DEPLOYMENT OF LOW INTERACTION HONEYPOT IN A PRIVATE NETWORK

Jashanpreet Singh Toor
Department of Computer Engineering
Punjabi University, Patiala, India

Er. Abhinav Bhandari
Department of Computer Engineering
Punjabi University, Patiala, India

Abstract: A honeypot is a security system whose value lies in being probed, attacked. A honeypot is forcefully made to be attacked to gather information about unauthorized activity. Our research paper provides a brief explanation of such a system and demonstrates how it can be implemented to improve the security of the organization and across critical systems and networks. In the experiment performed in this paper, such a trap is laid in the form of a low interaction honeypot deployed using pentbox 1.8 framework in a private network. The results of deployment are presented.

Keywords: Honeypot, network, IDS

1. INTRODUCTION
As the organizations are becoming more and more dependent upon their network infrastructures, these network infrastructures are becoming more and more complicated for providing the necessary services [1]. Due to this added complicacy in the network architectures to provide seamless automation to the organizational day to day routine work the conventional network security devices are failing to provide the level of comfort required by the network administrators. Hence there is a need of a context sensitive approach/technique for the prevention, detection and responding to the attacks performed on these complex networks.

A honeypot is deliberately to be attacked to gather information about unauthorized activity (Kinsella, 2005). An intrusion detection system which generates no alerts may be indicator of normal network activity. However a honeypot that does not get attacked is worthless. Here in this paper we have done such a study by deploying a low interaction honeypot by using pentbox framework in a private network. The results are presented along with benefits and issues involved in such deployments.

2. WORKING OF HONEYPOTS
The concept of honeypot is quite simple. It acts as a resource which has no productive value, it works by deceiving intruders into believing it to be genuine system with genuine data and they attack the system without knowing that they are being observed completely. [3] Honeypots are, in their most basic form, fake information severs strategically-positioned in a test network, which are fed with false information disguised as files of classified nature. When any external system tries to connect to the honeypot, all of its system related information, such as the IP address of the attacker, operating system, port accessed, browser, version etc. will be collected. Most important part of a honeypot system is capturing data, payloads, packets the ability to keep log, alert, and capture everything the attacker is doing. Features of a honeypot system as suggested by Bouget & Holz
A. To divert the attention of the attacker from the real network, and making sure that the main server is not compromised.
b. To identify the preferred attack methods used more commonly and make similar profiles of attackers as used by law enforcement agencies in order to identify a criminal.
c. To capture new attack entities for future study
d. To identify new vulnerabilities and risks of various operating systems, environments and programs which are not thoroughly identified at the moment [4]

In a more advanced context, a group of Honeypots becomes a Honeynet. It acts as a tool that monitors wide group of possible threats which gives a systems administrator more information for study. It makes the attack more fascinating for the attacker due to the fact that Honeypots can increase the possibilities, targets and methods of attack [5].

HONEYPOT DESIGN AND ITS DEPLOYMENT ISSUES.
On the basis of design deployment of the Honeypot, it can be divided into Production and Research Honeypot [6]

A. Production Honeypot
These honeypots are used to protect the organizations in real production operating environments [7], constant attacks 24/7. These honeypots are constantly gathering more importance due to the detection tools they provide and because of the way they can complement network and host protection. This type of honeypot emulates specific services and sometimes even operating systems to lure the attackers.
A honey pot cannot prevent an unpredictable attack but can detect it. One case where they prevent the attacker is when he directly attacks the server. It will prevent attack on a production system by making the hacker waste his time on a non-sufficient target. [8].
B. Research Honeypot
Research honeypot collects important information about the nature of attacks, their motives and methods and tools used by attackers. Honeypot provides detailed information of the attack i.e. how attack happens, tools used by attackers etc. It is used to research the threats organizations face, and to learn how to provide better protection against those threats. According to the level of interaction of the honeypot [9], it can be divided into low, medium and high interaction honeypots

C. Low Interaction Honeypot
Low interactive honeypots are system which emulates the services and are easy to configure, deploy and setup and has lower interaction performance. It helps to detect known vulnerabilities and measure how often attackers attack

D. Medium Interaction Honeypot
This honeypot deceive the attacker with providing fake interfaces of the attacker and then stores all the activities done by attacker against different services. A medium interaction honeypot is somewhat advance than low interaction honeypot. These can range from simple port listener to a complex complete host just sitting on a network waiting to be attacked.

E. High Interaction Honeypot
These system provide real service to the intruders and full OS access to them. As attacker can get root access so the risk associated with these honeypots is the maximum.

PENTBOX 1.8 FRAMEWORK
Pentbox is a framework that consists of security and stability testing oriented tools that are commonly used in networking. It is developed in ruby and oriented to GNU/Linux systems, but is compatible with every systems where Ruby works. Tools in pentbox 1.8 :

I. Cryptography tools
- Base64 Encoder & Decoder
- Multi-Digest (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)
- Hash Password Cracker (MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD-160)
- Secure Password Generator

II. Network tools
- Net DoS Tester
- TCP port scanner
- Honeypot
- Fuzzer
- DNS and host gathering
- MAC address geolocation (samy.pl)

III. Web
- HTTP directory brute force
- HTTP common files brute force

3. HONEYPOT ARCHITECTURE AND CONFIGURATION

A monitoring infrastructure needs to be deployed in a well-controlled lab environment consisting of sensor, honeypot server as well as a logging server. One more sensor Wireshark will be working with the honeypot at the server.

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark helps us understand what is happening in our network on a microscopic level.

Configuration of honeypot.
We have used Ubuntu operating system for setting up the server. After firing up the terminal we start the pentbox 1.8 framework. Pentbox honeypot will only work if we give sudo privileges.

First go to the pentbox directory and the path of its ruby module.

Cd pentbox-1.8 / sudo .pentbox.rb
Then select option 2. **Network Tools.**

Start Wireshark and then click on the network interface you want to use to capture the data. On a wired network, it will likely be eth0. On the honeypot we use wireshark to monitor the network traffic. We have activated honeypot on port 80.

Port 80 is the port number assigned to commonly used internet communication protocol, Hypertext Transfer Protocol (HTTP). It is the port from which a computer sends and receives Web client-based communication and messages from a Web server and is used to send and receive HTML pages or data.

The server is usually the IP the TCP SYN packets are sent to, while the source of the SYN packets in the client. So you could filter on the SYN packets using "tcp.flags==2" and see which IPs are targeted.

One way is to click Statistics>Conversations this will open a new window and you can click ipv4 or tcp option to check out the Destination IP/src IP/port/dst port.

**Fig3 Screen shot of Real time capture of tcp packets using Wireshark.**

**Fig4 Screenshot of Wireshark statistical analysis for source and destination addresses.**
4. RESULT AND CONCLUSION

After the service runs we will see how pentBox will record every connection made. Honeypots, by definition, see only "bad" traffic. Honeypots only report the connections they receive and most of these will be real attacks. Whenever a system tries to connect with the honeypot server, the server records its information.

Fig 5 Screen shot of Honeypot showing the information about every connection that is detected.

Information recorded by our honeypot.

INTRUSION ATTEMPT DETECTED! From 192.168.232.1:52419 (2017-07-29 12:16:03 -0700)
GET / HTTP/1.1
Host: 192.168.232.128
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/59.0.3071.115
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8

INTRUSION ATTEMPT DETECTED! From 192.168.232.128:58618 (2017-07-29 12:21:29 -0700)
GET / HTTP/1.1
Host: 192.168.232.128
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv: 45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive

After knowing which IPs are trying to attack, we can do prevention by blocking the ip or applying our tools as required. As you can see, we now know where the attacker came from, what exploit method was used and the time the exploit was attempted.

Honeypots can be used in securing the network of an organisation. Honeypots acts as early alarming tools to secure the organization technologies. Still IDS technology is not such powerful to protect global information infrastructure completely. In this paper we have reviewed a basic honeypot. Hence we can safely conclude that different types of honeypots can be used to detect different types of attack signatures and rules can be defined to filter the traffic based on information gathered.

REFERENCES

[1] Saurabh Chamotra, J.S.Bhatia, Raj Kamal, A. K. Ramani “Deployment of a Low Interaction Honeypot in an Organizational Private Network” IEEE 2011.
[2] Qassim Nasir and Zahraa A. Al-Mousa “Honeypots Aiding Network Forensics: Challenges and Notions” Journal of Communications Vol. 8, No. 11, November 2013
[3] Carlos Francisco Lerma Reséndez, Miguel Hernández y López “Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses” Informing Science & IT Education Conference (InSITE) 2008
[4] Spitzner, L. (2002). Honeypots: Tracking hackers Boston: Addison-Wesley.
[5] http://www.honeynet.org.pt/index.php/HoneyMole
[6] John Harrison, J.H (2003) Honeypots: The sweet spot in network security.
[7] Miguel Hernández y López (2008). Honeypots: Basic Concepts, Classification and Educational Use as Resources in Information Security Education and Courses. Proceedings of the Informing Science & IT Education Conference (InSITE) 2008
[8] http://www.infosec.gov.hk/english/technical/files/honeypots
[9] Neha Sahu, Vineet Richhariya ‘Honeypot: A Survey’ IJCST Vol. 3, Issue 4, Oct - Dec 2012
[10] Mohd. Junedul Haque “An Approach for Intrusion Detection using Honeypots to Improve Network Security” (IJRASET-2015)