International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

Modern Attack Detection Using Intelligent Honeypot

Rahul koul[1], J. W. Bakal[2], Sahil Dhar[3]

[1]Department of Computer Engineering, PCE College, New Panvel, Maharashtra, India
[2]S.S. Jondhale College of Engineering, Thane, Maharashtra, India
[3]Security Analyst, Security Innovation Pvt. Ltd., Pune, Maharashtra, India

---

Abstract - *In today's networked world, it is very important for any organization to protect its assets from being attacked by attackers. To pursue the dream of total security, one needs to be one step ahead from the attackers or we can say one needs to determine the possible attack before its been taken place. One such tool to monitor the behaviour of attackers is honeypot. A Honeypot is a network system to determine the unauthorized use of information system by analyzing the behaviour of attacker in an isolated and monitored environment. But, there are tons of honeypot implementation implemented till date, however one thing missing from each of the honeypot implementation is continuous learning of trending attack scenarios and no human decision-making capabilities. In this paper, we proposed a solution for detecting modern attacks by introducing a semi automatic approach of attack detection via honeypot coupled with human decision-making capabilities. We have introduced a separate team that will analyze the uncommon web/network attack pattern and update the honeypot attack detection database and thus improving the overall attack detecting efficiency of honeypot.*

Key Words: **Honeypot, Attack, Detection, Behaviour Analysis, Attack Pattern, Manual Analysis.**

1. INTRODUCTION

In the past few years many security tools have been developed to protect organizations from cyber threats. Despite of these security tools and security layers such as traditional Firewalls, IDS, IPS etc. in place, attackers were still able to carry out high level targeted attacks. A failure in operational security depends on numbers of variables, however majority of them depends on differentiating between an attacker and a legitimate user. To overcome the failure in understanding the difference between a legitimate request and a malicious request, tools such as Honeypots were introduced. A Honeypot is a information system whose values lies in monitoring, detecting and deflecting possible attacks from the attacker by posing itself as a vulnerable system.

The purpose of Honeypot systems is to log every possible malicious activity of an attacker depending on the type of Honeypot system implemented within infrastructure. Honeypot systems can be used to identify different types of malicious activities such as web application attacks, known vulnerability exploitation, exploitation of outdated software/system and automated attacks by malicious bots. Apart from detection of different types of attacks, a well implemented Honeypot system can also be used to detect lateral movement attacks i.e. Privilege escalation attacks and their possible causes. The logic of identifying different Privilege escalation attacks revolves around implementing an infrastructure with vulnerable systems and week configurations. When an attacker exploit any of these week configurations or credentials from these intentionally vulnerable systems, Honeypot can detect that an attacker has compromised one of the intentionally vulnerable systems and is in the process of lateral movement. A modern Honeypot can combine the mentioned and different other techniques such as identifying network scans, performance monitoring, Log analysis etc. to effectively analyze the behaviour of attacker and make definite decisions to either log/block the activity of an attacker.

2. LITERATURE SURVEY

Liberios Vokorokos, et.al, 2013 [1], proposed the urbane hybrid honeypot system. These systems Propagates and maintains the interaction with attackers and record all activities and perform data analysis, thus allowing improving security of computer systems. Furthermore in order to induce security authors also did managed to amalgamate passive fingerprinting technique. It also promotes the implementation of multiple Decoys (two Decoy Servers) in order to reduce the probability of missing the malicious activity on the server by changing the level of interaction.

Albert Sagala, 2015 [2], emerged with an idea of collaborative honeypot and intrusion Detection System where in the logs file from Honeypot server is passed on to the snort in order to generate the rules for Snort that acts similar to the firewall. The rules for the SNORT will be inevitably generated by the IDS using the logs provided by the honeypot tracked by the system. The rules generated are in the form of alerts for illegal activity.

Pavol Sokol, Martin Husak and Fratisek Liptak, 2015 [3], Sketched the issues related to privacy from the technical aspects pertaining to the honeypots and honeynet. The concepts like Privacy, Network Monitoring, storage Management, Inaccurate Results, discovery and fingerprinting, risk of taking over. It also covers the role and concepts of Privacy and honeypots mentioned in EU law, network and Monitoring, data retention, collected data and legal collection of data collection.

Marius Alin Lihet, Vasile Dadarlat, 2015 [4] had successfully implemented a honeypot applying Kippo honeypot suite which is an Ubuntu VPS application on to the cloud. The Author manipulated series of configuration especially SSH port to 22 instead of 2222 to deceive the attackers. Results

where promising as about 6000 unique IPs from different locations system was compromised and detected the attackers' locations. The author has also underlined the issue that arises if in case the honeypot is not installed properly.

Vishal Mehta, et.al, 2015 [5], in order to provide the prediction and AI capability to Honeypot various algorithm precisely machine learning algorithm is used for optimum prediction these algorithms are OSSEC as HIDS and SNORT for network detection system. The entire packet that have been sniffed or traced through internet is accumulated in the form of logs. These logs are analyzed using OSSEC. OSSEC uses 4 processes mainly Remoted, Analyzed, Mailed, and Executed.

Robert Koch, 2013 [6], proposed the system to tackle sophisticated attackers by applying it on a bare metal system that violates the two conditions of honeypot which are (1) Realistic and (2) Undetectable thus creating a separate bare metal honeypot extending the functionality to two levels coined as the Application Control and the Behavior Control to overcome the violations of the honeypot Author implemented the system based on the sebec System.

As we review the existing literature, we understand that not much work has been done for the blocking of any particular attack. As most of the paper is focused on how the attack can be detected and also no manual analysis has been done in order to make sure that the particular behaviour is an attack or not.

3. PROPOSED SYSTEM

The proposed system is mainly composed of four different components namely External Firewall, Honeypot VM, Knowledge Base and dedicated SOC (Security operational Centre) Team for manual log analysis. Different modules will be implemented in order to find out the most accurate results which help the administrator to take the decisions based on the logs being generated. The proposed approach consist of following modules:

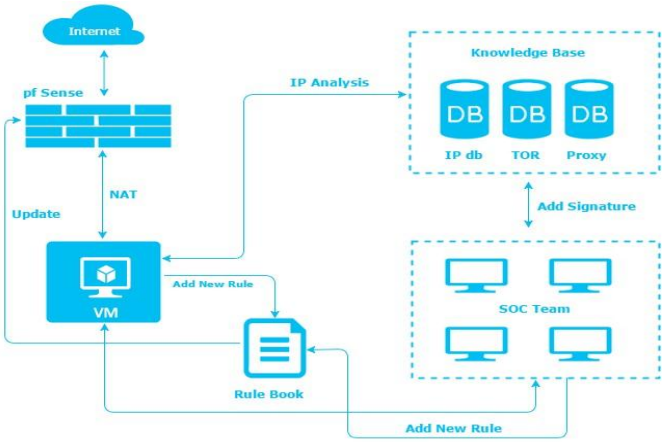

Fig -1: Proposed Architecture

Firewall, VM(Honeypot), Knowledge Database, IP Analysis, Rule Book, SOC Team (Security operational centre).

3.1 Firewall

The entire system consist of two types of firewalls i.e. Network based firewall and Host based firewall (iptables) which are responsible for handling tasks such as packet filtering, network segregation and Intrusion Prevention. The Network based firewall is used for Network Segregation separating the Honeypot, SOC and database network. It also exposes 4 common services such as SSH (22), FTP (21), HTTP (80) and MySQL(3306) to the public network which is likely to be attacked by some malicious party. The rule for Host based firewall is periodically added either by the system or from the results of manual log analysis performed by the SOC team. These rules are automatically updated by the different protocol monitors. Some standard rules are also automatically added by the system during initial setup to prevent standard Denial of service attacks.

3.2 VM (Honeypot)

The main system is basically a parent process with multiple child processes handling different tasks individually.

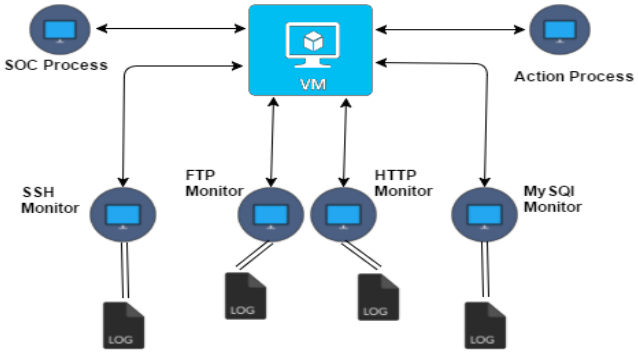

Fig -2: Internal working of Honeypot

Currently the system consists of six child processes further these processes are divided into different categories such as:

Service Log Monitor: Service log monitor are mainly responsible for parsing service log files. The data fetched from the different service logs is updated into an in-memory cache/standard data pipelines shared with parent process Currently the systems consists of four service log monitors, individually monitoring exposed services such as SSH, FTP, HTTP and MySQL.

Action Process: The Action process is managed by the parent process in order to take any action based on the malicious events submitted by the Service Log Monitors. The Action is based on severity level of the malicious events trigged for any particular IP address. The severity table consists of 3 types of actions namely Normal, Possible Attackers, Attack pattern found and blocked. In Normal phase, the system will simply allow any further traffic from that particular remote host. Normal phase also pertains that the remote host packet count does not exceeds threshold value. In second phase any remote host with the certain number of suspicious events (measured by attacks executed

in certain amount of time) fall in this category. When the system does not have any specific information about that particular IP address, notification is send to the SOC team for manual analysis of the logs that are being generated for that particular IP address. In last phase any remote host with the certain number of suspicious events fall in this category, when the system found a definite match for any attack pattern from the knowledge database. Further, the malicious hosts are being blocked from receiving any further communication.

Table -1: Action based on Severity Level

IP Address	Severity Level	Action
15.172.167.169	0	Normal
45.238.120.96	1	Possible Attacker
30.2.128.14	1	Possible Attacker
40.62.183.94	2	Attack Pattern Found and Blocked
25.159.248.88	2	Attack Pattern Found and Blocked

3.3 Knowledge Database:

Currently, the Knowledge Database is primarily composed of three different types of datasets which are Proxy, TOR and IP Database. . In Proxy database, during initialization phase, the system fetches the proxy server IP addresses over a periodic interval from the various online services and add them to the offline database. This database can be further updated by the system as a result of manual analysis performed by the SOC team. In TOR database, the system uses an API call to fetch all external nodes from the TOR circuit and updates them in TOR database periodically. In IP database, it is further divided into different datasets primarily blocked hosts, malicious signature, possible attackers, request count and status of any particular IP address.

3.4 IP Analysis Algorithm:

In this, following steps needs to be performed based on severity level to take further action.

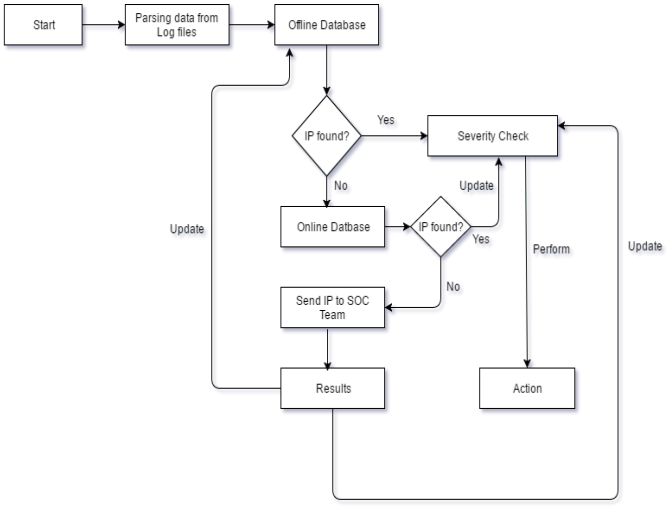

Fig -3: Flowchart of IP Analysis

Step 1 : Parse data from log files of all exposed services.

Step 2 : Fetch out IP address and look for relevant information in offline database.

Step 3 : If match found in offline database, check severity level and perform action.

Step 4 : If not found in offline database, request information from online database.

Step 5 : If match found in online database, update severity and perform action.

Step 6 : If not found in online database, send IP to the SOC team for further analysis.

Step 7 : Perform manual log analysis and update results in offline database, severity level and perform action.

3.5 Rule Book:

A rule is basically a protocol that the firewall will follow in order to suppress the malicious activities. Rule Book is a collection of both standard and customized rules that the firewall will automatically fetch over a periodic interval. Besides of standard rules that the firewall will insert during the initialization phase the SOC team can also update rules based on various scenarios.

3.6 SOC Team:

SOC (Security Operation Centre) team is a group of individuals that manually analyse the data from various sources and bring an activity or event to a conclusion in terms of severity level. The main advantage of SOC team is to follow a semi automatic approach of performing both automatic and in depth manual analysis of any malicious incident and narrow down the results with zero false positive.

4. CONSLUSION

The main aim is to create the self sufficient decentralized system to observe attacker's behaviour using semi automated approach. The proposed system overcomes all the challenges faced by the previous implementations such as minimizing the false positive by performing manual analysis. It includes logic for performing a basic behaviour analysis by monitoring different file paths and types of request within a certain periodic interval to differentiate between normal and malicious activities of end user. It also involves human interaction and data verification from various online resources to produce most accurate results.

REFERENCES

[1] Liberios Vokorokos, Peter Fanfara, Ján Radušovský and Peter Poór, " Sophisticated Honeypot mechanism-the autonomous hybrid solution for enhancing Computer system security", IEEE SAMI 2016.

[2] Albert Sagala, "Automatic SNORT IDS Rule Generation Based on Honeypot Log", ICITEE 2015.

[3] Pavol Sokol, Martin Husak, Fratisek Liptak, "Deploying Honeypot and Honeynets: Issue of Privacy ",International Conference on Availability, Reliability and Security, 2015.

[4] Marius Alin Lihet, Vasile Dadarlat, "How to build a honeypot system in the cloud", pp.190-194, IEEE, 2015.

[5] Vishal Mehta.et.al, "Threat prediction using honeypot and machine learning", pp. 278-282, ABLAZE-2015.

[6] Robert Koch, Mario Golling and Gabi Dreo, "Attracting Sophisticated Attacks to Secure Systems: A new Honeypot Architecture", IEEE Conference on Communication and Network Security, 2013.

[7] https://www.projecthoneypot.org/

BIOGRAPHIES

Rahul Koul has completed his B.E in Computer Science from University of Mumbai, India. He is currently working as Lecturer in Computer Science Department, at PCE, New Panvel, University of Mumbai. He is having 3 years of Experience in teaching. His area of interest are Networking and Information Security.

Dr. J. W. Bakal received M.Tech in Electronics Engineering, from Marathwada University. Later, He has completed his Ph.D. in the field of Computer Engineering from Bharati University, Pune. He is a PhD supervisor in CSE at University of Mumbai. He is presently working as principal at the S.S. Jondhale College of Engineering, Thane, India. He was a chairman of board of studies in Information Technology in University of Mumbai. He has publications in journals, conference proceedings, and books in his credits. He has prominently worked for IETE as a chairman, Mumbai section.

Sahil Dhar has completed his BE in Information Technology from PCE, New Panvel, University of Mumbai. He is currently working as Information Security Analyst with more than two years of hands-on experience in Application Security, Penetration Testing, Vulnerability Assessments and Server Config Reviews. He has also been acknowledged and rewarded by various organizations like Google, Apple, Microsoft, Adobe, Barracuda, Pinterest, Symantec, Oracle etc for finding vulnerabilities in their online services.