HONETPOT Based Tool using ANN

Pathare Pratiksha Balu[1] Jadhav Prajakta Ashok[2] Kakulte Manisha Vasant[3] Gawande Darshana Milind[4]

[1,2,3,4]Department of Computer Engineering

[1,2,3,4]Bharati Vidyapeeth College of Engineering for Womens

Abstract— A honeypot is a non-production system, design to interact with cyber-attackers to collect intelligence on attack techniques and behaviors. There has been great amount of work done in the field of network intrusion detection over the past three decades. With networks getting faster and with the increasing dependence on the Internet both at the personal and commercial level, intrusion detection becomes a challenging process. The challenge here is not only to be able to actively monitor large numbers of systems, but also to be able to react quickly to different events. Before deploying a honeypot tool it is advisable to have a clear idea of what the honeypot should and should not do. There should be clear understanding of the operating systems to be used and services (like a web server, ftp server etc) a honeypot will run. The risks involved should be taken into consideration and methods to tackle or reduce these risks should be understood. This honeypot tool is developed by using ANN. This Honeypot tool has greater efficiency. Honeypot tool 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.

Key words: ANN, Artificial Neural Network, HONETPOT

I. INTRODUCTION

An intruder can be defined as somebody attempting to break into an existing computer. This identity is popularly termed as a hacker, blackhat or cracker. The number of computers connected to a network and the Internet is increasing with every day. When combined with the increase in networking speed has made intrusion detection a challenging process. System administrators now days have to deal with larger number of systems connected to the networks that provide a variety of services. The challenge here is not only to be able to actively monitor all the systems but also to be able to react quickly to different events. Traditionally intrusion detection involved a defensive approach where systems were either dedicated computers like firewalls or host based detection systems aimed at detecting attacks or preventing them. These systems existed as a part of the commercial/in-use networks and used techniques like pattern matching or anomaly detection. Another type of security systems are system integrity checkers, which are, typically host based. The problem that these systems face is that they are running on computers, which are in use on a daily basis. These systems usually have to deal with large number of connections and data transfers which results in huge log files and also makes it difficult to differentiate between normal traffic and intrusion attempts accurately. Many of these systems are also known to generate many false positives or in some cases false negatives. Moreover these systems provide very little insight to the tools and methods employed by the blackhat community . Honeypots are an exciting new technology with enormous potential for the security community. The concepts were first introduced by several icons in computer security, specifically Cliff Stoll in the book The Cuckoo's Egg", and Bill Cheswick's paper " An Evening with Berferd." Since then, honeypots have continued to evolve, developing into the powerful security tools they are today.

II. SYSTEM ARCHITECTURE

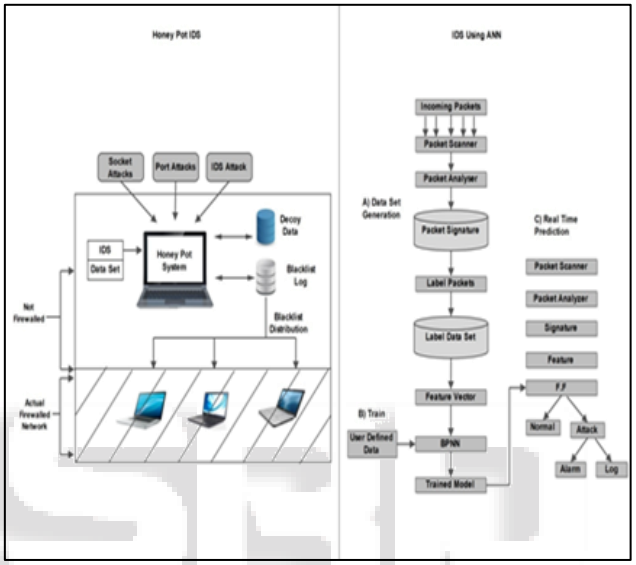

Fig. 1: System Architecture

The system architecture diagram as shown above.It consists of following components:-

- Data Set Generation
- User Defined Data
- Run Time Prediction

A. *Data Set Generation:*

In data set generation, incoming packets are scanned by packet scanner then this packet are analysed by packet analyser after analyzing packets packet signatures are stored into packet signature then labeling the packets and generate label data set after generating label data set extract features.

B. *User Defined Data:*

In user defined data model,feature vector are given to the BPNN(back proposition neural network) algorithm.

C. *Real Time Prediction:*

In real time prediction model,we give the trained model to the FF(Feed Forward) algorithm.By using this algorithm we check whether the packet is malicious or harmful to our system or not.

III. ALGORITHMS

A. *Artificial Neural Network:*

In our system we used Artificial Neural Networks (ANN) provide main features, such as: flexibility, competence, and

capability to simplify and solve problems in pattern classification, function approximation, pattern matching and associative memories.

Different techniques are used in ANNs such as back propagation neural network, feed forward.

1) BPNN Algorithm:

Back-propagation Neural Network (BPNN) algorithm is one of the most widely used and a popular technique to optimize the feed forward neural network training.

2) Feed Forward Neural Network:

A feed forward neural network is an artificial neural network where connections between the units do not form a directed cycle. This is different from recurrent neural networks.The feed forward neural network was the first and simplest type of artificial neural network devised. In this network, the information moves in only one direction, forward, from the input nodes, through the hidden nodes and to the output nodes. There are no cycles or loops in the network.

B. Mathematical Model:

S={A,D,Dc,HPs,P}
Where,
A=set of attacks.-F
which include following attacks:
- Socket attacks
- Port attacks
- IDS attacks.

D=data set.-I
Dc=decoy data.-F
HPs=honeypot system-F
S=all system within network-I
P=incoming packets-I
Ps=scan packets .(network ,scanning packets)
Sg= signature (Ps)
Lp=label packets (Sg)
D=add packets with label (Lp)
F=feature vector (D)
T(Training model)=apply BPNN (F,Ui)
A(IDS attack)[y/n]=feed forward(Ps,T)

IV. ACKNOWLEDGMENT

It gives me great pleasure and satisfaction in presenting this project on “Honeypot Based Secure Network System”.

I would like to express my deep sense of gratitude towards my guide Prof.K.S.Warke who at very discrete step in study of this Project, contributed his valuable guidance and help me to solve every problem that arose.

I would like to give thanks to HOD COMP Prof.D.D.Pukale for his constant guidance. My special thanks to the Project coordinator Prof.S.B.Jadhav and project in charge Prof.S.P.Kadam for their valuable support.

My special thanks to all my friends for their valuable comments and suggestions and for helping me & providing their valuable support.

I would like to thanks all those, who have directly or indirectly helped me for the completion of the work during this seminar.

REFERENCES

[1] Securing wmn using hybrid honeypot system International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012 DOI : 10.5121/ijdps.2012.3304 29
[2] Yogendra Kumar Jain et al. / International Journal on Computer Science and Engineering (IJCSE)
[3] Honey pot based Secure Network System
[4] Jammi Ashok et. al. / International Journal of Engineering Science and Technology Intrusion detection through honeypots Vol. 2(10), 2010, 5689-5696
[5] The research and design of honeypot system applied in the LAN Security 978-1-4244-9698-3/11/2011 IEEE
[6] Honeypot technique used for intrusion detection system International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 12, December 2013
[7] Honey pots design & implementation of honeyd to simulate virtual honeypots IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 1 (July-Aug. 2012), PP 28-34
[8] Honeypot: a Supplemented Active Defense System for Network Security 0-7803-7840-7/03/2003 IEEE.
[9] Web based honeypots network International Journal of Scientific and Research Publications, Volume 3, Issue 8, August 2013 1 ISSN 2250-3153

