KEMENTERIAN PENDIDIKAN TINGGI

JOJAPS

eISSN 2504-8457

POLITEKNIK MALAYSIA PORT DICKSON

Journal Online Jaringan COT POLIPD (JOJAPS)

Network Defender with Fake Server: A New Way for Network Protection

Mohd Tamizan Abu Bakar[1], Mariati bt Mad Samad[1] & Akhyari Nasir[1]

[1]*Faculty of Computer, Media & Technology, TATI University College, Jalan Panchor, Teluk Kalong, 24000 Kemaman, Terengganu.*

Abstract

Network Defender as an advance security system is another way to be guard for network connection or system. The main thing to strain is the security of the network itself. In this project, as to maintain the security, Honeynet will be used to act as the administrator to protect the network system. In the architecture of the Honeypot, Honeywall CDROM and Sebek will be used as two different tools. Honeywall CDROM is more controlling data. It controls the attacker's activity by limiting what can happen inbound and outbound. Furthermore, Sebek is major in capturing data. As with data control, it is to capture the entire attacker's activity without them realizing they are within a Honeynet. With the combination of two tools with advance features, it will give lots of benefits in a way to secure the connection. In addition, this system also can give lots of information of the attackers that try to attack the network and it is depends on how the administrator will handle with it. In this cyber world, even for a small company, security is the most important.

Key-word: - Network, Network Security, Information Security , Network Defender, Network Protection.

1. Introduction

A honeypot is closely monitored computing resource that wants to be probed, attacked, or compromised. More precisely, a honeypot is "an information system resource whose value lies in unauthorized or illicit use of that resource". The value of a honeypot is weighed by the information that can be obtained from it. Monitoring the data that enters and leaves a honeypot lets us gather information that is not available to Network Intrution Detection System (NIDS). For example, we can log the keystrokes of an interactive session even if encryption is used to protect the network traffic. To detect malicious behavior, NIDS requires signatures of known attacks and often fail to detect compromises that were unknown at the time it was deployed. On the other hand, honeypots can detect vulnerabilities that are not yet understood. For example, we can detect compromise by observing network traffic leaving the honeypot, even if the means of the exploit has never been seen before.

A honeynet creates a fishbowl environment that allows attackers to interact with the system while giving the operator the ability to capture all of their activity. This fishbowl also controls the attackers' actions, mitigating the risk of them damaging any nonhoneypot systems. One key element to a honeynet deployment is called the Honeywall, a layer 2 bridging device that separates the honeynet from the rest of the network. This device mitigates risk through data control and captures data for analysis. Tools on Honeywall allow for analysis of an attacker's activities. Any inbound or outbound traffic to the honeypots must pass through the Honeywall. Information is captured using a variety of methods, including passive network sniffer, IDS alerts, firewall logs, and the kernel module known Sebek. The attacker's activities are controlled at the network level, with all outbound connections filtered through both an intrusion prevention system and a connection limiter.

There are two (2) Problem Statements in this research project:

i) Intrusion Detection System (IDS) will not detect all types of attack. It detect based on rules that tools have.

ii) DMZ or server always being the target for attacker to attack as there has lots of information for each organization.

The main objectives for this project are:

i) To lure the attacker from attack the real server

ii) To gather information of attacker

iii) To learn where the systems has weakness

This project is about to collect the information of attacker and lure the attacker to attack the fake server. Below is the scope from the tools that have in the system:

i) Sebek
Allows administrators to collect activities such as keystrokes on the system, even in encryption environments

ii) Snort_inline
Combine with netfilters/iptables operating as a bridging firewall to send packets to userspace for processing

iii) Rc.firewall
Act as a firewall

Other than that, this system is suitable to use at admin building which contains lots of server that may interact attacker to attack.

2. Methodology

In this project, there are many things that require in implementing the project. This project needs highly performance hardware compatible with the required software. Basically, this project requires one server and a network device for the hardware and also requires software. All required equipments must have own specification.

This project is about to collect the information of attacker and lure the attacker to attack the fake server. Below is the scope from the tools that have in the system:

i) Honeywall CDROM

- Is a CentOS-based distribution with the goal of capturing the activities of cyber threats and analyzing the captured data
- Utilizes existing Honeynet data control and data capture technologies

ii) Sebek Client

- Operates as part of the kernel itself
- Works by monitoring system call activity and recording data of interest
- The data then exported in a covert manner to the server

iii) Ubuntu

- Ubuntu is a computer operating system based on the Debian Linux distribution
- Ubuntu is composed of multiple software packeges of which the vast majority is distributed under a free software license

The development of the project is divided into eight phases. The eight phases are:

i) Feasibility study.

- Gathering data
- Make research
- Find information

ii) Order and purchase.

- Choose the suitable hardware for the project
- Choose the suitable cost that fixed with the budget

iii) Setup firewall and server.

- Setup and configure honeypots
- Complete the hardware

- Test whether it compatible or not with the operating system

iv) Configure and program system.

- Configure the honeypots with Snort
- Make sure honeypots can connect with pfSense
- Make sure Snort run smoothly in honeypots
- Test either Snort can detect in network connection or not.

v) Internal network testing.

- Testing the system whether it can achieve the objective or not
- Find a solution if there have any problem with the project

vi) External network testing.

- Testing with someone being an attacker and try to make the network connection failed
- Testing by using high traffic through the network connection

vii) Documentation.

- Compile all the report and make a final documentation

In every phase, there are many tasks and the contents that have to be implemented. During the construction of this project, a very precise and prudent planning and scheduling have to be carried out systematically to ensure that the project can be implemented on time and to make sure it is successfully running. A specific program has been used to guide me in doing the planning and scheduling of the project. A clear Gantt chart has been produced to indicate the list of tasks to be performed, the time scale allowed for the tasks and task bars for a better visualization of the project phases. This Microsoft project has been used to:

- Produce a scheduling – time frame.
- Remind the following job tasks.
- Guide the construction of the project.
- Trace the progress of job task.
- Ensure the every single job must be done.

As seen in Diagram 1, the processes of Network Defender were included all tools above.

Diagram 1: Flow chart for Network Defender

Diagram 2 and 3 shows the view of Network Defender generally and internally.

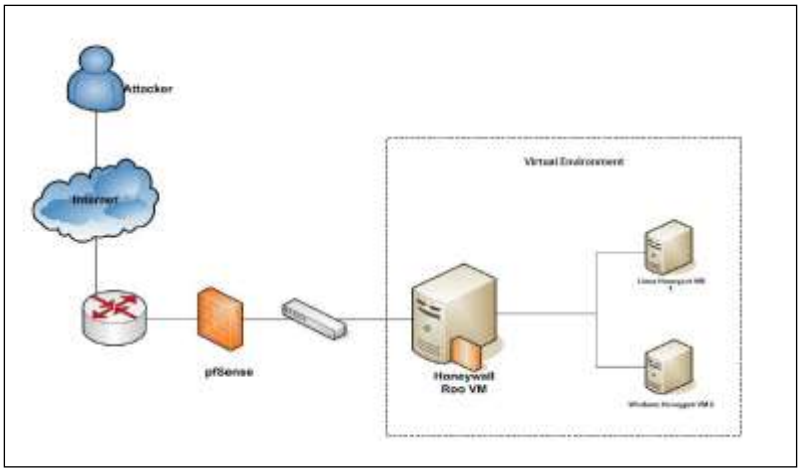

Diagram 2: Logical view of Network Defender generally

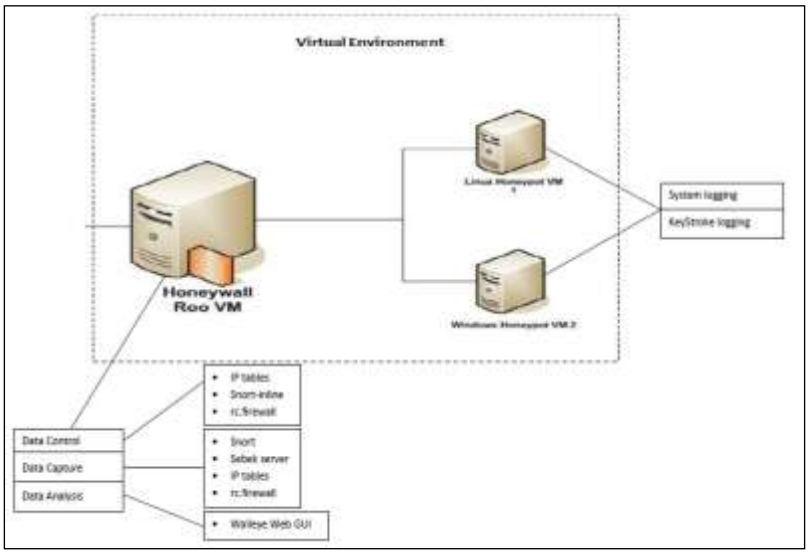

Diagram 3: Logical view of Network Defender internally

3. Result, Discussion and Recommendation

This paper proposed new network security models that have several main objectives are:

i) To lure the attacker from attack the real server
ii) To gather information of attacker
iii) To learn where the systems has weakness

This project objective is about to collect the information of attacker and lure the attacker to attack the fake server. Below are the problems that can be solve using tools that have in the system:

i) Intrusion Detection System (IDS) will not detect all types of attack. It detect based on rules that tools have.
ii) DMZ or server always being the target for attacker to attack as there has lots of information for each organization.

For the project recommendation, there are a lot of things can be enhanced to produce better system tool to secure the network. Our recommendations are:

i) Integrate with Metasploit
When there have Metasploit integration, the system can fight back with the attacker, so the attacker will not getting any chance to get through access to the real server to get the information. Other than that, it also helps to secure the system if the administrator did not know how to control the attacker if the attacker being more aggressive

ii) Using Tar Pits
To delude clients so that unauthorized or illicit use a fake's service might be logged and slowed down. Switch to a window size of zero so can prohibits the attacker from sending any more data

4. Conclusion

In this paper, we introduce the new way of network protection with the main objective to achieve is implementing the honeypots to secure the network that use to develop an Advance Security System. This system is useful for prevent the actual server and lure the attacker to attack the fake server. By doing this, the administration will notify what the attacker will do and the level of weakness of the network itself. This is another ways to help in securing the network. By doing this system, we hope that this will help lots on securing the network. As in future, there is still lots thing can be done with this project to make it more interesting. As we proposed in this paper is only for detection and luring, in future, they can make such as fight back for the attacker and auto block the attacker. Other than that, this system is suitable to use at admin building which contains lots of server that may interact attacker to attack. Hopefully, this advance security system will expand the features of securing the network in future.

References

Ahmad Shuja, F. (2012), Virtual Honeynet: Deploying Honeywall using VMware, Pakistan Honeynet Project.
Gonzalez, D. (2012), Installing a Virtual Honeywall using VMWare, Spanish Honeynet Project.
Rmcmillen, (2012), Builing and Installing Sebek Client in Ubuntu.
Siles, R (2010), Sebek 3: Tracking the Attackers, Part Two.
Patel, A., Qassim, Q & Wills, C. (2010), A survey of intrusion detection and prevention systems, Information Management & Computer Security Journal.
Awodele, O., Idowu, S., Anjorin, O. & Joshua, V. J. (2009), A Multi-Layered Approach to the Design of Intelligent Intrusion Detection and Prevention System (IIDPS), Babcock University.
Shibli, M.A. & Muftic, S. (2008), Intrusion Detection and Prevention System using Secure Mobile Agents, IEEE International Conference on Security & Cryptography (2008).
SANS Institute (2008), Host Intrusion Prevention Systems and Beyond.
SANS Institute (2008), Intrusion Detection and Prevention In-sourced or Out-sourced.
Guimaraes, M. & Murray, M. (2008), Overview of Intrusion Detection and Intrusion Prevention, Information security curriculum development Conference by ACM (2008).
Provos, N. & Holz, T. (2007), Virtual Honeypots: From Botnet Tracking to Intrusion Detection, Addison Wesley Professional.
The Honeynet Project , (2003), Know Your Enemy: Sebek, A Kernel Based Data Capture Tool.
Spitzner, L. (2002), Honeypots: Tracking Hackers, Addison Wesley.