that can be used in real analysis of data traffic.

Intrusion Prevention System (IPS)
Instruction prevention system are network security appliances that monitor network and system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about said activity, attempt to block/stop activity, and report activity. Intrusion prevention systems are considered extensions of intrusion detection systems because they both monitor network traffic and system activities for malicious activity. The main differences are, unlike intrusion detection systems, intrusion prevention systems are placed in-line and are able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, unfragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options.

II Literature Survey
Honeypot based Secure Network System
Honeypots are a computer specifically designed to help learn the motives, skills and techniques of the hacker community and also describes in depth the concepts of honeypots and their contribution to the field of network security.

Honeyd: A Virtual Honeypot Daemon
This paper presents Honeyd, a framework for virtual honeypots that simulates virtual computer systems at the network level.

On Recognizing Virtual Honeypots and Countermeasures
Honeypots are decoys designed to trap, delay, and gather information about attackers. It can use honeypot logs to analyze attackers’ behaviors and design new defenses.

An Advanced Honeypot System for Efficient Capture and Analysis of Network Attack Traffic
The logs generated by honeyd can grow very large in size when there is heavy attack traffic in the system, thus consuming a lot of disk space.
III EXISTING SYSTEM
Problem identification
In the existing system vulnerable to logging of failed connections in detection system, it attempts only occurs when services are not listening on a scanned port. Log files in the existing system are not encrypted. Unauthorized user can hack the log files.

IV PROPOSED SYSTEM
The Main problem in existing system is insecure of the log files. In proposed system log files are encrypted using AES (advance encryption standard) algorithm.

Positioning of the honeypot
The honeypot is positioned to receive the capturing of data to which can be used to analysis the data through which can be used to allow network traffic of data. It is positioned next to firewall in the network.

Logging
Logging is which used to collect the information about the person who are using the network. The framework uses sys log to store the information on the system. In most situations, we expect that Honeyd runs in conjunction with a NIDS.

Capturing Packets
Packet capture is the act of capturing data packets crossing a network. First the data is captured the anonymus data, then the packets which is from accepted IP address is register to log files.
Processing and storing
The processing of the log is done by changing the format of the records slightly. A couple of new fields are added that help in doing this job. A number of records are considered at a time and they are processed to find whether they belong to a particular flow. The processing module waits for these numbers of records and then starts execution. By flow we mean that the packets have same source IP address, source port, destination IP address, destination port number, flags Any Thus, in the worst case also the log is not going to increase. From the knowledge of attack traffic and the tools that are used to attack it can be easily verified that it is very less probable case. Hence the system is going to decrease the log size in most of the cases without losing information.

Analyse the capture packets

The log files are secured using AES algorithm AES is based on a design principle known as a substitution-permutation network, and is fast in both software and hardware AES is which has a fixed block size of 128 bits

AES Description
Key Expansion—round keys are derived from the cipher key.
Initial Round Add Round Key—each byte of the state is combined with the round key using bitwise xor.
Rounds Sub Bytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
ShiftRows—a transposition step where each row of the state is shifted cyclically a certain number of steps.
MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.

AddRoundKey
Final Round (no MixColumns)
SubBytes
ShiftRows
AddRoundKey

V CONCLUSION
The experiment will show the improvement in the web traffic. IPS system which is used to have only authorizes access of data to be viewed by the user comparing to the previous research the data traffic could be reduced.

VI FUTURE ENHANCEMENT
Main drawback of this is that honeypots is that is the attacker find out that honeypot is present that attacker will not get caught so I have planned to make a disguise so that the honeypot for more effective usage of the Instrustion prevention system.
VII RESULT ANALYSIS

VIII REFERENCES