

An Approach to for Improving the Efficiency of IDS System Using Honeypot

By

Khushboo Saxena, Akanksha Saxena, Seema Arya
Technocrats Institute of Technology, Bhopal, India
Suresh Gyan Vihar University, Jaipur, India

sexn.khushboo@gmail.com, akanksha.saxena23@gmail.com, seema.aarya@gmail.com

ABSTRACT

Increasing technology space has pressurized the organisational environment to safeguard its network from outside as well as inside attack. Any malicious intrusion can drag down a highly reputed organisation to the floors of defamation and even insolvency. Henceforth network security is one of the biggest challenge for organisation. Although traditional concepts of firewall and intrusion detection system is prevailing yet there is a need to secure the environment from the so called zero day attacks. Attackers every now and then generate exploits to penetrate the secure network environment and the existing known signatures are not able to detect such an attack. This paper brings forth the concept of deployment of honeypot so as to make the IDS system more effective and efficient for the zero day attack leading to least penetration to the network environment. This paper lays down a new network architecture so that the IDS system can be updated with the latest attack scenarios. The aforesaid objective is achieved with the help of establishment of honeypot. Later tcpdump is used for the further analysis of payload so as to generate alert signature in IDS (Snort v2.0).

Keywords

Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

1. INTRODUCTION

The high use of internet in today's IT world has purged in the concept of security deployment in the organization so as to make it almost immune to various upcoming attack scenarios. One of the critical areas is the protection of internal network from new attacks. Although the most desirable is the deployment of intrusion and prevention system in the network architecture but this system is still vulnerable to zero day attacks. The IDS generally includes signatures for known attacks and generates the alerts for the same but if any new attack penetrates the system then it lags behind. To deal with

this problem the concept of honeypot can be used along with any packet analyzing tool so as to generate signatures for zero-day attacks in IDS.

The Intrusion Detection System specially involves two types of techniques: Anomaly Detection involving the detection based on behavior/heuristic rules and Misuse Detection involving the detection based on patterns and signatures. Anomaly detection lags behind as it requires too much time to detect the behavior and Misuse Detection lags behind for detection of new attack signature. So Honeypot is used as a tool to support the technique of Misuse Detection so that new attacks can be detected before they can harm internal network and the signature can be framed in the IDS to defend the network from internal and external threat of such attack in future.

Honeypots are Bait Servers which are not the part of any production server in the organization and are just placed isolated so as to attract the attackers to plug and play with it and at its end it logs all the actions of the attacker so that it can be analyzed further to generate signatures for IDS. Attackers before making an attack perform a ping sweep and if the honeypot is pinged. As the request reaches the honeypot server it records all the activities, even the keystrokes typed by the attackers so every command entered by the attacker becomes a part of log to the honeypot server. It also stores all tools used by the intruders in records as a forensic machine.

The given paper describes how the data returned from the honeypot server is used to write custom IDS rules. Thus new network architecture is designed to collect the response to write custom IDS rules by seeing the data payload and writing the rules matching the payload.

2. RELATED WORK

One of the drawback stumble upon with network intrusion detection systems is that the logging of failed connection attempts just occurs when services are not listening on a scanned port. When a RST signal terminates a TCP connection attempt, the system never logs the data packet that the remote machine was trying to send into the network. A honeypot as a one of the greatest security tool suggests a mechanism by completing the connection attempt and providing an attacker a false illusion of accessing the critical servers and then recording the interactions between the honeypot and the remote machine.

Honeypot placement is one of the greatest issues to be taken care of to optimize the efficiency of the implemented Intrusion Detection System. Various network architectures are presented till now to achieve the aforesaid motive but the basic idea behind this as we suppose is detection of hackers scripts and actions to penetrate into the system and henceforth the proposed architecture is presented which will help the organizational security to build up patches for the existing loophole and make their system robust and stringent to attack scenarios.

3. PROPOSED DESIGN AND IMPLEMENTATION

In this section we outline the requirements of the proposed infrastructure which is considered as a solution to decrease the malicious inflow of packets in the organizational environment and enhance the efficiency of IDS system deployed.

The real honeypot server is used to safeguard the main server from if the hacker is able to compromise the honeypot server. Although it is hard to implement the real honeypot but it is desirable for large organizations as such servers do not hamper the production process in the organization and only IT staff is able to access the required logs. Neither the attacker nor the organizational staff knows where honeypot is placed.

The given network architecture is used to develop an understanding as to why and how honeypots are used to enhance the work of IDS system.

In this configuration, main network is a "TCP/IP based network" which contains clients and servers. Snort 2.0 is used as IDS and is capable to be configured with server. Honeyd is a honeypot system that is configured as a separate server and is connected to the main server. We assume a "switched network" in our approach, with a configurable switch which is connected to the main server and the respective clients. As the LAN architecture is developed in within a primary network henceforth the server is supported with two Ethernet cards eth0 and eth1. Eth0 directs the internet connection to the main sever and eth1 manages the intranet traffic within the private LAN 192.168.0.1.

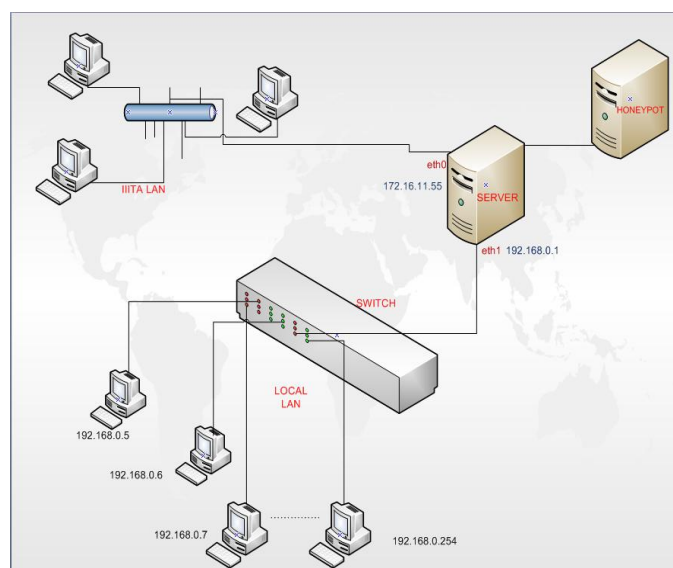


Fig 1.1 Deployment of IDS & honeypot in the LAN Architecture

The attacker first performs a ping sweep attack to detect the available servers in the network and the honeypot server entices him to perform attacks to penetrate the network. Once the requests are directed to the honeypot server the incoming connection is established with the attacking system. As the attacker gets a feel of entering into the server it performs all his efforts to penetrate into different servers. Honeypot gives him the illusion of different servers and constantly interacts with him to record his activities and send the specific response to the syslog server for future analysis and investigation.

4. Experimental Setup

To implement honeypot an additional tool Arpd is embedded in it. Honeypot cannot do everything alone and requires the help of Arpd. Arpd is used for ARP spoofing; this is what actually monitors the unused IP space and directs the attacks to the honeypot. Honeyd is only able to interact with attackers. For example if the aim is to monitor all the unused IPs in the 192.168.1.0/24 network, the required commands to start both Arpd and Honeyd are as follows:

```
arpd 192.168.0.1/24
honeyd -p nmap.prints -f honeyd.conf
192.168.0.1/24
```

Based on the commands, the Arpd process monitors the unused IPs, directs all corresponding attacks to the honeyd and spoofs the victim's IP address with the MAC address of the honeypot. For the honeyd command -p nmap.prints refers to the nmap fingerprint database and -f honeyd.conf is the honeyd configuration file.

Once the installation is honeypot server is completed the traffic directed to honeypot server is dumped o other system using packet analyzing tool tcpdump with the help of following command:

```
tcpdump -nn -x -s 1500 host 192.168.0.145 -w store.cap
```

The tcpdump command will dump all the malicious packets directed to the honeypot and hence will help in writing the snort rule set by analyzing the payload.

4.1 Writing of Snort Rules:

Penetrating in the network to gain access by getting the etc/passwd file in the Linux environment or the password shadow file i.e. etc/shadow which contains the username and password of all users. No such rule is defined in the latest snort rule set. Suppose you get the following log generated in honeypot:

```
# cat 44F75D6380122.shell  
.....  
GET/unauthenticated/..%01/..%01/..%01/..%01/..%01/..  
%  
01/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..  
.br/>%01/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..  
1/.br/>.%01/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..  
01/  
..%01/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..  
01  
/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..%01/..  
%0  
1/..%01/..%01/..%01/..%01/..%01/etc/shadow HTTP/1.1  
Host: 202.174.22.145:10000
```

It is visible that the attacking port is 10000 thus port 10000 is of interest. The various ip addresses from where such request came can be filtered using tcpdump analysis.

4.2 Results and Discussion

Once the analysis is done now it is the time to write the snort rule. By the analysis of the payload it is visible that the string started with “GET/unauthenticated/” thus following snort rule can be set:

```

alert tcp $EXTERNAL_NET any ->
$192.168.0.1 10000\ (content:"GET /unauthenticated/";
msg:"Get unauthenticated");

```

Now any attack coming from the specified port will generate the alert to the administrator of penetration for unauthorized access in the network environment by the attacker.

If the set rule has to be further customized then the following payload can be added:

```
alert tcp any any -> any 10000 \
(content:"GET /unauthenticated/..%01/..%01/"; msg:"Get
unauthenticated");
```

The point of concern here is that adding too much of payload may result in false negatives which will overall lower down the implementation of snort in organizational network.

5. Conclusion

The Intrusion detection system can only give the optimum benefit if it is also able to detect those attacks for which signatures are not defined in its database. The area of work will be to give attention to this Snort limitation and thus increasing the scalability and responsiveness of the system towards the various types of attacks so as to achieve the motto of building a smart agile and secure system to face the new challenges of technological arena. Though honeypot deployment is a cost-effective solution for the security of large organization but in future refinement is required to elimination false alarm generations.

6. REFERENCES

- [1] Vidar Ajaxon Grønland: Building IDS signatures by means of a honeypot Norwegian Information system Laboratory.
- [2] Chi-Hung Chi , Ming Li Dongxi Liu : A method to obtain Signatures From Honeypots Data, School of Computing National University of Singapore
- [3] Babak Khosravifar, Jamal Bentahar: An Experience Improving Intrusion Detection Systems False Alarm Ratio by Using Honeypot.
- [4] Department of Electrical and Computer Engineering, Concordia University
- [5] Greg M. Bednarski and Jake Branson: Understanding Network Threats through Honeypot Deployment, Carnegie Mellon University March 2004.
- [6] Richard Hammer : Enhancing IDS using, Tiny Honeypot SANS Institute InfoSec Reading Room
- [7] Solution Base: What you need to know about honeypots http://articles.techrepublic.com.com/5100-22_11-5758218.html