IJID International Journal on Informatics for Development, *e-ISSN :2549-7448*
Vol. 2, No. 1, 2013

Honeypot Log Analysis as a Network Security Support

Tri Widodo, Elvanisa Ayu Muhsina, Bambang Sugiantoro
Informatics Department
Faculty of Science and Technology, State Islamic University (UIN) Sunan Kalijaga
Yogyakarta, Indonesia
bambang.sugiantoro@uin-suka.ac.id

***Abstract*—The development of information and communication technology could not be separated from the development of computer network and interconnected network (internet). On the other side, there are people who try to access the information illegally, even try to disturb and destroy the flow of information. These people are called hacker or cracker. Because of that reason, it is needed tools to prevent this information. Those tools are like firewall, IPS (Intrusion prevention system), IDS (intrusion detection system), anti-virus, and other tools. This research does literature review by analyzing one of IDS tools that is honeypot using a method of data analyzing using secondary data from Honey net Project Research at January 7th until 29th 2003. The result published by those researchers is a DDOS attack was happen at January 18th and 19th 2003 that caused one of the computer servers with IP (internet protocol) 10.1.1.101 went down at January 19th 2003. A computer with IP 10.1.1.101 at January 18th 2003 started to get over packets, that is 293 packet or 41.1% from 707 packets, but the computer had not gone down yet. However, at January 19th 2003 the computer got more packets, that was 795 packets or 58% from 1,370 packets, that cause the computer became down. The evidence was unconnected computers at January 20th 2003. Based on these analyzing we concludes that honeypot is very effective to be a supporting tool to detect a network intrusion, especially DDOS. And the addition value of honeypot implementation is a log which gives information for network administrators to know any activities on the network, both normal activities, or disadvantage activities.**

Keywords-Internet; hacker; DDOS; IDS; honeypot.

I. INTRODUCTION

A. Background

Information technology, especially internet, has rapidly developed. Many companies use facilities on the internet for promotional and accelerate the flow of information. In addition, companies have also implemented local area networks or local computer networks to facilitate data sharing, printer sharing, sending and receiving e-mails, promotion through websites and information sharing. Beside the development of information technology and the internet, also developed techniques or capabilities of cybercriminals (black hat) to steal data, deface, and other illegal activities. To protect computer networks and data, a company must have a strong fortress, both with firewalls and other security programs. Without adequate security, the important or confidential data from the company could be easily stolen by irresponsible parties.

Generally, network security software is relatively expensive, therefore only big companies could buy software licenses, while small and medium-sized companies could not afford to implement the network security software.

B. Purpose

This study aims to analyze the advantages and disadvantages of honeypot, especially in detecting DDOS attacks, so it could be concluded whether honeypot is effective when applied as a tool to support computer network security, especially to detect and recognize DDOS attacks.

II. STUDY LITERATURE

A. Study Literature

Research or books related to network security handling using honeypot is not easy to find, especially in Indonesia. We only founded two books that discuss honeypot, first is Trapping Hackers Tricks with Honeypots [1], second is Know Your Enemy, Learning About Security Threats [2]. From those two books, researchers are still very difficult in understanding and applying honeypot in a computer network. In fact, in the second book, it turns out that honeypot and honey net are very different, if honeypot is a system, then honey net is a network created specifically for hackers. Indeed there are similarities in the goal, but technically it will be very different [3].

Founded many references and articles that contained research and theories related to honeypot, such as research from The Honeypot Project (www.honeynet.org), articles from Bernadski and Branson [4]. Bernadski explored thoroughly from discussion of network security, honeypot and analysis of various hacker attacks.

B. Theory

1) DOS (Denial Of Services)

According to [5], DOS attacks are simply malicious acts to deny access to a system, network, application, or information to a legitimate user. DOS attacks can take many forms and can be launched from single systems or from multiple systems [5].

2) DDOS (Distributed Denial Of Services)

According to [5], DDOS are simply DOS attacks that originate from a large number of systems [5]. The attack aims to spend resources on a computer network equipment so that computer network services become disturbed.

Figure 1 shows differences among DOS, DDOS, and DRDOS attacks. On DOS attacks, an attacker only sends packets from one or two computers, whereas with DDOS, an attacker tries to attack by sending packets simultaneously from various computers even hundreds while trying to divert attention by using zombie computers (computers that have been infected by Trojans) to attack. The DRDOS (Distributed with Reflective DOS) attack is an indirect DDOS attack, which uses reflections or reflective computers to multiply attacks.

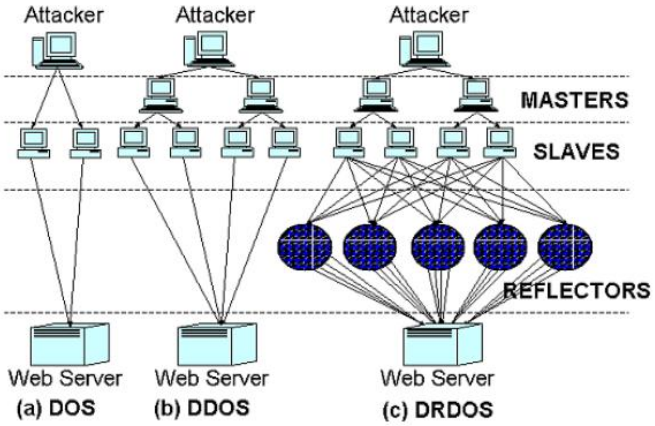

Figure 1. Illustration of DOS, DDOS, and DRDOS attack

3) Honeypot Definition

L. Spitzner's definition of the term Honeypots as cited in [3] is as follows: "A honeypot is a resource whose value is being in attacked or compromised. This means, that a honeypot is expected to get probed, attacked and potentially exploited. Honeypots do not fix anything. They provide us with additional, valuable information".

4) Placement

Honeypots do not require a specific placement on the network because it is a standard server without special needs. Honeypots can be placed anywhere like a server, but it would be better placed in an accessible place. Honeypots can be used on the internet or intranet depending on the services needed. Placement of honeypots on the intranet can be useful for detecting an attacker on an internal network. If the main focus is on the internet, honeypots can be placed in three locations:

a) in front of the firewall (internet)
b) DMZ
c) behind a firewall (internet)

Each placement has its advantages and disadvantages. Sometimes it is not possible for a server in front of a firewall [3].

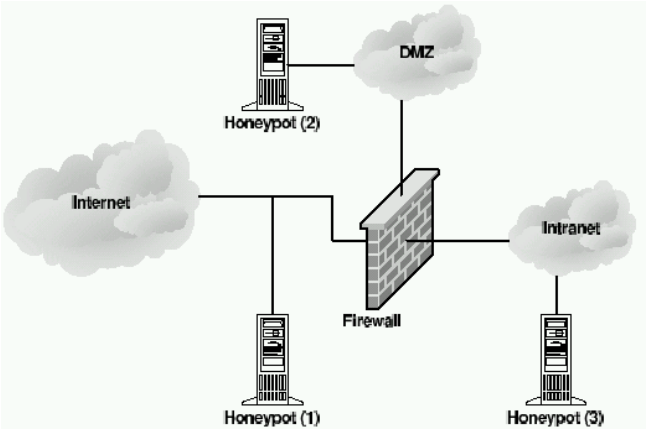

Figure 2. Honeypots Placement

By placing honeypots in front of a firewall, see Fig. 2, the risk for internal networks does not increase. The danger of compromising systems behind a firewall can be reduced. Honeypots will generate a lot of unwanted traffic like port scan or attack patterns. By placing honeypots outside the firewall, such events will not be able to break through the firewall and the internal IDS system will not display alerts.

C. Honeynet

A honey net is not a single system, but a network of honeypots systems designed to capture hackers within highly controlled and monitored networks [2]

D. Honeynet sebagai perkembangan dari honeypot

Honey net is the development of a type of honeypot with a high level of interaction (high involvement honeypot). Honey net has more value to examine what tools, tactics and methods are used by hackers when attack a network. Even honey net can be used to identify hackers [6].

III. Research Method

A. Research Objects

The object of this research is a log from the honey net demo data version 1.0 which was taken from Gen II Honey net which was conducted in January 7th , 2003 to January 29th , 2003 [2]. The results of the research published in Know Your Enemy, Learning about Security Threats in 2004.

B. Research Flow

The research method used in this study described in the following stages:

1) Study of literature

Literature study conducted to study theories related to research, therefore collected data for analysis is accurate. Theories related to this research include the concept of computer networks, layers in computer networks, network security, attacks on computer networks and honeypots.

2) Data retrieval

The data collection came from research conducted by The Honey net project in 2003. All the results of the study subsequently published in a book entitled Know Your Enemy in 2004.

3) Log analysis

After data retrieval, the author will describe, analyze and map all existing logs starting from January 7th, 2003 to January 29th, 2003 to prove as well as examine all data completely and accurately.

4) Final evaluation and conclusion

After the data analysis stage, an evaluation of various network activities carried out, and mapped any activities that include illegal activities and types of activity. Furthermore, it is concluded whether the honeypot is effectively implemented or not and what is added value obtained from the implementation of the honeypot.

IV. Result and Analysis

A. Result

It was stated in the previous heading that the data source of this study was a log from the research of The Honey net Project. This study does not examine and analyzed all existing data, but only some data as material for analysis, they are given as follows:

1) Number of source IPs

The first data is the number of source IPs; this data will be information for network administrators to measure how much data traffic is on the network. So the admin can estimate the strength of the network, whether it is capable or down. It is shown in Fig. 3.

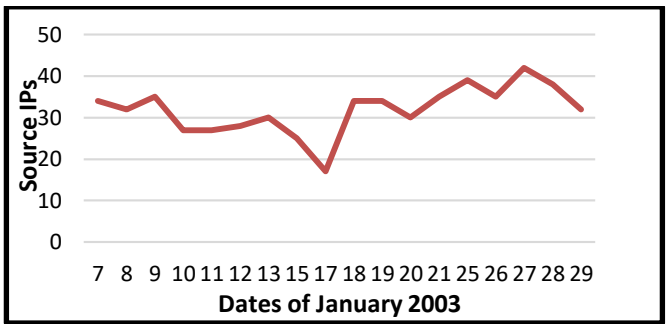

Figure 3. Number of Source IPs Chart in January 2003

2) Number of packages

The number of packages gives an overview to administrator to see various incoming and outgoing data, so it could be prepared anticipations in the form of package restrictions, or additional bandwidth. Figure 4 shows this measurement.

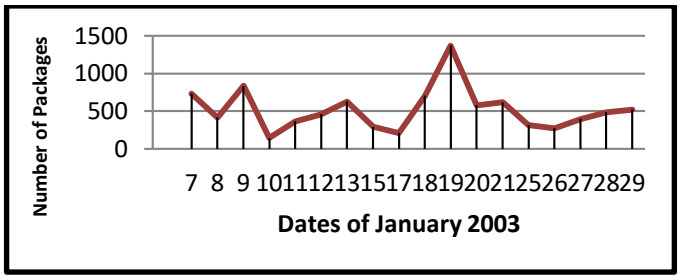

Figure 4. Number of Package Chart in January 2003

3) Protocol

The protocol will provide information of protocol type in the network that works the most, this protocol is closely related to the type of attack carried out by hackers, so administrators will be more active in preparing various types of protection on the network. It is shown in Fig. 5.

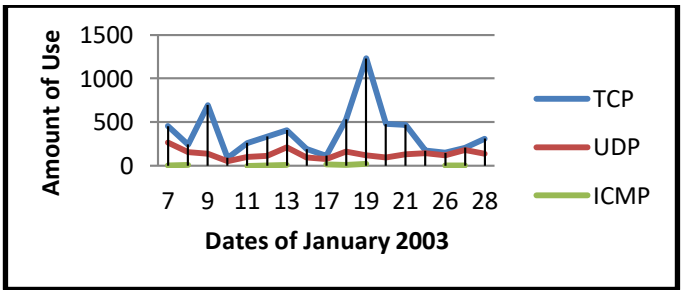

Figure 5. Protocol Chart IPs in January 2003

4) Number of Destination IPs;

The fourth data is the number of destination IPs, when the administrator knows the number of destination IPs, He will be able to detect whether the number is normal or not. When a server receives a number of packets from a very large number of IP addresses, the administrator must be vigilant and immediately check whether it is a normal activity or an attack from a hacker. Figure 6 shows this measurement.

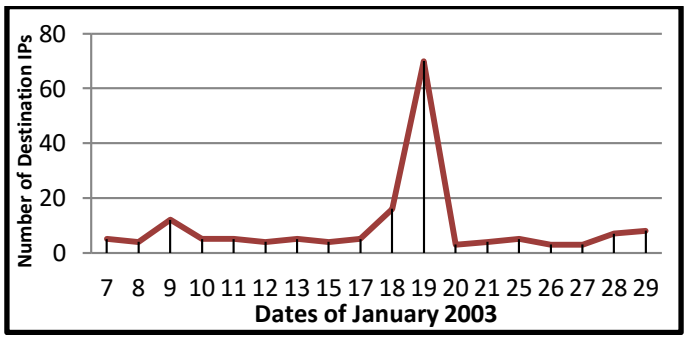

Figure 6. Number of Destination IPs in January 2003

B. Analysis

1) Main data used

This study examined and observed five data for helping the analyzing.

a) Sources IP

In the concept of DOS or DDOS attacks, could be seen that DOS/ DDOS attacks are attacks that consume target resources by constantly requesting connections or continuously sending packets. So it could be immediately suspected when there is one or several IP addresses that are constantly connecting, whether the connection from that address is a normal connection or DOS/ DDOS attack.

b) Source ports;

As in point a, in the concept of DOS/ DDOS attacks there is BOT or zombie which is a kind of computer that has been infected with a worm/ virus from a hacker, so that the computer can be controlled by hackers to attack the target. Furthermore, to control the BOT or zombie, hackers need programs such as MIRC and terminals which in carrying out their activities, the programs use certain ports, for example MIRC uses ports 6667.6668.6669. By knowing the source of the port, it can be seen what tools are used by hackers.

c) Destination ports;

Like the source port, the network administrator should also know the destination port for immediately preparing the anticipation. For example, in disrupting web traffic, hackers will flood port 80 with garbage packages. When the administrator knows there is excessive activity on port 80, the admin could immediately block the sources of existing packages, so that traffic does not jam or hang.

d) Protocols;

It should also be known what protocols are used by users, whether they use TCP or UDP. Connection oriented TCP protocol and connectionless oriented UDP will be effective to find out whether the network is being attacked by hackers or not.

e) Destination IPs.

Destination IPs also included as main data, because the IP address is part of the TCP / IP protocol, where hackers can carry out DOS / DDOS attacks towards the IP address, with the aim that the victim's computer is busy answering ACK from zombie computers. When destination IPs is only one or two but there are many sources IPs or source IP is only one but it sends packets continuously, meaning that the destination IP has been hit by a DOS or DDOS attack.

2) Log Analysis

A log is a record of the activities of a network, from the log we can find out what activities occur on a network, both legal activities and illegal activities. Examples of legal activities are accessing sites, accessing e-mails, downloading files, etc. These activities are considered legal if they run properly and not excessive. Illegal activities are activities that run without going through network authentication, or through network authentication but resulting in loss on the network, for example a computer that continuously makes requests to the server, excessive use of this bandwidth will result in slow network, even making the network down like DOS, DDOS, Flooding, email bomb attacks, etc.

After seeing, observing, and examining the results of the research, concluded that between one data and another data has a relationship. These links, if strung together, will produce a useful conclusion, especially in network security.

After analyzing the sample data from logs of the research, founded a correlation and the relationship that from these data could be determined whether there has been a DOS/ DDOS attack on a network.

V. CONCLUSION AND SUGGESTION

A. *Conclusion*

Based on the research and analysis, honeypot has various functions and benefits in supporting network security, including:

1) Honeypot can be used as an IDS, which is a tool to detect an attack on a computer network by studying the logs generated by honeypot;

2) Honeypot can be used effectively to detect DOS and DDOS attacks;

3) Honeypot has added value in supporting the security of a network by studying and analyzing recorded logs.

B. *Suggestion*

Honeypot is inseparable from its weaknesses. In order to create a safe network, when implement the honeypot pay attention to the following:

1) Network administrators in addition to implementing honeypot, should also implement other network security support tools, such as firewalls, intrusion prevention system, anti-virus, as well as other network security support tools;

2) Network administrators routinely study and analyze logs generated by honeypot;

3) Network administrators create a concept of network management policy appropriately, including limiting the number of incoming and outgoing packets and closing ports that are very vulnerable to attacks.

REFERENCES

[1] F. Utdirartatmo, *No Title*. 2005.

[2] T. H. Project, "No Title," 2004.

[3] S. Agiyanto, "Teknik Mengenali Penyerang Sistem Komputer dan Internet dengan Honeypots," *Tek. Mengenali Penyerang Sist. Komput. dan Internet dengan Honeypots*, no. ITB, Bandung, 2004.

[4] G. M. Berdnaski and J. Branson, "Information Warfare: Understanding Network Threats through Honeypot Deployment," no. Carnegie Mellon University, Pensylvania, 2004.

[5] E. Maiwald, *Network Security A Beginner's Guide*. The McGraw-Hill Companies, Inc, 2001.

[6] L. Spitzer, "Honeypots The Future." .