Communication of nodes in Hybrid honey pot system for the Network Security

Prof Sulakshana B Mane
(Computer Engineering Department),
BVCOE, kharghar , Navi Mumbai
sulumane@gmail.com

Prof. Khiarnar V .D
H.O.D (Information technology Department)
TEC, Nerul, Navi Mumbai
khairnar.vaishali3@gmail.com

***Abstract*— in this Paper, I present how nodes are communicated with each other in hybrid honey pot system for the network security. Hybrid honeypot system is a combination of low and high interaction system. Whatever drawbacks of low interaction and high interaction that is removed by hybrid honeypot system. In the hybrid honey pot system, first nodes are communicated with each other and how all nodes are communicated with server and then which nodes ports ip address are open that is port scan identified by the hybrid honey pot system.**

Keywords— VMware, Low-interaction honey pot, High-interaction honey pot, Proxy etc

1. Introduction

. Sometimes threatening is done by the open pots also. The purposes of honey pot are to detected and learn from attacks and use that information provides network security. Honey pots are analyzed by their role of application, which is meant it can be used for production and research.

2. Definition of honey pot

"A honey pot is security resource whose value lies in being probed, attacked, or compromised".

The main functions of a honey pot are

1. To divert the attention of the attacker from the real network, in a way that the main information resources are not compromised.
2. To capture new viruses or worms for future study
3. To build attacker profiles in order to identify their preferred attack methods, similar to criminal profiles used by law enforcement agencies in order to identify a criminal's modus Operandi.

3. Level of interaction

The level of interaction is defined as the range of attack Possibilities that a honey pot allow an attacker to have, where as it can be classified as high- interaction honey pot and low interaction honeypot there are two types of honey pots

1. Low interaction honey pot
2. High interaction honey pot

3.1 High- Interaction Honey pot

In high- interaction honey pot, attacker interaction with real operating systems, services and programs and it can be used to observe the attackers behavior, their tools, and motivation and Explored vulnerabilities. This kind of honey pot must have a robust containment mechanism in order to prevent, once compromised, its use to attack other networks. One goal of a hacker is to gain root and to have access to a machine, which Tools like Sebek can help high-interaction honey pot to instrument to log and/or System calls.

3.2. Low- Interaction Honey pot

In low- interaction honey pot, there is no operating system is involved that an attacker can operate on. Tools are installed in order to emulate operating systems and services. And they interact with the attackers and malicious code. This will minimize the risk significantly.

© 2013 IJAIR. ALL RIGHTS RESERVED

This kind of honey pot has a small chance of being compromised. It is production honey pot. Typical use of low-interaction honey pot includes port scans identification, generation of attack signatures, trend analysis and malware collection. On the other hand, this is also a disadvantage it is not possible to watch an attacker interacting with the operating system, which could be really interacting. Example of low interaction honey pot is honeyed. Honeyed is an open source low-interactivity honey pot system that creates virtual hosts that can be configured to run arbitrary services and their personality can be adapted so that they appear to be running certain operating systems. Honeyed, enables a single host to claim multiple addresses. Honeyed improves cyber security by providing mechanism for threat detection and assessment. It also deters adversaries by hiding systems in the middle of virtual systems.

3.3. Comparison between low- interaction honey pot and high interaction honey pot

Each level has advantages and disadvantage as mention Below;

	Low interaction honey pot	High interaction honey pot
Degree of involvement	Low	high
Real Operating System	No	Yes
Risk	Low	high
Information gathering	Connections	all
Compromised Wished	No	yes
Knowledge to run	Low	high
Knowledge to develop	Low	Mid high

Table 1 comparison between low interaction and high interaction

3.4 **Hybrid honey pot system**

Low-interaction honey pot is more secure than high- interaction honey pot because of running real service; it lacks the ability to provide a good level of realism. However, high-interaction honey pot provides the best possible level of realism but it has more risk.

. In this system, low- interaction honey pot act as lightweight proxy. We want high-interaction honey pot to process all traffic destined to black IP address space. We need to offload them as front end to high-interaction honey pot because it is instrumented machines. Honeyed has the appropriate properties to play the role of the front end and acts as a filtering component. The lightweight proxy responds only to TCP/SYN requests to ports that are open. For any other ports, it just absorbs and records the packets received. When the three-way handshake has completed properly between the attacker and

the low- interaction honey pot, the connection must be handoff to the appropriate high-interaction honey pot . At this point, also referred as zero point, the low-interaction honey pot set as

a connection with the high- interaction honey pot. The low interaction honey pot sets as like relay agent. Any application level data coming from attacker is forwarded to the high interaction honey pot and vice versa, until the connection is terminated. This behavior is embedded to the honeyed implementation, know as proxy mode. The proxy mode is instrumented to record the message exchanges, for further analysis purposes. Hand-off is useful in case of port scanning, where low-interaction honey pot will absorb all incoming connections without disturbing high-interaction honey pot.

3.5 How it works?

In the following illustration, initially, the attacker sends a TCP/ SYN packet to the low-interaction honey pot. If the honey pot is configured to listen to the port, then it sends a SYN/ACK packet and waits to receive the next

© 2013 IJAIR. ALL RIGHTS RESERVED

packet. If the packet is not an ACK then the low-interaction honey pot assumes that it was a port scan and the connection is dropped. If the third packet received is ACK then it is a valid TCP connection and the zero point is reached. Thus the low interaction honey pot connects with the high-interaction honey pot running the requested service. Then after the connection establishment the low-interaction honey pot continues to work as a proxy. As low and high-interaction honey pots belong to the same local network, no additional delay will be perceived by the attacker.

3.6 actual mechanism of communication of nodes in hybrid honey pot system

For the implementation of hybrid honey pot system there are two phases this one phase in which first all the nodes are communicated to each other .In the second phase, whose nodes poets are open form where attack will be happen that will be shown by the yellow packet transferring and honey pot it will detect the port open address it is shown by the yellow colour of packet is transferred.

Here i am first phase is implemented.

Here 10 nodes are considered then out of 10 one node is considered as a server. This will be shown as yellow colour as a server. Here there is wired communication is happen. Routing method is considered as a hybrid honey pot system here there are three levels are considered one as high two as low and three as a hybrid. Interval time is considered a as ten set i is as a 0 then i increments by one till 10 and nodes are displayed. 0^{th} node is considered as server. When server is considered with colour red.

Considered for the communication of two nodes i and j value is considered creating duplex link between i and j by 1.5Mb time is 10ms and drop tail then server is set then level of interaction are set as one condition is if interaction level is one then it is high interaction then it starts the simulation when source as a udp node as a source attached with udp source.

Source cbr is created that cbr source is connected with the udp source have a packet size 512 interval time is considered then then udp connected with the null agent then. source tcp is created source tcp have a packet size is of 200,tcp link is created .udp is created with 200 packet size, in this way this we can create the udp and link is done through ping .

When it is tested, ten numbers of nodes are connected to each other and they are communicated to each other which will transfer the packet to according to it

There are 10 nodes path are considered for the 10 routing paths.

Here there are 10 nodes, wired channel, interval time is 10 .Red coloured node acts as server .value of server is set as 0. for the creation of link between the two nodes two variable are considered i and j .first i is 0 it will increments the value till 6 and j it checks the value exp i+5 increments j then link is created between nodes with 1.5 Mb and time is 10 ms

Node 0 to node1
Node 0 to node2
Node 0 to node3
Node 0 to node4
Node 0 to node5
Node 1 to node2
Node 1 to node3
Node 1 to node4
Node 1 to node5
Node 1 to node6
Node 2 to node3
Node 2 to node4
Node 2 to node5
Node 2 to node6
Node 3 to node4
Node 3 to node5
Node 3 to node6
Node 4 to node5
Node 4 to node6
Node 5 to node6

© 2013 IJAIR. ALL RIGHTS RESERVED

Here i and j two variables are considered set value of i i checked till val (nn)-4 increments i set j j is i +5 increments j creating link between i and j link is duplex 1.5 Mb and 10 ms i.e. bandwidth and delay

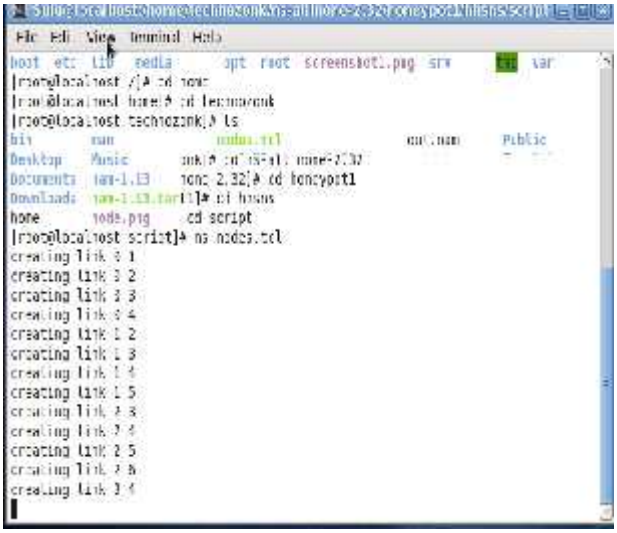

Fig 1. Communication between10 nodes

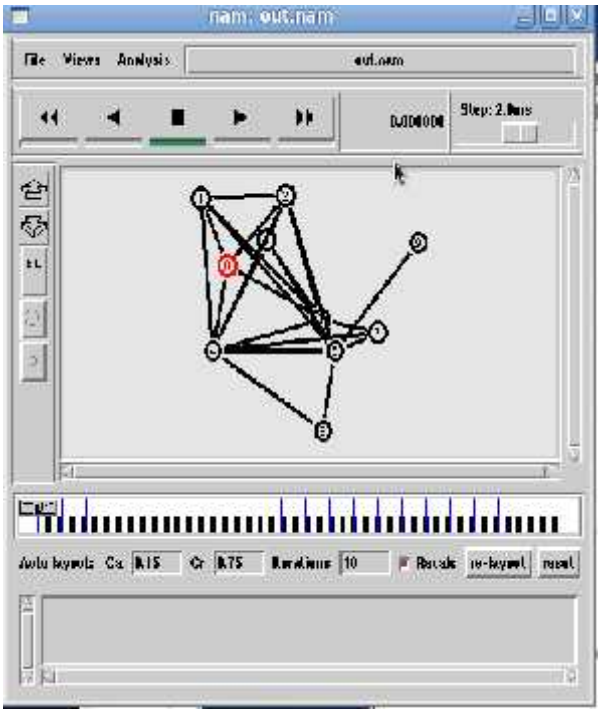

Fig 1 output file of Communication between10 nodes.

After some simulation times it is 0 as a red coloured as server.

In this trace file has 8 receive files indicated by r and 9 are at enqueue files 8 are dequeue files.

11.040853 1 2 tcp 240 0 1.1 6 1 3

11.40853 is the simulation time 1 is is from that node being traced till 2 node tcp is the type of packet,240 is size of packet 0 flag 1 is node and port is 1 6 is source address 1 destinations addrss1 is sequence number 3 is packet id

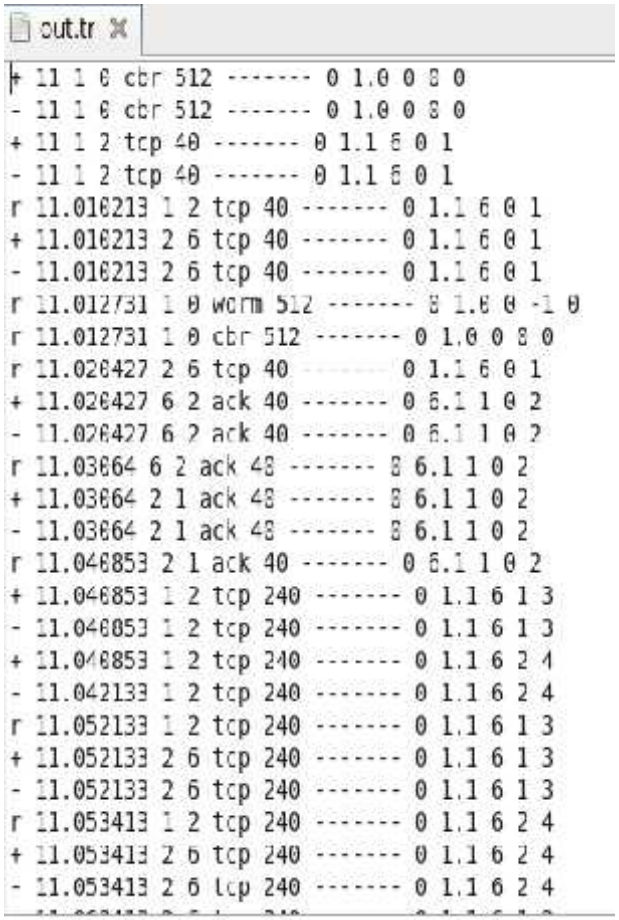

Fig 3. Trace files of communication of 10 nodes

Conclusion:

Using hybrid honey pot, I will achieve a number of goals. All port- scan attempts or connection to port that is not open will be stopped by honey pots server. In this paper all the nodes are connected to each other and send the packet between them and detect it .

© 2013 IJAIR. ALL RIGHTS RESERVED

References:

[1]
"Hybrid Honey pot System for Network Security"
By Kyi Lin Lin Kyaw, Department of Engineering Physics, Mandalay Technological University, Pathein Gyi, Mandalay.vol World Academy of Science, Engineering and Technology 48 2008

[2] Improving network security with Honey pots.

[3] **"**Taxonomy of Hybrid Honey pots"
Hamid Mohammadzadeh.e.n 1, Masood Mansoori 2 and Roza Honarbakhsh 3
1 Faculty of computer Science & Technology, University of Malaya, Kuala Lumpur
2 Faculty of Computer Science and Software Engineering, University of Canterbury, New Zealand
IPCSIT vol.11 (2011)

[4] "A Technique for Detecting New Attacks in Low-Interaction Honey pot Traffic"
S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann
Information Security Institute, Queensland University of Technology
Brisbane, Queensland, Australia
{s.almotairi, a.clark, g.mohay, j.zimmerm}@isi.qut.edu.au
2009 Fourth International Conference on Internet Monitoring and Protection

Bibliography

Author1
Name: Mrs Sulakshana B Mane
Designation: Assistant Professor
BVCOE, kharghar, Navi Mumbai
Teaching Exp: 8 years
No of Published Papers 05

Author 2
Name: Prof Vaishali D Khairnar
Designation: H.O.D (Information Technology) TEC, Nerul, Navi Mumbai
Teaching Exp: 12 years
No of Published Papers 12

© 2013 IJAIR. ALL RIGHTS RESERVED