# THE RESEACH AND DESIGN OF HONEYPOT SYSTEM IN THE LAN SECURITY

Prof .R.V.Agawane , Mr.JagrutiNaikare, Ms.ChaitraliLonkar, Ms. AparnaSawant,

**Abstract** - The purpose of this paper is to design a system that detects the attacker on the system, storing the information about the attack such as the IP address of the attacker, day and date and timing. Also the type of attack we have implemented such as E-mail scan, Socket scanner port scanner. This software we have specially designed for providing security to the LAN. Also we have implemented a client module which will run on the LAN.In e-mail scan we scan mails and deleted the spam mails. In port scanner we scan the ports to check which portsare opened or not. In packet scan we capture the packets.

***Keywords: Honeypot, HoneyTrap, LAN Security, Honeypot in LAN Security, honeynet***

## I. INTRODUCTION

Now a days the attacks are increasing very rapidly hence controlling them and maintaining its LOG is being difficult. Especially in LAN it becomes difficult for the admin to control the attacks that are been made. In LAN the attackers are mostly attracted by the servers. Since all the data is provided on server. So providing security to Server is important task.Moreover the attackers are hidden. So it becomes difficult for the admin to know the attack. Hence the concept of Honeypot was introduced. If the information regarding the attacker is known then it becomes useful in future.

.

## II. Related Work

The Cuckoo's Egg and Evening with BerferdClifford Stoll was been developed by them in 1990/1991[5].CyberCop was the first commercial honey pot developed who's developer was Alfred Huger. In this a single honeypot could control all the other computers in a network. It was found Cyber Cop Sting to be limited, since attackers could only connect to certain ports and read the banners.Also some Honeypot tools/ software are available such as SNORT-INLINE 12, SEBEK. Snort- Inline Snort to block and disable attacks instead of just detecting them. Sebekprovided a means to capture hacker activities in Honey Pots by logging their keystrokes in them[1].

## III. System Objectives and Goals

The objective of the system is to create a dummy server that is honeypot server. The attackers then attack this sever. The Objective of the attacker is to keep the log of the attacks being made to it. The admin gets the detail LOG of the whole day. Also SMS facility is given so if the admin is not present there then he can get the details through mail. The Goal of this system is to reduce the amount of attack being made and secure the LAN form it.

## IV. System Architecture

The system is software which does all the functioning. In this we there is a LAN out of which one is the Honeypot server all the other are the clients. The main software is run on the Honeypot Server. In the architecture there is a LAN connected. The modules of our project are shown. There is a Honeypot server. Computers are connected in LAN by the Switch.

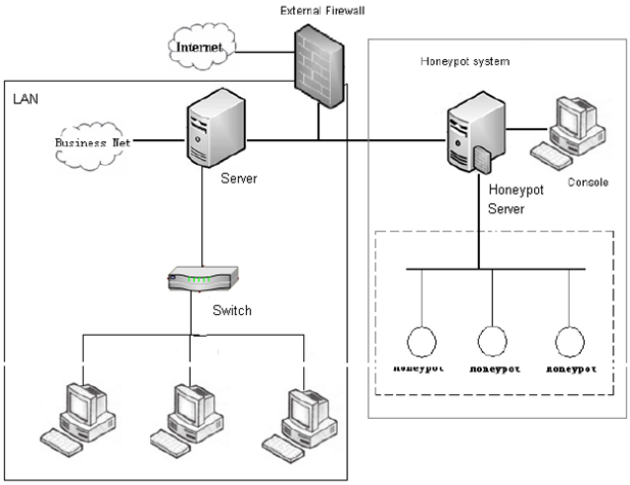


Fig 1. System architecture

This system includes 4 modules :

## A. Port Scanner

In this we have to give certain range of port numbers. The module then scans and tell which ports are listening ie which are used currently and which are not listening. A log is created which specifies the details about the listening port and the date and time. This module is displayed in fig. 2.

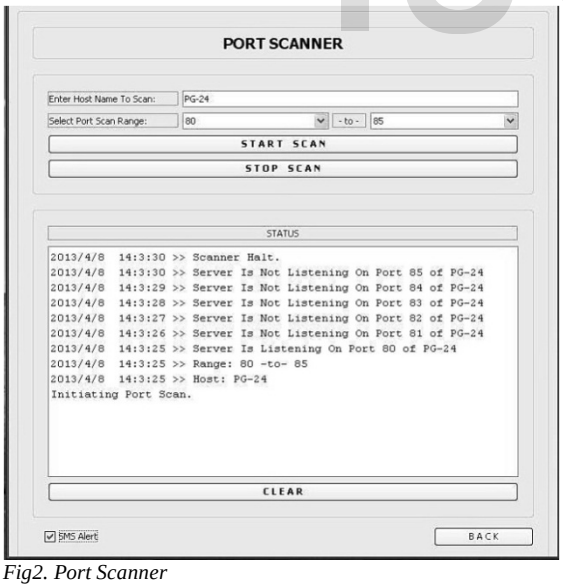


*Fig2. Port Scanner*

## B. Socket Scanner

In this we capture the incoming packets which are coming to the honeypot system. The real time IDS (Intrusion Detection System) is used for this module. The IPAddress of the incoming packet is tracked and the IPAddress is blocked. The blacklisted IPAddress are then saved in a DAT file for further use. Also we have provide a functionality of SMS alert. If Admin is not present there then if he checks the SMS alert button SMS is send on his no regarding the attack. This module is displayed in fig. 3.

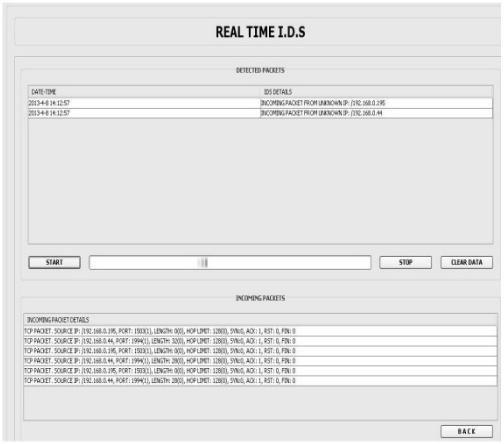


*Fig 3. Socket Scanner*

## C. Email Scanner

In this the E-Mail ID is provided which needs to be tracked. The mails which are received on this mail ID are blacklisted and the mails coming from this mail ID are deleted automatically. The blacklisted Email_ID are saved in a file.

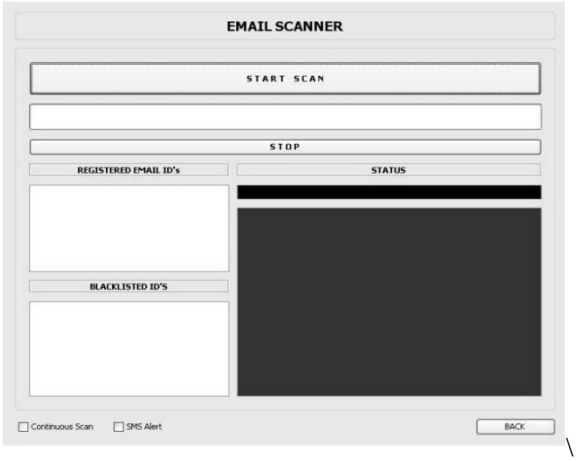


*Fig 4. Email Scanner*

## D. Client Module

This module we have specially done for the LAN part. By this module the computer in LAN cane get the details of the

Blacklisted IP and E-mail ID. The LOG can be sent to them.

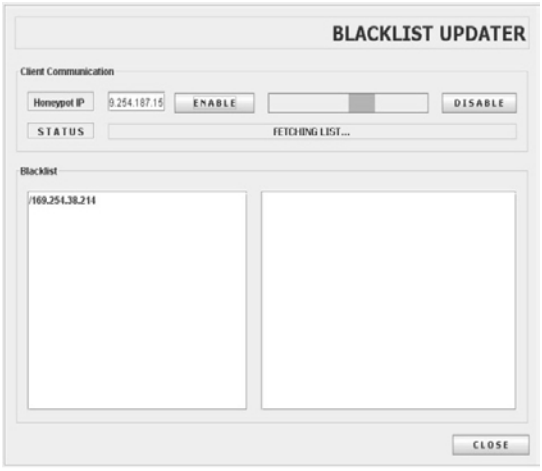


*Fig 4. Client Module for Broadcasting Blacklist*

### V. Mathematical Module

- Honey Pot system can be represented by set representation as:

S= {I, Bdb, F, O}
I1, I2, I3... In ∈ I
Where I is the input to the Honey Pot system.
E.g. I1= e-mail
I2=socket connection
I3= port connection
Bdb is set of Blacklisted IPs
F is the evaluation function
f1=email evaluator
f2= port scanner
f3=socket scanner
O is output function where O= F (I, Bdb)

A. Algorithm for email evaluator

1) Connect to server
2) Start session
3) Specify UserID and password
4) Access folder in R/W mode
5) Access Inbox
6)for all messages m
- Read from ID
- Check if not in white list
- Check if not in Black list then add to Blacklist
Next
7) Logout and close session
8) Stop

For this algorithm time complexity can be O (N), where N is the number of mails. Because there is no parallelism to read e-mails, fixed flow.

## CONCLUSION

The basic idea in this project is to protect a network from. unauthorized use. In order to achieve this we implement HoneyPot. HoneyPots are a cheap and simple way to add protection to a network. They allow the study of attacker's methods of operation. It help in emerging new ways for countering them.In this way the HoneyPot would provide security from the attacker and prevent our pc's getting affected from the attacks

### ACKNOWLEDGMENT

We would like to thank our guide Prof. Rohini V. Agawane, for her guidance and support. We will forever remain grateful for the constant support and guidance extended by guide, for the completion of paper.
Also we thank International Journal of Scientific & Engineering Research (IJSER).

### REFERENCES

[1] Li Li, HuaSun ,Zhenyu Zhang, "The Research and Design of Honeypot System Applied in the LAN Security", School of Information Science and Engineering Xinjiang University Urumqi 830046, China
[2] G. Mohammed Nazer,"Current Intrusion Detection Techniques in Information Technology – A Detailed Analysis",European Journal of Scienti_c Research, EuroJournals Publishing, Inc. 2011
[3] Amit D. Lakhani,Deception Techniques Using Honeypots, Information Security Group Royal Holloway, University of London UK.
[4] Muhammad Fahd, KaleemUllahSaleh,Honeypots A Force Multiplier in Educational Domain, Lule University of Technology
[5] Addison Wesley - Honeypots - Tracking Hackers - 2002

## Author's Profile

- Prof. Rohini V. Agawane Currently working as Assistant Professor with K.J.College of Engineering & Management Research, Pune in the Department of Computer Engineering.

- Jagruti S. Naikare, currently pursuing B.E. in Computer Dept. from K J College of Engineering & Management Research, Pune.
EmailID:jagrutinaikare@gmail.com

- Chaitrali V. Lonkar currently pursuing B.E. in Computer Dept. from K J College of Engineering &

Management Research, Pune.
Email ID: chaitralilonkar@gmail.com

- Aparna A. Sawantcurrently pursuing B.E. in Computer Dept. from K J College of Engineering & Management Research, Pune.
Email ID : aparnaswnt@gmail.com