Effective of Unicast And Multicast IP Address Attack Over Intrusion Detection System with Honeypot

Auttapon Pomsathit

Faculty of Science and Technology.
Suansunandha Rajabhat University
Bangkok, Thailand
e-mail : auttapon.po@ssru.ac.th

Abstract This research presents an intrusion detection system (IDS) with honeypot over distributed networks. The main objective is compare measuring the effectiveness of attacks between IDS and IDS with honeypot by unicast IP address attack and multicast IP address attack. These attack forms generating by NESSUS is a attack program via wire network and wireless network consists of Snort is a program that is used to detect intrusion and Honeyd to simulate a honeypot computer, which is installed on the system practical for Linux with a number of more 2 points (Sensor) to detect each program will be sent to the primary database for the analysis of experimental results. From this project will allow administrators to monitor and protect their networks more efficient organization.

Keywords: Snort, IDS, Honeypot

I. INTRODUCTION

Intrusion Detection System, IDS is another kind of the tool used for security system of computer network. IDS detects intruder which trying to intrude the computer system. IDS is divided into two types, Host-Based IDS and Network-Based.

1) Host-Based IDS

Host-Based IDS is the software working on host. IDS ordinarily analyzes the log to find detail of the intrusion. For example, IDS ordinarily detects event logs such as system, application and security for Windows. IDS will read the new event in the log and compare to the rules as they are set before. If it matches to the rules, IDS will alert. This action needs event log data which record all important events of the log file system. Unless there is no record in event log, IDS will not be used to analyze data that have been intruded.

2) Network-Based IDS

Network-Based IDS is the special software working on the individual computer. This type of IDS uses Network Interface Card to work in promiscuous mode. As of this mode, Network Interface Card (NIC) will send every packet which run on the computer network to application process. NIC which working in ordinary mode will receive only packets that has the IP address same as

destination computer. After packets were sent to IDS application, they will be analyzed and compare with the rules. IDS will alert when the match data is found.

Figure 1 : Design Structure of Main System in IDS

IDS with Honeypots can be classified based on their deployment and based on their level of involvement. Based on the deployment, honeypots may be classified as

1) Production honeypots are designed primarily for network security and defense. They have not been designed to collect information on hacking activities

2) Research honeypots are made specifically for collecting information about attackers and malicious software. They are usually managed by educational institutions or non-profit research organizations and are used to gain more insight on internet "black hat" operations, strategies and motives. The ultimate purpose is to identify threats and find ways of dealing with them more effectively.

In this research using Honeyd, they are a type of daemon honeypot licensed by GPL that has the ability to simulate a big network while using only a single host. To outsiders, the Honeyd looks like a computer network on a network's unused address space.

II. DESIGN AND INSTALLATION

Program designing of main intrusion system is objected to detect network intrusion effectively and better than detecting by only Snort Sensor. As shown in figure 1.

According to Main System in the design of Intrusion Detection System (IDS) as figure 1, the system will work by Linux system. This system consists of two components, IDS and Database.

1) Intrusion Detection System (IDS) : This component works by Snort which operating under Open Source Linux Operating System. Snort Program consists of important files. These files need configuration to be suitable for the test which is Snort.conf. The rules can be edited as the study above which is Snort Rule.

2) Database : The system for database has been used is MySQL. This perfectly support with Linux Fedora OS and Snort. MySQL Database has the phpMyAdmin program to manage the database system to work more effective.

3) Honeypot : Honeypot require adjust honeyd.conf to customize it, they decide whether to make a mock-up as any kind of Windows-based operating system version that is available to the config file. To make a machine that acts as a mock-up something like Web Server, Mail Server and FTP Server.

4) Install the equipment in the lab as a network diagram in Figure 2. and scanning network to run the test.

4.1) Network Accessories Setting

- Switch Accessories Setting

Set the Switch configuration by Cisco Catalyst 2950 series which has Spanning Port, Switch will send packages from one port to the others.

- Router Accessories Setting

Set the Router configuration by Cisco 2600 series. Set the Router to reach DHCP Pool and Router RIP property.

III. EXPERIMENTAL RESULT

Efficiency Experiments of Intrusion Detection System and Intrusion Detection with Honeyd show results of intrusion through

computer network as shown in three types of attack graphs which are TCP, UDP and ICMP. These results referred to the test of Intrusion through computer network by NESSUS are divided into these following processions.

1) Design the intrusion through the victim in the form of Unicast IP Address by setting network system and setting tool as shown in figure 2. According to the result of mainly scanning protocol TCP, most of intruders scan target, computer network system, to find weakness of the vulnerability. This procession results will be divided by forms of intrusion and protocol. The analysis will be divided by each protocol. According to the analysis of the results, only the results from the main protocol used to send the important data and intrude the computer network system. Intrusion detection of Unicast IP Address by protocol TCP which is shown in figure 3. These intrusion detections by protocol TCP show the same number of detection from both using only IDS and IDS with Honeyd.

Figure 2. network diagram showing intrusion to server

Figure 3. TCP attack by unicast IP address

According to figure 3, the detection by protocol TCP shows that the IDS with Honeypot can detect intrusion nearly the detection by IDS only.

Figure 4. UDP attack by unicast IP address

According to figure 4, the intrusion detection by protocol UDP shows average of the results which IDS with Honeypot can detect the intrusion nearly the detection by IDS only.

Figure 5. ICMP attack by unicast IP address

According to figure 5, the intrusion detection by protocol ICMP shows average of the results which IDS with Honeypot can detect the intrusion more than the detection by IDS only average 9.97 %.

According to the analysis result of intrusion by Unicast IP Address shown on the graphs, the protocol TCP and UDP will show the nearly number of detected Packets because of the ability of NESSUS which is mainly to scan protocol TCP

and it only attack through the server. According to the graph of protocol ICMP, IDS with Honeypot can detect Packets more than the detection by IDS only

2) Design to attack the Multicast IP Address. According to detection analysis, only the protocol which used to send the important data and mainly used to attack as this following.

Figure 6. TCP attack by Multicast IP address

The detection result by protocol TCP as shown in figure 6 shows that IDS with Honeypot can detect the intrusion more than the detection by IDS only average 24.15 %

Figure 7. UDP attack by Multicast IP address

According to figure 7, the detection of protocol UDP shows that IDS with Honeypot can detect the intrusion more than the detection by IDS only average about 90.91%

Figure 8. ICMP attack by Multicast IP address

According to figure 8, the detection of protocol ICMP shows that IDS with Honeypot can detect the intrusion more than the detection by IDS only nearly UDP attack about 84.31%

The analysis result of attacking through Network (Multicast IP Address), the protocol TCP, UDP and ICMP can detect Packets by IDS with Honeypot more than the detection by IDS only

III. CONCLUSION

The results of experimental measurements of the entire database from various attacks. Table 1 can be seen that the attack on the 3 pattern (TCP, UDP and ICMP) of Unicast IP Address at the Snort Sensor is placed in Broadcast Domain with Server IDS sensor and Honeypot can detect intrusion even worse than Multicast IP Address attacks.

Table I. compares the average percentage of detection Packets between the intrusion detection system that works with Honey and intrusion detection systems alone.

	TCP attack	UDP attack	ICMP attack
Unicast IP Address	4.21	5.25	9.97
Multicast IP Address	24.15	90.91	84.31

Reference

- [1] Chunfu Jia and Deqiang Chen, "Performance Evaluation of a Collaborative Intrusion Detection System", IEEE, 2009, pp. 409-413.
- [2] Jianxiao Liu and Lijuan Li, "A Distributed Intrusion Detection System Based on Agents", IEEE, 2008, pp. 553-557
- [3] Krawetz, N.(2004). Anti-honeypot technology .IEEE Security & Privacy, pp.76 - 79.
- [4] Liu Jianxia and Li Lijuan, "Research of Distributed Intrusion Detection System Model Based on Mobile Agent", IEEE, 2009, pp. 53-57.
- [5] Wang Hairui and Wang Hua, "Research and Design of Multi-agent Based Intrusion Detection System on Wireless Network", IEEE, 2008, pp. 444 – 447.
- [6] Wira, Z. A. Z., Ahmad, S. R. and Aziz, N. A.(2008). Deploying virtual honeypots on virtual machine monitor. International Symposium on Information Technology,(ITSim), pp. 1-5.
- [7] Yu-Xin Din, Min Xiao and Ai-Wu Liu, "Research and implementation on snort-based hybrid intrusion detection system", IEEE, 2009, pp.1414-1418.