RISS Journal
Randwick International of Social Sciences (RISS) Journal
Vol. 2, No.1, January 2021 | Page: 124-135
ISSN Online: 2722-5674 - **ISSN Print**: 2722-5666
http://www.randwickresearch.com/index.php/rissj

Analysis and Implementation of Honeyd as a Low-Interaction Honeypot in Enhancing Security Systems

DOI: *https://doi.org/10.47175/rissj.v2i1.209*

| Abdul Muin Nasution[1,*] | Muhammad Zarlis[2] | Suherman[3] |

[1] *Master of Informatics Engineering Study Program, Faculty of Computer Science and Information Technology, Universitas Sumatera Utara, Indonesia*

[2,3] *Departement of Computer Science, Universitas Sumatera Utara, Indonesia*

[*] *muin.nasution@gmail.com*

ABSTRACT

Every computer connected to a wide computer network is vulnerable to the occurrence of data, information, resources and services that exist in the system from actions such as intrusion, wiretapping, theft and misuse of important data to damage to network systems, which are carried out by irresponsible intruders, wiretapping, theft and misuse of important data by individuals, groups, within a company/government agency or private sector, even damage to computer network systems may occur. in a company, which is done by an intruder or attacker who is not responsible. Honeypot honeyd is a method that can be applied, implemented in medium to large scale companies, especially those that have implemented computer-based systems and technology, to prevent, anticipate bad actions before they occur and take quick action when bad impacts occur. Honeypot honeyd with low-interaction, which is to interact indirectly with the attacker, because honeyd positions itself as a bait or a shadow server that is deliberately attacked so that the results of the attack can be known and analyzed. In this research, honeyd honeypot is a shadow server that resembles a real server, which has several services along with ports that are deliberately opened for attack. The results of this research can be seen that there is an infiltration or direct attack, seen from the increase in network traffic above normal on the monitor system, and also can be seen log files from Honeyd in detail what the attackers have done or are currently doing to be analyzed and then take precautions, anticipation, socialization of security in carrying out activities that are directly related to the outside world through the network, improving both servers, network systems and existing services. Thus the honeyd honeypot can help save important data, resources and can improve computer network security systems.

KEYWORDS

network security; service; honeypot; honeyd; attacker; log files; socialization of information technology

INTRODUCTION

The development of information technology on computer networks is growing fast, but along with the development of serious problems on the network such as security factors still occur. This security factor needs special attention because information is not open and not everyone can access it legally. The emergence of several CyberCrime cases in Indonesia in 2016 such as hacking of social media accounts, hacking religious sites, hacking browsing applications and hacking banking sites (Laksana, 2017). Among the ways that are done to secure a computer network system is by combining servers or involving honeypots in securing systems in a network.

A honeypot installed on a server computer can be used as a data center or information similar to a real server that can be accessed by anyone, including people who want to try to access it, because this honeypot is open and illegal so that any activity is unconsciously that the server computer has recorded all dangerous activities or activities carried out by the intruder or attacker for later analysis. (Utdirartatmo, 2015, p.7)

In this research, the authors use the Honeyd Honeypot which can be used for free and can be developed, namely by analyzing and implementing the honeypot in the virtualization system. This Honeyd Honeypot is classified as a low interaction type, which is a type designed to provide services such as servers in general, for example FTP, HTTP, telnet and other services. Based on the log files obtained from this honeyd honeypot, analysis of new and unknown intrusions or attacks can be carried out to further strengthen the network system that is actually being used, as well as changes or issuing a policy, socialization in the use of information technology if necessary.

LITERATURE REVIEW

Computer Network

A computer network is a group or several computers that are connected to each other in an internal or external scope with the aim of being able to exchange data or information. There are so many benefits that can be obtained if a computer is connected to a network as well as a network consisting of several computers connected to other networks, including the network can be used as a centralized source of information, centralized data storage, sending messages, accessing resources and being able to communicate via chat or video conferencing, so that it can make it easier for employees, company staff where and at any time to interact (Supriyadi, 2007)

Services on Computer Networks

There are many services that can assist users in exchanging data or information if a computer is connected to a small to large-scale network, which can share files, printers, databases, emails, mailing lists and browse, download and upload. While server services on computer networks meet the needs of clients in one network, including DNS, DHCP, FTP, Mail server and Web server.

Port on Computer Network

A port on a TCP/IP network is a connection from a computer that originates to do with other computers, which are contained in a computer network system. This port explains that a service provided by the server computer can be accessed by users or client computers from any area and connected to the network..

According to website of Wikipedia (2020), it is stated that the port number consists of 16-bit numbers grouped by the type of transport protocol used into TCP and UDP ports.

Table 1. List of Ports on the Computer Network

Port Number	Port Type	Keyword	Function
21	TCP, UDP	FTP	File Transfer Protocol.
22	TCP, UDP	SSH	Putty
23	TCP, UDP	telnet	Telnet
25	TCP, UDP	SMTP	Simple Mail Transfer Protocol (Mail)
53	TCP, UDP	domain	Domain Name System Server
69	TCP, UDP	TFTP	Trivial File Transer Protocol
79	TCP, UDP	finger	Finger

80	TCP, UDP	www	World Wide Web (HTTP)
92	TCP, UDP	NPP	Network Printing Protocol
93	TCP, UDP	DCP	Device Control Protocol
110	TCP, UDP	POP3	Post Office Protocol version 3 (Postoffice)
123	TCP, UDP	NTP	Network Time Protocol (ntpd ntp)
137	TCP, UDP	NetBIOS-ns	Net BIOS Name Service
138	TCP, UDP	NetBIOS-dgm	NetBIOS Datagram Service
139	TCP, UDP	NetBIOS-ssn	NetBIOS Session Service
161	TCP, UDP	SNMP	Simple Network Management Protocol
220	TCP, UDP	IMAP3	Interactive Mail Access Protocol versi 3

(Source: Wikipedia, 2020)

Network Security System

If a computer is connected to the network, it is vulnerable to unwitting threats or interference. The existence of a computer network security system is important to anticipate disturbances and threats as well as safeguard existing resources, safeguard information, maintain validity and integrity as well as guarantee the availability of services to the user/client.

By taking precautions, controlling the network security system, risks such as threats, theft of data or hardware, damage to devices, wiretapping and viruses and sniffing can be anticipated as early as possible.

.

Data and Information Security Management in Network

There are various ways to manage data so that it is completely safe from theft or misuse by unauthorized people.

- IDS (Intrusion Detection System)
  According to Onno W. Purbo (2010), IDS is an attempt to identify any intruders who try to enter a system with the intention of misusing resources without having legal rights. IDS is an application or program to detect disturbances that are detected in the system, for example Snort. IDS performs surveillance by checking and recording every incoming data packet (inbound) and outbound data packet on traffic or traffic to the network. IDS will provide direct warnings to administrators accessed through the IDS console.
- Risk Management
  A strategy or method of how to minimize the occurrence of bad things in an agency or company, namely by making or taking a risk management decision related to information activities, threats and weaknesses before or when bad impacts are detected that must be faced

Firewall

Firewall is a mechanism or system that is applied to hardware, software and on the system itself to protect, limit, filter every activity that takes place on a network involving servers, clients or network devices.

Honeypot

A honeypot is a system that is made as closely as possible to the original system and is actually fake with fake services in order to trap intruders or attackers (Nugraha, 2013). A honeypot can be said to be a distraction to an intruder or attacker who thinks that they have succeeded in retrieving data on a network, the data is fake or insignificant data (Purbo, 2008)

Honeypot can be said to be a deliberate tool to be attacked with the aim of getting as much information as possible from the actions of the attacker for this information to be learned and analyzed for every action (Raharjo, 2004)

Types of Honeypot Interactions are divided into two:

1. *Honeypot Low-Interaction*
   Honeypot In its application, low interaction honeypot uses the operating system installed on the honeypot when dealing with an attacker. The low interaction honeypot has limited interaction with the attacker. The attacks faced are usually in the form of port scanning and also digital signature attacks (R. Upadhayay, 2017).
   Interaction on low interaction honeypots with other hosts is limited so that their capabilities are limited and attackers can easily recognize them but behind the limitations of low honeypot interactions have low risks (A. Jain and DB Buksh, 2015).
2. *Honeypot High-Interaction*
   High interaction honeypot uses the original operating system to further motivate the attacker to attack the system so that the strategy and attack mode can be recorded and analyzed in more detail. Honeypot high interaction is able to process and differentiate between clean packets and packets sent by the attacker so that the packet cannot damage the original server (R. Upadhayay, 2017).

Honeyd

Honeyd is a Low-Interaction Honeypot that was created as a replacement for Nepenthes. Honeyd is made from the python scripting language. Honeyd was created to obtain duplicate data from malware actions (Ion, 2015). Honeyd's ability to detect and evaluate the payload in order to obtain a copy of the malware.

RESEARCH METHODS

Data Collection

This method is carried out so that the results and analysis of this research are more focused with accurate data. Complete data can help in the process of preparing this thesis and be more time efficient. Includes 1) Literature study by finding and studying information sources from print and electronic media. 2) Observation activities by collecting information sources accompanied by direct observation of objects.

Sistem Analysis

The security system of a network is very important so that the validity and integrity of data or information is maintained by each user. The system must be completely protected from intrusions and attacks by people who do not have the right or do not have full authority. This analysis process is indispensable for network systems, to simulate the level or toughness of security on a network, because the right analysis can identify gaps or weaknesses in network security systems. On this basis, the honeypot can be made as a choice, a fake network system is built as a test facility on an original network system that needs to be kept secure and confidential.

Analysis on a system includes:

1. Analysis of hardware requirements
   The hardware needed in this research simulation is a laptop which will be divided into a virtual box::
   - PC server honeypot with Ubuntu server 12.04 operating system

- PC intruder/attacker with Ubuntu desktop 12.04 operating system

2. Software requirements analysis
   The software used on each PC/computer in the virtual box uses an open source operating system, namely Linux Ubuntu, including tools used by intruders or attackers. The following is the software used:
   - Virtual Box (Oracle VM VirtualBox 4.2.12)
     Simulation software that runs and connects the two PCs above in a virtual LAN network and to simulate attacks by PC intruders and entrapment by PC server honeypot in a virtual machine
   - Ubuntu server 12.04
     Server operating system software used by honeypot server PCs based on CLI (Command Line Interface)
   - Ubuntu desktop 12.04
     Desktop/GUI based operating system software for clients that are used on intruders/attackers' PCs
   - Honeyd
     Honeypot software that is included in the Ubuntu server package. This honeypot turns the PC server into a PC as if it were a real server that deliberately opened several services/ports such as FTP, HTTP, telnet to lure intruders/attackers into the trap system.
   - Zenmap
     One of the software or tools that can do a lot of things like port scanning
   - LOIC (Low Orbit Ion Canon)
     Software or tools used for attacks that can paralyze a network such as a DoS attack

System Planning

This research in simulating the implementation of honeypot in a virtual machine manager (virtual box), there is a PC server and PC Intruder/attacker. The PC server or honeypot server deliberately opens several http, ftp, ssh and telnet service ports to lure to find out what the intruders are doing, then there is a PC attacker that is used to infiltrate and attack with the help of tools such as zenmap and LOIC. From the results of the infiltration/attack, a log file is obtained which contains all activities carried out by unauthorized people such as intruders for analysis by administrators.

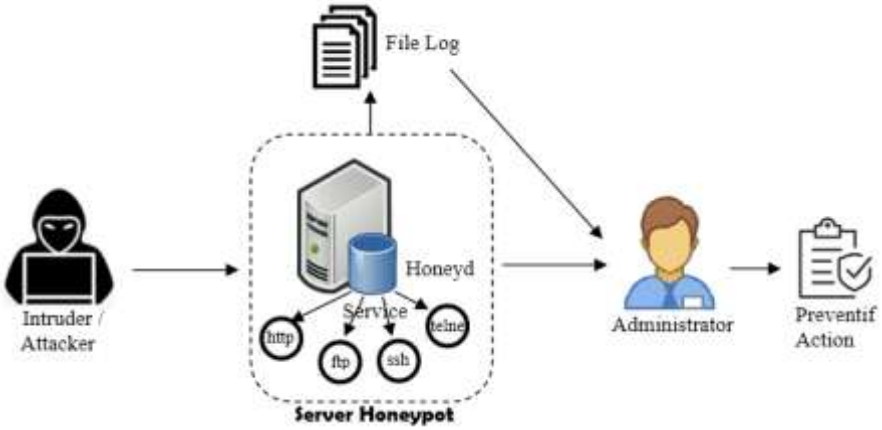

Figure 1. Simulation of implementation and analysis on a honeypot server

This design begins with installing and configuring the software which includes:

1. Oracle VM VirtualBox
2. Server Operating System in VirtualBox
   - Installation of the Honeypot Server operating system
   - Honeypot Server Configuration
     After the installation process is complete, proceed with the configuration to activate the honeyd honeypot
     > Update repository
     #apt-get update
     > Honeyd honeypot installation
     #apt-get install honeyd
     > Creating honeyd configuration file (opening service)
     #gedit honeyd.conf

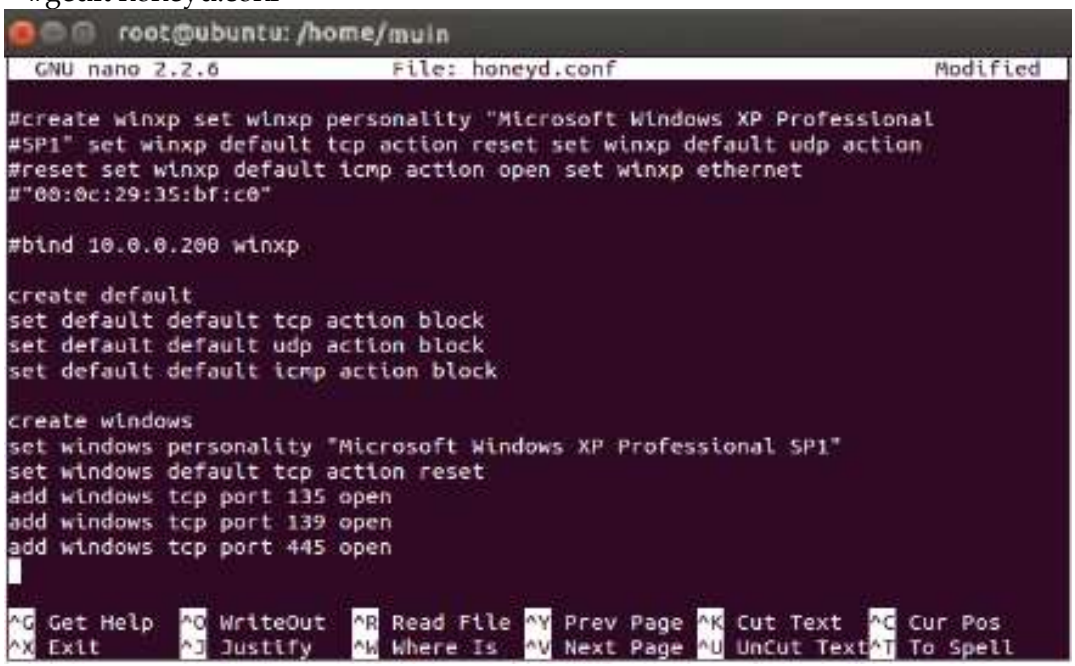

Figure 2. The process of filling in the honeyd.conf configuration

   - > Run honeyd
     #honeyd -d -f honeyd.conf

3. Operating System Attacker in VirtualBox
   After the installation process is complete, then installed tools to perform attacks such as zenmap, LOIC, filezilla

Testing Design

Simulation Testing Phase 1

The first test carried out is that the infiltration starts by detecting which ports are open on the target server, namely by running zenmap on the attacker's PC to perform port scanning, namely by determining the target of the attack.
Target IP server: 192.168.72.131

On the attacker's PC, run Zenmap then enter the IP in the target form, then click scan, or it could be the attacker to manually ping the IP address of the honeypot server computer via the command prompt (shell)
ping 192.168.72.131

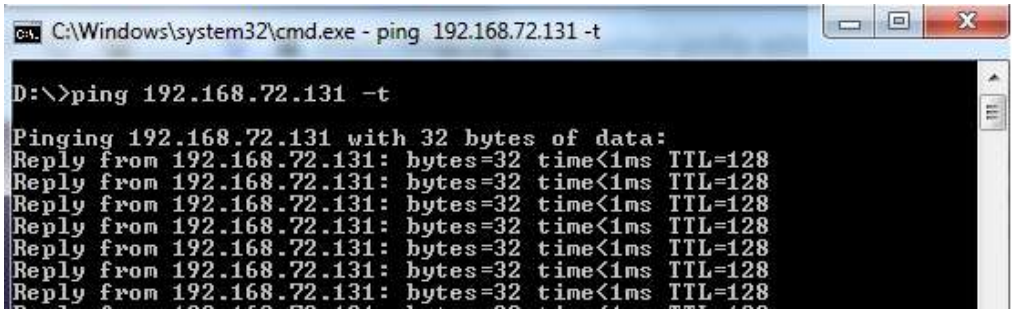

Figure 3. Ping Process to the Server IP

Simulation Testing Phase 1

This second test is a DoS (denial of service) attack, namely an attack by trying to flood the network so that traffic on the network slows down, access to server services is blocked, by entering the ping or nmap command into the target destination's ip address, for example.

Ping 192.168.72.131 –t

The LOIC tool can be used to carry out DDoS attacks, by entering the destination IP address, namely the IP server in the IP section, then determining the port and attack method such as UDP, then pressing the IMMA CHARGIN MAH LAZER button (button to start the attack). This tool can result in slow access to a destination IP that cannot even be accessed from other IPs in one network. This tool can also disable access to a web page that has a Public IP

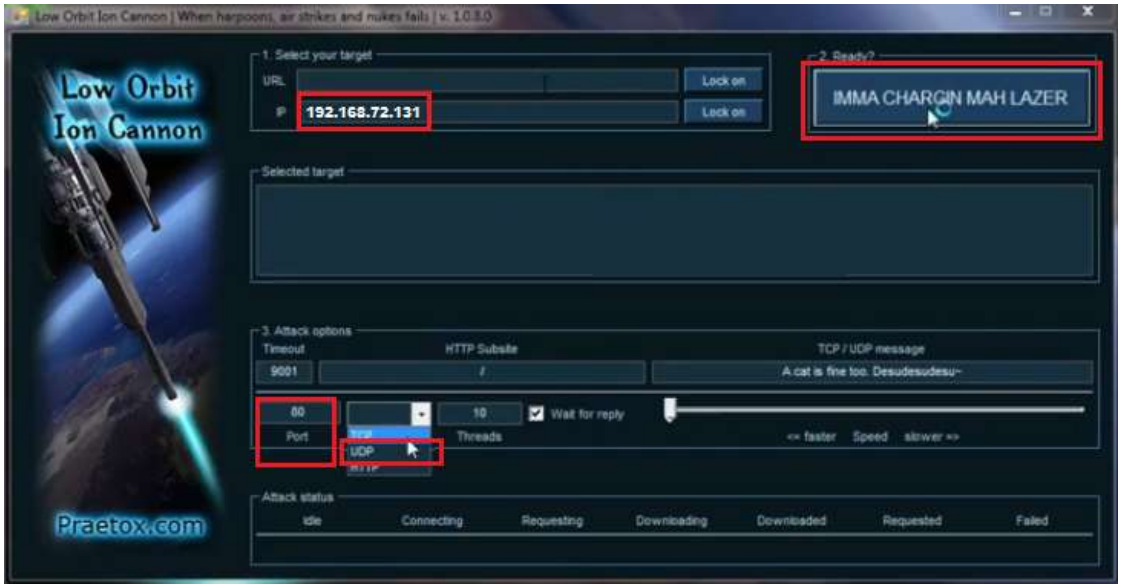

Figure 4. DDos Attack Process Using LOIC Tool

Simulation Testing Phase 3

This third test that will be done is an infiltration or attack via ftp, it can be done via the command line shell or using a browser such as Mozilla Firefox or Google Chrome.

ftp://192.168.72.131

We can also use the FileZilla tool, by entering the IP address on the host, filling in the anonymous username and password as a first step

Figure 5. The Process of Accessing the Server IP via FileZilla

RESULTS ANDA DISCUSSION

Honeyd Testing Responses

Tests have been carried out so that the results of the test are obtained such as honeyd responses to ping by attackers, honeyd responses to port scanning attempts to honeyd servers, and informing the honeyd host operating system and services that have open ports to intruders using zenmap as shown in Figure 3. the results obtained from the honeyd response

Phase 1 Testing Responses

Honeyd response to the action in the form of port scanning using zenmap which was carried out by the intruder with the IP address 192.168.72.1

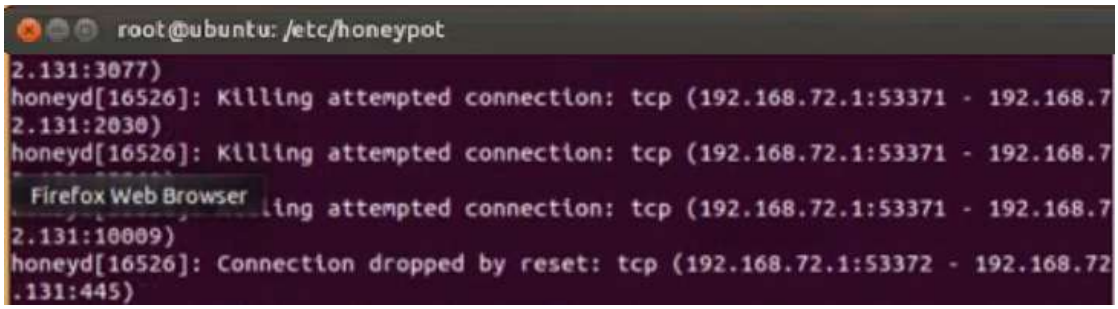

Figure 6. Monitoring or Honeyd Response to Attacker Port Scanning Using Zenmap

Whereas the following is the response or response from the honeyd server from ping on the command carried out by the attacker

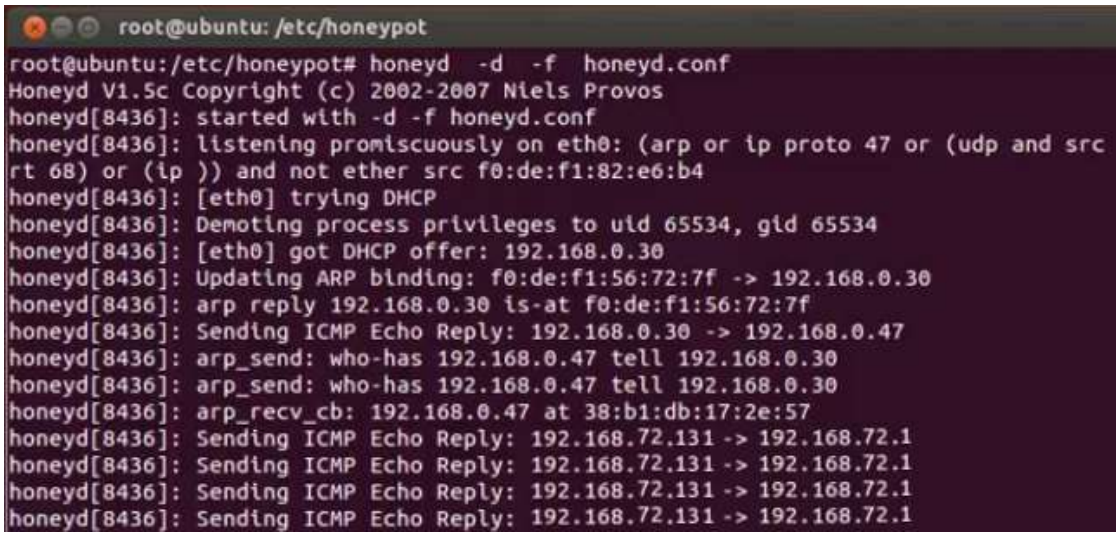

Figure 7. Honeyd Monitoring or Response to Port Scanning from Attacker using Ping Command on Command Line

Phase 2 Testing Responses

Honeyd response to actions in the form of DoS (denial of service) using the ping ipaddress command (ping 192: 168.72.131) and / or using the LOIC tool carried out by the intruder with the IP address 192.168.72.1

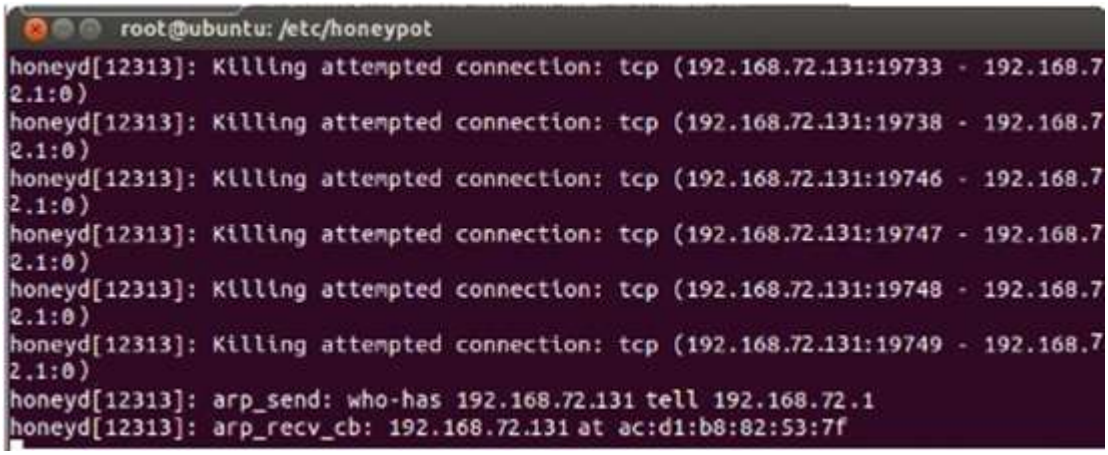

Figure 8. Monitoring or Honeyd Response to Ping from Attacker

The results of the attack carried out through the attacker's PC (192.168.72.1) prove that the attacker did not get any data which is generally indicated by packet loss. Meanwhile, from the computer side, the honeyd server will display the attacker's IP until the attack on the attacker's computer or PC stops by itself without getting anything.

Furthermore, on the honeyd server computer, observations can be made of the logs stored in the honeyd log file which contains notes or notifications of DoS attacks where previously there were three attempts to attack the honeyd server computer. The following is a table of the results of the DoS attack trial

Table 2. DoS Attack Test Results

Attack Trial	IP Address	Time (seconds)
1.	192.168.72.1	2
2,	192.168.72.1	3
3.	192.168.72.1	2
Average Time		2.33

Phase 3 Testing Responses

Honeyd's response to the action is to access FTP (File Transer Protocol), which is a buffer overflow attack aimed at obtaining shell commands. This command shell is needed by the attacker in order to have direct access to the server system and data files therein. Can be done via a browser or shell command, namely ftp: // ipaddress (ftp: // 192: 168.72.131) which is carried out by an intruder with an IP address of 192.168 .72.1

Figure 9. Honeyd's Monitoring or Response of the Attacker's FTP

The observations obtained in the honeyd log file on the FTP Attack via shell command show that based on observations of the time or average time it takes honeyd when the attack lasts, it ranges from 2 seconds from the three times the attack was tested.

Table 3. Test Results of FTP Attack

Attack Trial	IP Address	Time (seconds)
1.	192.168.72.1	1
2,	192.168.72.1	1
3.	192.168.72.1	1
Average Time		1

Honeypot Results

From the results of several tests carried out, namely port scanning, DoS and FTP attacks on the honeyd server computer IP, the honeyd log file produces notes or notifications where the IP source originates or the whereabouts of the attacker and the average time generated by Honeyd in detecting the attack occurs.

Attack Analysis Through honeyd-viz

Analysis of the attack aims to detect the test actions of the system that have been created, it can be seen by generating Honeyd-viz on the honeyd-viz web interface. The analysis, which is obtained from the honeyd log in the web interface, informs the activities or actions that the administrator can use to determine policies or provide rules in network system security. The results of this test were successfully carried out by showing reports of actions/activity attacks that have occurred in graphical form

Analysis of Attacks Through the Monitor System

On a PC honeypot server, you can also monitor the network to find out the conditions before and after or when an attack occurs through the system monitor tool. As in research, there is an increase in traffic on the monitor system when an attack occurs. Initially, the CPU load was below the average of 29.7%, 476 MB of memory in use changed to 48.9% and memory usage to 506 MB

Figure 10. Monitor System After An Attack

This monitoring system indirectly helps find out before and when an attack occurs on the PC server honeypot,

CONCLUSION

Research in the form of analysis of three phases / experiments on network security systems that have been carried out can be concluded that this study produces log files that are on the Honeyd system, which can provide detailed information on both the attacker's IP address, port and what the attacker does in the future. analyzed. Meanwhile, the monitoring system and honeyd-viz are also helpful in providing information in the form of traffic and graphic images as an overview before and during an attack.

Implementing a honeyd honeypot on a network security system can help improve security on the server, can assist administrators in analyzing, taking precautions in internal systems to making policies, socialization of the use of information technology wisely, which involves many people in a company or institution related to network system security, personal data security, company data in order to keep it properly.

REFERENCES

A. Mitchell. (2018). “An Intelligent Honeypot,” Cork Institute of Technology,

A. Jain and D. B. Buksh. (2015). “Advance Trends in Network Security with Honeypot and its Comparative Study with other Techniques,” *International Journal of Engineering Trends and Technology*, vol. 29, pp. 304–312

A.Wahyuningsi (2017). Mengenal Honeypot Sebagai Tools Untuk Menjebak Hacker. Netsec.ID, 13 Maret 2017. [Online] Available: http://netsec.id/honeypot.

Diansyah, H. P. (2014). Pengenalan IDS (Intrusion Detection System) Dan IPS (Instrusion Prevention System) Sebagai Manajemen Keamanan Informasi Dan Pengamanan Jaringan.

Ion. (2015). Visualizing Dionaea’s results with DionaeaFR. Diakses tanggal 15 Maret 2015 http://bruteforce.gr/visualizing-dionaeas-results-with-dionaeafr.html

Laksana, Dimas Danang. (2017). Implementasi Honeypot dengan Modern Honey Network, E-proceeding of Applied Science: Vol.3 No.3 December 2017, p.1815

Nugroho, Ardianto Setyo. (2013). Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan.Institut Sains & Teknologi AKPRIND: Yogyakarta.

Purbo, Onno W. (2008). Keamanan Jaringan Internet. Jakarta: PT Elex Media Komputindo.

Purbo, Onno W. (2010). Keamanan Jaringan Komputer. Handry Pratama. Jakarta

Purnomo. (2010). Membangun Virtual PC Dengan VirtualBox. Penerbit Andi: Yogyakarta.

R. Upadhayay, T. K. Mandal, S. Joshi, and M. Kala. (2017) "Data Security Using Honeypot," IJIRT, Apr. 2017.

Raharjo, Budi (2004). Teknik Mengenali Penyerang Sistem Komputer dan Internet dengan Honeypots, Modul Sistem Keamanan Lanjutan, Pasca Sarjana Teknik Elektro, ITB.

S. Gupta and V. Singhal (2011), "Honeypot a Trap for Hackers," INDIACom.

S. Z. Melese and P. S. Avadhani. (2016). "Honeypot System for Attacks on SSH Protocol," I. J. Computer Network and Information Security, Sep. 2016.

Samudra, M. I. (2016). Simulasi Kippo Honeypot Dengan Kippo-Graph Sebagai Pengumpulan Informasi Serangan Pada Jaringan.

Supriyadi, A., Gartina, D. (2007). Memilih Topologi Jaringan Dan Hardware Dalam Desain Sebuah Jaringan Komputer. Informatika Pertanian Volume 16 No. 2, 1037-1052.

Utdirartatmo, Firar (2005), Trik Menjebak Hacker Dengan Honeypot, Andi Offset, Yoyakarta

Wikipedia, (2021). Port Jaringan Komputer. Diakses pada halaman web https://id.wikipedia.org/wiki/Port_(jaringan_komputer)