Detection of threats in Honeynet using Honeywall

Navita Sharma[1]
Student of Master of Technology,
Computer Engineering Department,
Yadavindra College of Engineering,
Talwandi Sabo, Punjab, INDIA
skysdlimit10@gmail.com

Sukhwinder Singh Sran[2]
Assistant Professor,
Computer Engineering Department,
Yadavindra College of Engineering,
Talwandi Sabo, Punjab, INDIA
sukhwinder.sran@gmail.com

Abstract - **Information is a strategic resource and to protect this kind of confidential and private data against possible attacks, you must take into account some security mechanisms and measures. And as Computer network are subject to electronic attacks. This led to growing interest in more aggressive forms of defense to supplement the existing methods. One of these methods involves the use of Honeypots. A combination of bait and trap to capture the identity of intruder, as the intruder is not physically present is Honeypot. For securing large network we use honeynet which are network of honeypots. In this paper we are going to address the need of a honeywall and how it is used in honeynet environment to trap attackers. Honeywall is a power full tool for capturing attacks in honeynet environment. The information gathering from honeywall would be used in designing an efficient model against malware in computer networks.**

Keywords: honeypot, honeynet, honeywall.

I. INTRODUCTION

In recent years, with fast development, network has extended to every social and technical corner, and people have been led into the era of information technology. Computer networking remains one of the most exciting and challenging research domains of our time. As technology progresses, so do the capabilities of these networks. Security has become a growing concern today for organizations, networks and individuals etc. This led to growing interest in more aggressive forms of defense to supplement the existing methods.

One of these methods involves the use of Honeypots. Honeypot is a security resource whose value lies in being probed, attacked or compromised [5]. Today many non-profit research organizations and educational institutions

research use honeypots to analyze attacks and vulnerabilities, and learn more about the techniques, tactics, intention, and motivations of the attackers.

A Honeypot is a special constructed computer or network trap designed to attract and detect malicious attacks. It has no production value other than to draw malicious traffic and capture it. By avoiding legitimate traffic it can be considered that all the traffic that passes from a honeypot is malicious, and this means that false positives are avoided.

We can classify honeypots in two main categories on the bases of interaction [5]: low interaction and high interaction. Interaction we mean to say the level of activity a honeypot allow to an attacker. These help us to understand what type of honeypot we are dealing with.

In low interaction we provide emulating services and operating system to the attacker. This type of honeypots has limited interaction with the production system. These honeypots are easier to deploy and maintain. The emulated services mitigate risk by containing the attacker's activity, the attacker never has access to an operating system to attack or harm others.

In high interaction honeypot nothing is emulated it involve real operating system. We provide attackers real thing. By giving real system we can capture extensive amount of information, we can learn full extent of their behavior.

For securing large networks we use honeynet. A honeynet is collection of honeypots or network of honeypots. A Honeynet contains one or more Honeypots, which are computer systems on the Internet expressly set up to attract and "trap" people who attempt to penetrate other people's computer systems. The basic definition construct by Ryan Talabis[4] : "A honeynet is a network of high interaction honeypots that simulates a production network and configured such that all activity is monitored, recorded and in a degree, discretely regulated". Honeypnets are not a product; they are not a software solution that you install on a computer. Whereas honeynets are architecture, whole network of computers designed to attack.

II. Related work

Several papers have been published on honeypot technology. We are discussing few of them. In "A technique for detecting new attacks in low-interaction honeypot traffic", S**. Almotairi, A. Clark, G. Mohay, and J. Zimmermann** presents a technique for detecting new attacks based on principal component of attacks [1]. Shishir kumar presents solution for preventing a network from malware in "detection and prevention of new and unknown malware using honeypots" [2]. In "honeypot based defense system research and design" [3].zhang li-juan presents defense security network and distributd intrusion prevention model using honeypot technology.

III. Honeywall Tool

Honeywall is a gateway device that separates our honeypot from rest of the world. Any traffic going to or from the honeypots must go through the honeywall. This device should be invisible to anyone interacting with the honeypots. A Honeywall is used to safeguard honeypots in the network from malware. It can translate and route packets by changing IP and MAC addresses.

Honeywall has three main goals:

Data Capture: All activities of the attacker within the honeynet and the information that enters and leaves the honeynet should be captured without attackers knowing they are monitored.

Data Control: To control suspicious traffic entering or leaving the honeynet. Moreover, this mechanism must ensure that once a honeypot within the honeynet is compromised, all malicious activities must be contained within the honeynet.

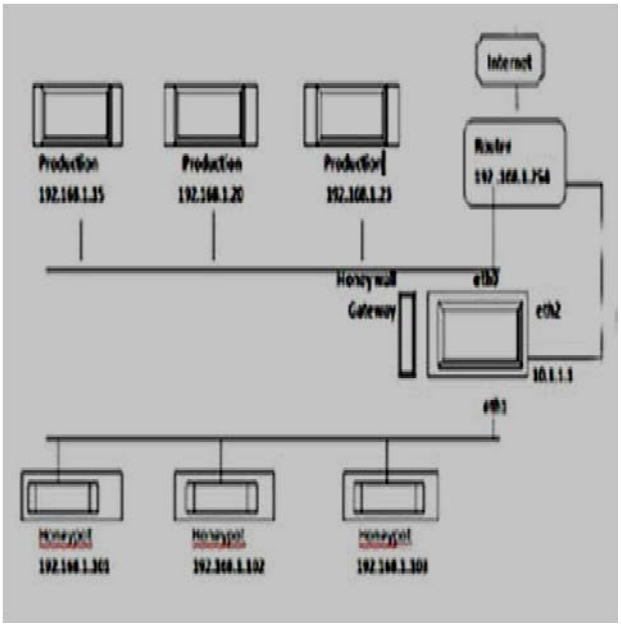
Data Analysis: The ability to analyze data. The whole purpose of honeypot to gather information, it is useless if we not able to convert the data into useful information. So it is necessary to analyze the data and use it for analysising attacks.

IV. Model architecture

The architecture given in fig.1 for deploying a honeywall in honeynet.In this architecture honeywall is deploy between the production system and honeypots. In this honeywall works as a gateway which separates the honeypots from rest of world. Any traffic going to or from the honeypots must go through the honeywall. Our honeywall has three interfaces. The two interfaces (eth 0 and eth 1) separate our honeypots from everything else. The third interface is optional for remote management.

Honeywall provides data capture, data control, data analysis and data collection. Implementing these keys is very difficult and time consuming. So honeynet project has developed a fast and easy way to deploy such functionality, its call honeywall CDROM [6]. The purpose of this bootable CDROM is to make it easy to deploy a honeywall.

Fig.1 Architecture of Honeywall [6].



Honeywall CDROM is a bootable CDROM which contain all the tools and functionality necessary to rapidly deploy, maintain and analyze a honeynet environment.

Honeywall CDROM includes the following security tools:

Tcpdump: Packet analyzer

Sebek: Data capture tool

Snort: Intrusion Detection System (IDS).

Snort_inline: Intrusion Prevention System (IPS)

Hflow2: A data correlation tool for Honeynet data analysis.

P0f: Passive OS fingerprinting tool

Walleye Web Interface: Walleye Web Interface is a web-based Graphical User Interface that is used for Honeywall configuration, administration and data analysis. We used this web interface in order to analysis the inbound and outbound traffic through a web browser client by typing https://193.x.x.x (where 193.x.x.x is the Public IP address).

Snort IDS and Snort-inline IPS

Snort as an Intrusion Detection and Prevention System is integrated into Honeywall. It is an open- source IDS, rule- and signature-based engine that can be run in one of the following modes: Sniffer Mode In this mode Snort is used as packet sniffer and displays IP headers on the screen. Logger Mode all packets are logged into the file and can be used for further analysis. Network Intrusion Detection Mode is the core mode of Snort. All incoming packets will be analyzed based on the user-defined rules and signatures. Snort will log, detect and alert if there is any anomaly detection in the packets then Inline Mode. In this mode, Snort acts as an Intrusion Prevention System (IPS) which is called Snort-inline. It resides on the Honeywall where the packets are analyzed and monitored using iptables in order to control outgoing packets from the honeypots. If the honeypots are compromised by worm or attacks, Snort Inline will prevent the attackers from compromising other machines in the same network.

Sebek as a Data Capture tool

Sebek is a data capture tool that is used to capture all attackers' activities (keystrokes, file transfer, encrypted traffic, and commands). It is based on client-server architecture, and it can be installed as a linux kernel module (LKM) on Linux and as an OS kernel driver on Windows. Then, the data captured from the honeypots by the sebek clients will be sent to the Sebek Server which collects and processes the received logged activities in the form of Sebek packets. These packets are hidden from the attackers. Sebek itself can be hidden and configured in such a way that attackers cannot detect it.

This tool is utilized for observing attacks and to learn the skill level of attackers. Thus the attacker's skill level can serve as a base for formulation of reaction model against the malware and black –hat community in the computer network organizations.

V. Conclusion and future outlook

In this paper, we have provided a brief overview of honeywall which is deployed in a honeynet environment for trapping attackers. This tool is easy to deploy and save time. It consists of many tools and functionality which make it powerful to collect extensive information on variety of threats. Hence, it helps in securing honeynet by detecting threats and attackers efficiently. the attacker's skill level can serve as a base for formulation of reaction model against he malware and black –hat community in the computer network organizations.

The honeynet is a new technology its aim to overcome traditional security tools. Although honeynet have obtains lot of focus in recent years, honeywall is still in the developing phase.Because they are used to gather information on attacks and threats, its implementation in an organization will prove a useful security tool. So in future scope the implementation of proposed technique is possible.

ACKNOWLEDGMENT

We are grateful to our computer science & engineering department for supporting us. This paper was written as a part of thesis work in master of technology, supervised by Sukhwinder Singh Sra.

REFERENCES:

[1] S.Almotairi, A.Clark "A Technique for detecting new attacks in low-interaction honeypot traffic" in 4th international conference on internet monitoring and protection, 2009.
[2] Shishir Kumar, Dugesh Pant "Detection and prevention of new and unknown malware using honeypot" in international journal on computer science and engineering vol.1 (2), 2009, 56-61.
[3] Zhang Li-juan, "Honeypot-based defense system research and design" in 2nd IEEE international conference on computer science and information technology, 2009.
[4] Ryan Talabis, "Definition of honeynet" in Philippine honeynet project.
[5] www.philippinehoneynet.org.
[6] Lance Spitzner, "Definition and value of honeypot" www.tracking-hackers.com .
[7] Lance Spitzner, "Know your enemy: honeywall CDROM".
[8] www.honeynetproject.org.