Available online at http://acfa.apeejay.edu

APEEJAY JOURNAL OF COMPUTER SCIENCE AND APPLICATIONS

ISSN:0974-5742(P)
Vol. 2, January 2014

Honeypot Security protocol in Multicast networking expending modern tools with optimal solutions

Dinesh Kumar[1], Dr. Parvinder Singh[2]
[1]Research Scholar, Punjab Technical University, Jalandhar, Punjab, India.
[2]Director-Principal, Rayat-Bahra Institute of Engineering & Bio-Tech., Kharar, Mohali, Punjab
E-mail: [1]dk_scorpio@rediffmail.com, [2]parvinder.sandhu@gmail.com

Abstract

We know that a Honeypot is an information system resource used to divert attackers and hackers away from critical resources as well as a tool to study an attacker's methods and we mainly focus on the vulnerability of the network to a suction attack called blackhole attack. With the development of the network technology, the risk and attack technique has also been increased; also the increase of the security risk on the internet. The basic purpose of Honeypot technology and the tools used and required to prevent a network system in detecting various attacks, we explore the use of intelligent agents in the form of honeypots which are roaming virtual software agents that generate a dummy route request (RREQ) packets to attract and catch blackhole attackers. In our research paper, the tool used is honeyd and compared with other tools as described for creating honeypots in single and M-cast networks. Also, the logs generated by extensive honeyd can be maintained and which will grow very large in size when there is heavy attack traffic in the system, thus consuming a lot of disk space. So, the proper utilization and maintenance of disk has been achieved by using some new approaches like the development of a genetic algorithm the optimization methods are to be used for the control of network system.

Keywords: RERQ (Route request), E- Honeyd (Expanded-Honeyd),M-Cast(Multicast)

1. INTRODUCTION

The existing network system may be classified as private or public network and further may be of any topology such as Multicast or Unicast network system. The user of the any public network system, often called node carrierand there is very limited access to outside world in a private network which is used and managed by an organization for its own purposes. In M-cast network system the Spammers continually scan the Internet for open proxy relays: by using these open relays, they can obscure their originating IP address and remain anonymous. However, from the user’s point of view, each computer appears to attach to a single large multicast network represented as a cloud and related terms used among various computer researchers and scientists. The requirement of such technology have to be developed which can proactively detect and respond to the intrusion and the attack of the network and we have expanded the basic characteristics and applications of Honeyd and given the name E-Honeyd (or Expanded-Honeyd).These approaches can be classified in different ways as per their types of existing technique used as described below:

Types of Honeypot system

The honey pot system can be classified on the basis of existing M-cast network system which may be a Public network system or a private network system. But there are two levels of interaction available in the existing network system. These can be classified as:

a. Low Interaction Honeypots: In this category, there is very less interact ion of honeypot system with the attackers as no operating system will support the existing network system.

b. High Interaction Honeypots: In this category, the interaction between the attackers and the system is very high. As, it also keep track of all attackers and makes certain records for the research purpose.

Features

The various features of the Honeypots must ensure the system security because there is a big threat to the public or private network system. The most common features are:

a. The monitoring and record keeping of large number of attackers will be performed by the existing system.

b. The true identity and valuable information about the spammer is collected and keeps a log whenever the spammer comes across a service on a honeypot and help unmask it.

c. It will prevent our network system by using such tools like Honeyd which is the part of Honeypot technology and it is easy to manage and will work in a sequence order.

2. COMPARISON AND RELATED WORK

As per the security is concern maximum work was performed by Singh, et el. [1] in which the huge log size poses difficulty when they are processed and analysed by security analysts as they consume a lot of time and resources. The Security mechanism of the network system was very well described by J. Bao, et. el[2], where the characteristics and effectively limit the spread of the aggressive behaviour on the network was analysed. The author L. Spitzner[3] shows what type of specific threats do computer networks face from hackers and who's perpetrating these threats and how? The defence mechanism was practically described by MuhlbachS.et.el in year 2010 [6].

In reviewing the literature, it became apparent that the research can be broken down into five major areas by Mathew L. Bringeret.el [4] in year 2012:

a. Establishing and stabilising honeypot detections by attackers,

b. To improve the accuracy in threat detections and the proper utilization of honeypot output data

c. To cope with emergent new security threats new types of honeypots must be used in the existing multicast network system.

On the basis of previous research work and considered by various authors to implement the Honeypot tools such as was very well designed by N. Krawetz [6]. But, the above mentioned points will focus on a new kind of theory and comparison factors. So, the various objectives time to time has been defined to make the network system secure.

3. PROPOSED WORK

Our work will provide a better security as compared with the previous security tools. In first step, we have proposed to design a Honeypot tool i.e., “Extensive Honeyd” which is used to make the network system better and more secure. In the next step, the exploration of the intelligent agents in the form of new Honeypot tools is to be compared with other security tools to maintain the minimum use of disk space and to keep track of intruders or hackers.

The logs have to be kept as a record to check the single or multiple attackers in the system and to provide a genetic approach to remove these types of attackers. The proposal will minimizes the main issues in the previous research approaches. The Pareto dominance approach is to be added as a better solution and better approach.

a. Our security tool extensive Honeyd is proposed to monitor and to keep records of large number of attackers.

b. The extensive Honeyd gives our server the true identity and the valuable information. The other tools like wireshark are also to be used as a support to monitor the various users and identifies the spammers among them and The other method for the optimization control of the network system is used by using some mathematical techniques.

c. Extensive Honeyd tool is very easy to manage and collect the information. It will prevent our network system by using such tools, which is the part of Honeypot technology.

The other optimizing technique in the network system where the single node is supposed to be travelling with its better performance factors. As, these factors considers the various shortest paths and utilizing maximum efficiency which includes cost function. The optimal solution can be taken by using Pontryagin’s Principle whether maximum or minimum principle or simply known as Pontryagin's Principle.Another optimum control problem is to find the way to check the travelling node so as to minimize its energy consumption, given that it must complete a given course in a time not exceeding some amount. A more abstract framework goes as follows. Minimize the continuous-time cost functional

$$J = \Phi\,[\,\mathbf{x}(t_0), t_0, \mathbf{x}(t_f), t_f\,] + \int_{t_0}^{t_f} \mathcal{L}\,[\,\mathbf{x}(t), \mathbf{u}(t), t\,]\;\mathrm{d}\,t$$ subject to the Ist-order dynamic constraints (1)

x(t)=a[x(t),u(t),t],

(2)

the other algebraic *path constraints*

b[x(t), u(t),t]<=0 (3)

and the boundary conditions

$$\boldsymbol{\phi}\,[\,\mathbf{x}(t_0), t_0, \mathbf{x}(t_f), t_f\,] = 0$$ (4)

Where,

x(t) = *state,*
u(t) = *control,*
t = independent variable (generally speaking, time),
t_0 = Initial time, and
t_f =Terminal time.

The terms Φ and $\mathcal{L}$ are called the ***endpoint cost*** and ***Lagrargian*** respectively.
Furthermore, it is noted that the path constraints are in general *inequality* constraints and thus may not be active (i.e., equal to zero) at the optimal solution. It is also stated that the optimal control problem as stated above may not have single or unique solution, It may have multiple solutions for a single problem.

4. CONCLUSION AND FUTURE WORK

We have proposed Extensive Honeyd tool to identify the intruders and to control and manage the various kinds of network systems especially the multicast network system where the probability of intruders is at very risk.In this work, we have described some of the previous efforts to check the performances of various Honeypot security tools. So, we have found some of the problems and difficulties in their performances. As, it was believed that a episodic, complete evaluation of Honeypot tools could be appreciated for network and data managers. However, various kinds of attacks in a network traffic are so variable from site to site, and because normal and attack traffic evolve over time Solving the problem of high availability and security simultaneously offers the opportunity for more reliability than systems which solve the problems separately, in addition to being easier to implement, and offering increased opportunity for recording and da ta analysis. In future, as per the authors' opinion that this type of system could provide a much more security tool, however, a good transaction of streamlining work could be done in the future.

REFERENCES

[1] Singh. A.N,Joshi R.X,Signal Processing , communication, computing and Networking technologies (ICSCCN-2011) Internenational conference on 21-22 July 2011,pages 514 - 519, ISBN 978-1-61284-654-5 (IEEE)

[2] J. Bao, C. Ji and M. Gao,"Research on network security of defense based on Honeypot", In International Conference on Computer Applications and System Modelling, 2010.

[3] L. Spitzner, "The Honeynet Project: Trapping the Hackers," IEEE Security & Privacy vol. 1, no. 2, pp. 15-23, 2003.

[4] Mathew L. Bringer, Christopher A. Chelmeki, and Hiroshi Fujoniki, “A Survey: Recent Advances and future trends in Honeypot Rsearch, I.J. Computer Network and Information Security, 2012,10,63-75 (Published online September 2012 in MECS).www.mecs-press.org.

[5] N. Krawetz, "Anti-honeypot technology," IEEE Security Privacy, Vol. 2, no. 1, pp. 76-79, 2004

[6] Muhlbach S., Koch A., A dynamically reconfigured network platform for High speed Malware collection,"Reconfigurable Computing and FPGAs (ReConFig-2010) International Conference on 10.11.2009, published in 2010.

[7] MengVui, et.el,Information Technology, International Conference on Computer engineering and Management Sciences (ICM-2011), Page 100-103