International Journal of Scientific & Engineering Research, Volume 8, Issue 3, March-2017
339
ISSN 2229-5518

Security Enhancement for Military Intelligence Network using Honeypot

Binu Kuriakose Vargis

Abstract— Honeypot systems are those tools or a server which by definition captures all the intrusions directed towards a particular network in which it is placed. By integrating a honeypot based product with a system it can be converted into a high or low interaction honeypot system based on the product used. A simulation work demonstrating the use of honeypot for enabling a more secured network for military intelligence network is done in the research work. We observed that 49% of 4447 intrusions were from a unique IP. 18% and 12% of intrusions are from another IP. Military intelligence network both in India as well as in world are being attacked on a regular basis. Every threatful event against such organization's try to get the valuable information's from their network. For that regular intrusions are the starting process. This paper states steps to find out such events and finding out the suspected locations prior to attack.

Index Terms—Blackhats, Honeypots, SPIM, HICHP, Honeyspot, Blacklist, Scanport.

1 INTRODUCTION

In the recent trends of Network Security Honeypots are migrating from the roles of a research oriented concept and a tool to a more diversified methodology of detecting flaws in the Network Security. It can be used for detection purposes in various organisations to notify the changes in the main databases of the organisation. More intentionally it can be a major breakthrough in identifying the major threats to the organisation on the basis of IP addresses. IP addresses can although change but the ISP/ Location will be the same for all the IP addresses under the same ISP's. Our research work encourages, how the functionality of Honeypots can be useful for Military Based Intelligence Networks. The papers describes a very dynamic and strainghtforward tachnique which makes use of the detections made by the Honeypot and use these detection details for findong out any serious movements against those organisations especially it can be much useful against finding the locations related to terrorist activities/movements by the IP addresses. A dummy database should be made available in the network of the organisation and the honeypot system connected to it. Once the attacker intrudes the dummy database it will be deteted by the Honeypot at any case.

Honeypot system is a network based detectiong tool which adds to the network security. More precisely honeypots gives a upperhand in detecting tool as well as in analysing them. Adding to the features it can also capture the malicious content i.e. harmful executive files and can save even them in the system without any threat to the user. By definition honeypot is a resource tool to analyse the intrusions and study the activities of the intruder in a very simple and efficient manner [17]. A very simple but yet a very approved concept in security which now became a very eye-cathing concept for many top rated organisations such as microsoft.

The rest of this paper is organized as follows. In section II related works are outlined. Section III gives a description of the proposed methodolgy for developing a application using honeypot for millitary intelligence network. In section IV the implementation and analysis part is described followed by results and will conclude in section V.

2 RELATED WORK

In literature there are many scenarios and applications where honeypots had proved to be very useful. Some of those are described below:

A Banking security model was developed which identifies any changes in their databases. Database was designed into three different layers such that no harmful event can affect their network. Honeypot was used as IDS to protect their network [3]. Honeypots can be used to detect the attack patterns in Cloud computing as well and to block the attacker production honeypots are useful [9]. Detecting a malicious web page is possible by using High Interaction Honeypots (HICHP's). They use dynamic analysis and so they are effective at detecting unknown attacks and obfuscated patterns [8].

Honeyd based Honeypot as an alerting system to provide notification via email against worm and network traffic [8]. A spim honeypot was developed to counter SPIM (Instant Messaging Spam) and analyzed that SPIM is being sent using

widely distributed botnets. On the basis of experimental results this paper identifies that 1465 IP's sent SPIM which were unverified and they contributed 70.39%. Suspicious SPIM were sent from 276 IP's contributing to 13.26% and spam mails were sent from 340 IP's contributing to 16.34% [20]. Computer Forensics used honeypot technology and a host firewall tool was used to monitor all the incoming and outgoing connections from the honeypot [7].

To gather information on the attacks done on the wireless networks a wireless honeypot named Honeyspot. It can't be attacked globally but only by the nearby malicious users [13].

3 PROPOSED METHOD

SCANPORT: In this module, all the open ports are scanned for checking which ones are free and which ones are attacked and being used by the attacker. Functionality corresponding to port number will itself reveal much information regarding the attack. All the ports which are being used for communication in the network both the incoming and outgoing will be displayed. An algorithm has been proposed for the same:

Step 1: Open user interface for the scanport.
Step 2: Enter server ip address
Step 3: Enter port numbers to be scanned.
Step 4: Display the port numbers if not free.

ATTACK ANALYZER: In this module as soon as the attacker gains access to the system and starts attacking, it will be detected by the Honeypot and will start creating log files for the same. If in the network any harmful intrusions such as Trojans/Rootkit is also found then that will also be saved in the log file in the Captured files. Apart from these attacks we can check for system communications in details for which ports are engaged in communications in network of our system. The log files can be analysed from this module.

Step 1: Select a log file.
Step 2: Display the intruder's ip address.
Step 3: Display the port numbers of our system which are being communicated.
Step 4: Analyze both the log files and the port numbers in detail.

FIND BLACKLISTED IP: This module will check for the highly busy location from where the attack is occuring the maximum number of times. Once the IP address is retrieved it will be checked in the blacklisted logs. Now, it will check the frequency of the IP address attempting to open some document i.e. how many times does an attack followed from the same IP address. If the frequency of attacks exceeds the limit set by the administrator from military network then add it to the blacklisted IP. Such an IP add and its location will of much interest to the intelligence. Proposed algorithm:

Step 1: Enter the list of Foreign IP Address.
Step 2: Monitor the number of attempts made from that IP.
Step 3: If the number of attempts exceeds the limit set: Add it to BLACKLIST and look for time and location.
else if the number of attempts is less than the limit.
Goto step 2;Exit

Step 4: Disconnect Honeypot with the system.

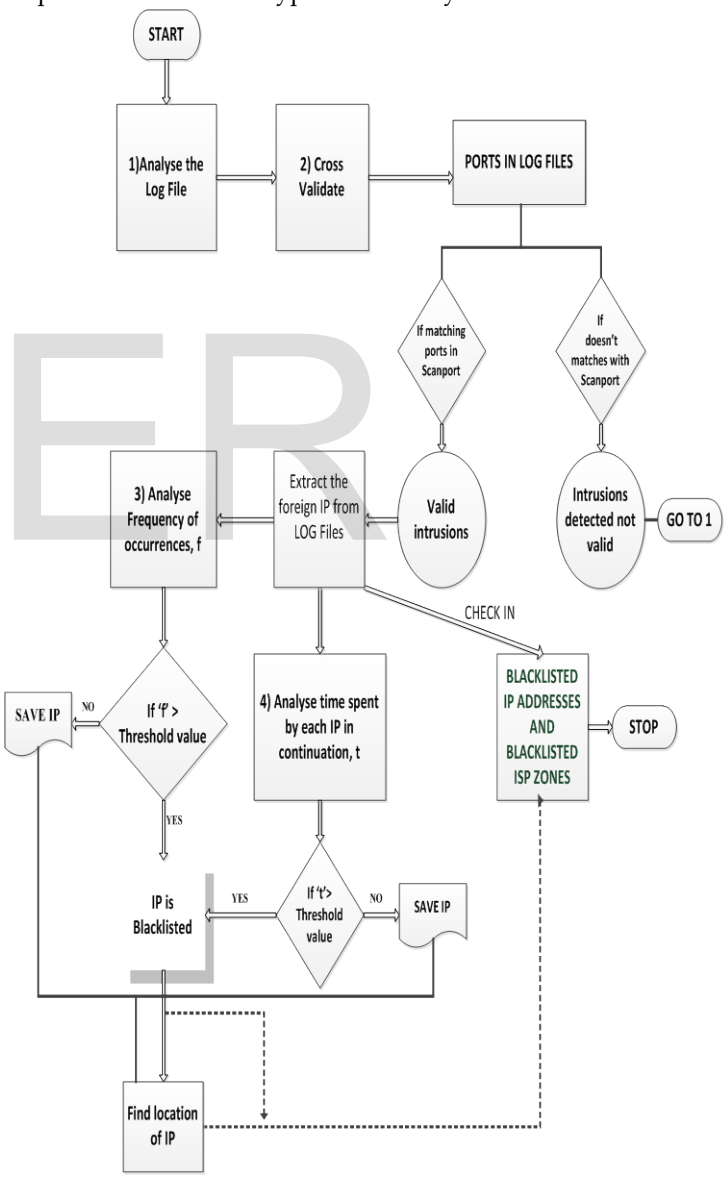

Fig 1: Representing Framework of the Implementation

4 IMPLEMENTATION & ANALYSIS

Network security is getting better day by day with addition of many new security measures to the existing ones. We have implemented our proposed methodology using HoneyBot a honeypot based product.

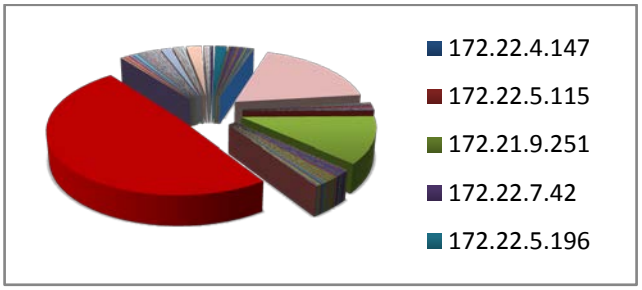

Fig 2: Representing total intrusions by different IP are detected by the Honeypot.

HoneyBot is a low interaction honeypot and the most significant part is that it is available free of cost and it has no problem in deployment as it supports windows platform.

The observation collected from the honeypot of 4447 intrusions is shown in figure 2. From detection point of view it can detect Trojans/Rootkits and stores all those in a capture file apart from log files. In capture files Trojans/Rootkits are stored not in the ".exe" form but in some other form so that its chances of getting executed in the compromised system is lowered. We have used Java for the modules in our proposed methodology. The following algorithm will show how our system will work for filtering out harmful intrusions detected by the honeypot

1. Extract the intrusions using HoneyBot Log Files

Analyse the intrusions detected in the Log Files and extract them into .csv file format.

2. Analyse the local and remote ports used for communication

CrossValidate ()
{
If (ports in Log files == ports identified from Scanport)
Then
Intrusions detected by honeypot are valid;
Else
Intrusions not valid;
}

3. Extract the Foreign address from Log File, Create a list of Suspected Harmful Foreign addresses and create the Blacklisted IP addresses:

Set a threshold: Frequency limit (F.t);
If (occurrence of IP is >= threshold: Frequency)
{
IP is blacklisted;
Save IP and its count in a file; //for step 5//
}
Else
Store IP and its count in a file;

Set a Threshold Time Limit (T.t);
if (time spent on attack is>=threshold: Time)
{
IP is blacklisted;
Save IP and the time; // for step 5//
}
Else
exit;
GoTo Step 5;

4. Analyse the foreign/intruders address using the knowledgebase from previously analysed results from honeypot. Analyse:
if (Foreign Add matches the previously detected Blacklisted IP's)
then *Foreign Add = 'Blacklisted Intrusion';*
Else
exit;

5. Find out the geographical locations of the blacklisted ip addresses per 4000-5000 intrusions.

For (ip=0; ip<n; ip++)
{
If (ISP of a blacklisted ip == ISP of another blacklisted ip)
{
If (j>=m) //'j' refers to count of blacklisted IP
Location == Threatful;
Else
Location == suspected ;}
}
Else
Exit;

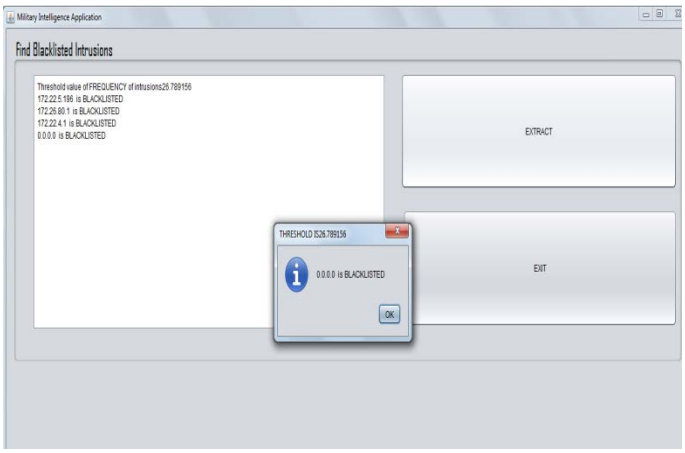

Fig 3: Showing Working Of Blacklisted IP Module

We have all the intrusions detected by the honeypot for a few months. All the details created from the log files in the system were then analysed. A code for the same was developed to detect the frequency of occurrence of each of the IP a day. Below is the threatful intrusions detected during the analysis on a particular day having a total of 4447 intrusions number.

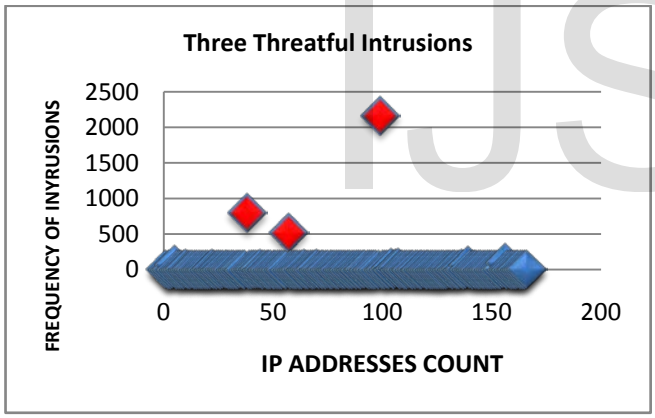

Fig 5: Representing the three threatful intrusions.

5 Conclusions & Limitations

This paper highlights the concept of honeypot. It then based on the detection done by the honeypot creates log files. These log files are then analysed based on the Remote IP address, port number on which the attack has been done and the time of attack. Our calculations were based on two parameters namely frequency of intrusion and the time taken by some specific IP in continuation. Based on the calculations on a sample of 4447 intrusions detected by the honeypot, two IP addresses were foundto be suspective on the basis of frequency and time spent on attack.

That IP address was added into blacklisted category and it was backtracked to find its geographical location. 49% out of 4447 attacks were registered by a single ip. Next to this were 18% and 12% by two other IP's respectively. Those three IP's are our threatful intrusions. Now continual intrusions from this location or from the ISP could eventually be the target for military intelligence network. Therefore, analysis of a big log file will be much easier by using the developed code to find the number of occurrences of each and every IP intrusions.

The limitation of this work is we have used a low interaction honeypot for detecting the intrusions, since deploying such a honeypot system is more convenient. So the amount of intrusions and the details of intrusions can also be upgraded by using a high interaction honeypot instead. Using high interaction honeypot will yield much more qualitative data and hence a more analytical information to understand the threatful activity to a military organization.

References

[1] Nicolette Vincent, Kaâniche Mohamed, Alata Eric and Herrb Matthieu, "Set-up and deployment of a high-interaction honeypot: experiment and lessons learned", published in Springer-Verlag France 2010, 27 June 2010.

[2] Aliyev Vusal, "Using Honeypots To Study Skill Level Of Attackers Based On The Exploited Vulnerabilities In The Network," as a Master Of Science Thesis In The Master Degree Programme, Secure And Dependable Computer Systems, Department Of Computer science and Engineering, Division of Computer Security, at Chalmers University Of Technology, Sweden in 2010.

[3] Chaware Sandeep, "Banking Security using Honeypot", in International Journal of Security and Its Applications, Vol. 5 No. 1, in January, 2011.

[4] Hunt Ray and Zeadally Sherali, "Network Forensics – An Analysis of Techniques, Tools, and Trends", in IEEE Network, 2012.

[5] Singh Kumar Ram and Prof. Ramanujam.T, "Intrusion Detection System Using Advanced Honeypot's", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 2, No. 1, in 2009.

[6] Rajnish Sharma, "Design and Development of a Linux Based Honeypot", a thesis work for Masters Degree in Software Engineering, Thappar Institute Of Technology, in May 2005.

[7] Zi Li Chen, Xiao Jia Li , and Lei Gong, "Computer Forensics System Based On Honeypot", in Proceedings of the Third International Symposium on Computer Science and Computational Technology(ISCSCT '10), pp.336-337, 14-15, August 2010.

[8] Hong-Geun Kim, Dongjin Kim, Seong-Je Cho, Moonju Park And Minkyu Park, "Efficient Detection of Malicious Web Pages Using High-Interaction Client Honeypots", Journal Of Information Science And Engineering 28, 911-924 (2012).

[9] Chandra Nithin S.R and Madhuri T.M, "Cloud Security using Honeypot Systems", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March 2012 .

[10] Jain Kumar Yogendra and Singh Surabhi, "Honeypot based Secure Network System" , International Journal on Computer Science and Engineering (IJCSE), Vol. 3 No. 2 Feb 2011, in 2010.

[11] W.Martin William, SANS Institute InfoSec Reading Room(2003), "Honey Pots and Honey Nets - Security through Deception", in May 2001.

[12] The Use of Honeynets to Increase Computer Network Security and User Awareness http://www.juliangrizzard.com/pubs/ 2005_krasser_jse.pdf.

[13] Siles raul, "HoneySpot: The Wireless Honeypot Monitoring the Attacker's Activities in Wireless Networks", The Spanish Honeypot Project, in Dec 17, 2007.

[14] Eric peter, Todd Schiller and Raj Jain, " A practical guide to Honeypots",2008.

[15] Chang-Lung Tsai, Chun-Chi Tseng and Chin-Chuan Han, " Intrusive Behavior Analysis Based on Honey Pot" publishes in IEEE society, in 2009. Krasser, Grizzard, Owen, Levine.

[16] Lance Spitzner. "Honeyd," Honeypots—Tracking Hackers, Addison Wesley, 2002, pp. 141-166

[17] The Honeynets Project, "Know Your Enemy: Sebek," http://honeynet.org/papers/sebek.pdf.

[18] N, Provos, " A virtual honeypot framework" , Proceedings of the 13th USENIX Symposium. 2004. pp.1-14

[19] Schryen, G. An e-mail honeypot addressing spammers' behavior in collecting and applying addresses. Proceedings from the Sixth Annual IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop, June 2005. pp. 37-41

[20] Aarjav J. Trivedi, Paul Q. Judge, Sven Krasser, "Analyzing Network and Content Characteristics of Spim using Honeypots".

[21] Vargis, B.K. &Tak,G.K.,(2013, March). A survey on various implementing scenarios of Honeypot. In the proceedings for International Conference on Computing, Communication and Advanced Network, ICCCAN, technically sponsored by IEEE. (pp. 6-10), 2013.