AN EFFICIENT SECURED SYSTEM FOR IDENTIFYING MALICIOUS NETWORK ACTIVITY USING SCALABLE HONEYPOT.

Rahul Patil, Ajinkya Virkud, Ajay Sagar, Swapnil Miniyar

Rahul Patil, Student, Computer Engg, SKNSITS, Maharashtra, India

Ajinkya Virkud, Student, Computer Engg, SKNSITS, Maharashtra, India

Ajay Sagar, Student, Computer Engg, SKNSITS, Maharashtra, India

Swapnil Miniyar, Student, Computer Engg, SKNSITS, Maharashtra, India

ABSTRACT

Now a day's in this world there are many malicious activities performed on internet or network. To prevent these IDS is used but in some cases it fails to capture intrusion. So we are using honeypot to prevent the malicious activity after IDS. Honeypot is system which is used capture the intrusion activity on network. Many organizations exert the honeypot to know the bound of attack on their network. In this paper, we are going to deploy several honeypot to grab the malicious activity. It can be easily exerted in many organizations without specialized hardware an d cost effective.

Keyword :- *Network Attack, IDS Evaluation, Honeypot Evaluation, Attack Handling, IDS Rules, Honeypot rules,*

1. INTRODUCTION

Now days, people are facing some malicious activities performed on networkand internet. So we are using Honeypot to captured malicious activity on network.Honeypot is a computer system which is used to capture a malicious activity. There are many honeypot available in the market like Dionaea, Kippo, Glastopf, and JHoneypot. In our systemwe are capturing malicious activity performed using Email, Filesystem, Port.

So most of the systemuses single honeypot for a particular intrusion activity.Dionaea aims to trap malware feat vulnerabilities exposed by services offered over a network (like IPv6 protocol and TLS service) and ultimately obtain a copy of the malware.

Now a day'sattackers are gaining interest in IPv6 networks. Therefore, we propose Dionaea, a low-interaction IPv6honeypot that can simulate entire IPv6 networks and which may be used to detect and analyze IPv6 network attacks. Dionaea the first low-interaction honeypot which is able to simulate entire IPv6 networks on a single host. We increase the chance for an attacker to find a target host in our IPv6 honeypot by reacting to the attacker's requests with the dynamic generation of new IPv6 host instances in the honeynet.

Honeypot is a system which is used to capture the intrusion in a network.But, IDS is not efficient to handle the intrusion. The common IDS's tends to provide the attacker with all the required resources needed for a successful attack. So we are using honeypot to know the intruders. Honeypot provide a platform to know which methods and tools are used to attempt the attack. In this we are using a different honeypot like Dionaea, Glastopf, Kippo, HoneyD and J-Honey.

2. LITERATURE SURVEY

[1]This paper describes a case study of Honeypot deployment inan organizational network. As per Wikipedia "honeypot is a trap that is set to track, deviate, or in some way rectify attempts at illicit use of information systems". These tricks could be any digital resource which range from a single computer to a network of such computers or a network application that appears tobe a partof organizational network resources but, actually is an unreal resource with no production traffic. Additionally the resources are closely controlled and the traffic to and from these resources is well under the mastery of the administrator. In the experiment performed in this paper, such a trick is laid in the form of a low interaction honeypot honeyD in the edge security of an organizational network. The results of deployment are unfilled and further various props and cons of such distributions are carried about.

[2]Progressive Technology in the area of intrusion detection is the Honeypot technology that distinct mutual IDS s inclines to provide the attacker with all the necessary resources required for a effective attack. Honeypot provide a platform for learning the methods and tools used by the intruders, thus deriving their value from the unauthorized use of their resource. To provide accessible, early warning and analysis of new Internet threats like worms or mechanized attacks, weoffer globally distributed, hybrid monitoring model that can capture and analyze new vulnerabilities and exploits as they occur. To achieve this, our Model increases the exposure of high-interaction honeypots to these threats by employing low-interaction honeypots as frontend content filters. Host-based techniques capture related details such as packet payload of attacks while network monitoring provides wide exposure for quick recognition and valuation. To lessen the load of the back end's, we filter rampant content at the network frontends and use a new handoff mechanism to allow interactions between network and host workings.

[3]A Honeypot is an information system resource used to avert invaders and hackers away from acute resources as well as a tool to study an attacker's methods. One of the most broadly used tools is honeyD for forming honeypots. The logs generated by honeyD can raise very huge in size when there is heavy attack traffic in the structure, thus overriding a lot of disk space. The huge log size stances trouble when they are processed and analyzed by security analysts as they consume a lot of time and resources. In this paper, we propose a system which addresses these issues. It has two important modules.The first one is classification module which saves disk space by falling the log size without losing data. The second module is a loganalyzer that can process this log to produce reports and graphs for the security administrators. The analyzer is regressive well-matched and can process the log file produced by honeyD as well. The investigational consequences show that the space required by log file reduces considerably.

[4]In this short paper, an involuntary malware analysis framework is introduced to simplify the security community to have the stride of rapidly fluctuating malwares. In our framework, thehoneynet technology and Taiwan Malware Analysis Net (TWMAN) can concurrently collect and examine the latest malicious software. The well-organized malware database and distributed platform can help security authorities in searching malware patterns. Owing to the occurrence of Bonnet, the number of malware increases rapidly. Our reflex malware analysis framework is an outstanding solution to pact with the Bonnet problem.

3. PROPOSED WORK

In this work, we will deploy scalable honeypot to capture malicious network traffic and malwares. Malwares captured using this mechanism was minimal. The scalable architecture well suited for organization to the effect of attacks that are on their network.

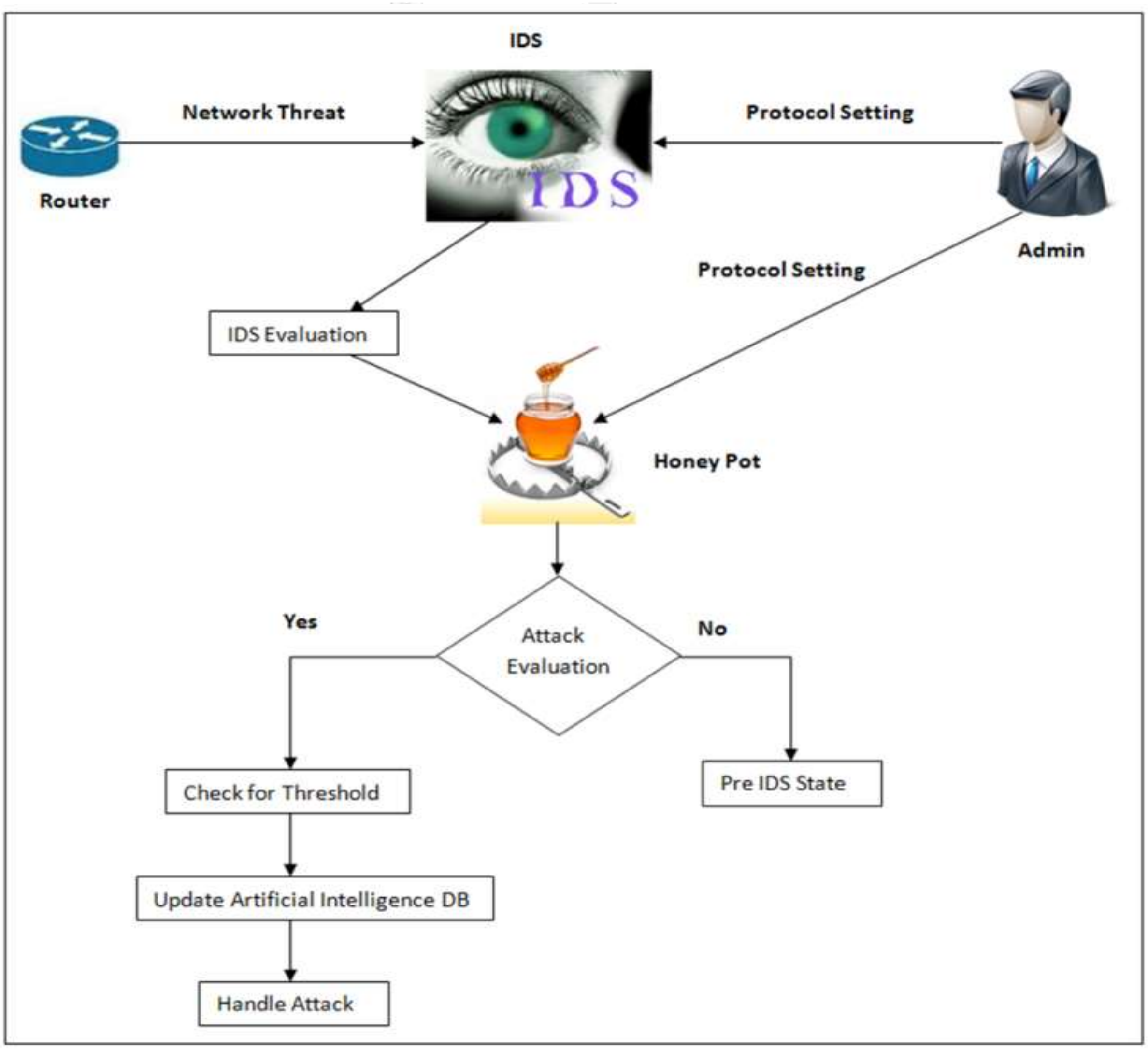
•ARCHITECTURAL DESIGN

- IDS:

Intrusion Detection System (IDS) is the system used for security in computer network. They are collect unused packets and stored into their database. The unused packets are fulfilling by the valid user.Every time IDS check the user valid or not.

- STORAGE NODE:

This is an entity that stores data from IDS and provide corresponding access to users. It may be dynamic or static. Similar to the previous schemes, we also assume the storage node to be semi trusted,that is honest but curious.



- Honeypot:

Server honeypot are services run in physical machine for the sole purpose of capturing attacks and malwares. These honeypot take up unused IP address space of an enterprise network and continuously listen on all the malicious activities performed by a hacker.Mostly,these are capable of collecting a vast amount of automated attack caused by botnets and other automated tools.Even though,there are couple of commercial product server honeypot are still evolving and are researched widely.

4.Mathematical Model::

SET THEORY OF PROJECT:

1. **SETTING IDS PARAMETERS**

Set I:

I0= Login using user name and password

I1= Set Intrusion keywords

I2= Set Website name for Web IDS

I3=Save in Database

2. **SETTING HONEYPOT PARAMETERS**

Set H:

H0= Login using user name and password

H1= Set HoneyPot Keywords

H2= Set Website name for HoneyPot

H3=Save in Database

3. **IDS ACTION**

Set A:

A0=Get data from email, port, IP and web

A1=checks for Keyword

A2=If found then declare as Intrusion

A3=Create a GIDO (Generalize Intrusion Detection Object) object

A4=send GIDO to honey manager

4. **HONEYPOT ACTION**

Set Y

Y0=Get GIDO object from IDS

Y1=Check for the key word in database as rules

Y2=If found then take create report

Y3= else, get the Pre IDS state from IDS

Y4= Restore action

5.Operating Environment

This project is stand-alone based, so it will be running on any machine which is powered with Java.

A.Operating Environment

1. Windows Xp,Windows 7, Windows 8, Windows 10

2. Ubuntu

B.Software Requirement

1) Platform: JAVA
2) Technology : JDK 1.6 and Above
3) IDE: Netbeans 6.9.1,
4) Data base : MySQL 5.0

C.Hardware Configuration:

A.**systems of following minimum configuration**

1) Processor: Dual Core of 2.2 GHZ
2) Hard Disc: 100 GB
3) RAM : 2GB
4) Network Switch : D-Link 5 port Ethernet
5) Cables : CAT 5/6

6.ALGORITHM

```
Input: Attack Threat from network data
Output: Handling attack
Step 0: Start
Step 1: Receive threat T by IDS
Step 2: Check for the protocol in the database
Step 3: If present in the DB
Step 4: then label threat T as $T_i$(Identified Threat) by IDS
Step 5: Forward to Honeypot
Step 6: Receive $T_i$ by Honeypot
Step 7: Check for the protocol in database
Step 8: If present in the DB
Step 9: then check for threshold
Step 10: Update AI database
Step 11: Handle attack
Step12: Else
Step 13: Maintain Pre IDS state
Step 14: Stop
```

7. CONCLUSION

Our demonstration showed that most of the malicious activities were brute force logging in the service to access data of the system. The malwares which were captured using this function was minimal. The scalable deployed architecture is well suited for organization to understand the consequence of the attacks that are on the system.

.

8.REFERENCES

[1] Hamid Mohammadzadeh.e.n, Roza Honarbakhsh, and Omar Zakaria, "A Survey on Dynamic Honeypots", International Journal of Information and Electronics Engineering, Vol. 2, No. 2, March 2012

[2] Sanjeev Kumar, Paramdeep Singh, RakeshSehgal, and J. S. Bhatia, "Distributed Honeynet System Using Gen III Virtual Honeynet", International Journal of Computer Theory and Engineering, August 2012

[3] Paul Baecher , Markus Koetter , Thorsten Holz , MaximillianDornseif , Felix Freiling, "The nepenthes platform: an efficient approach to collect malware", Proceedings of the 9th International Conference on Recent Advances in Intrusion Detection, September, 2006

[4] Dionaea honeypot Tool, http://dionaea.carnivore.it

[5] Glastopf Tool, http://www.glastopf.org

[6] HoneyD, http://www.symantic.com/connect/articles/open-sourcehoneypots-learning-honeyd