International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 1, January-February 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Analysis of Honeypot Networks and Intrusion Prevention System (IPS) on Wireless Networks

Karina Asmara, M. Fakhri, Togu Harlen Lbn. Raja

Institut Bisnis Dan Komputer Indonesia, Sumatera Utara, Indonesia

ABSTRACT

Honeypot is a way to trap or ward off unauthorized use attempts in an information system. Honeypots are a distraction for hackers, so that it appears as if they have succeeded in breaking into and retrieving data from a network, even though in fact the data is not important and the location is already isolated. One type of honeypot is honeyd. Honeyd is a honeypot with a low interaction type which has less risk than the high interaction type because the interaction with the honeypot does not directly involve the actual system. Security issues are one of the important aspects of a network, especially network security on servers. This problem underlies the need to build a system that can detect threats from parties who do not have access rights (hackers), namely by building a honeypot security system. Honeypot is. The aim of implementing Honeypot and IPS is that it can be used as a tool for administrators to view activity reports produced by Honeyd and administrators can also view reports stored in logs to help determine network security policies.

KEYWORDS: *Network Security, Honeypot, Honeyd, IPS*

How to cite this paper: Karina Asmara | M. Fakhri | Togu Harlen Lbn. Raja "Analysis of Honeypot Networks and Intrusion Prevention System (IPS) on Wireless Networks" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-1, February 2024, pp.721-727, URL: www.ijtsrd.com/papers/ijtsrd63502.pdf

IJTSRD63502

1. INTRODUCTION

1.1. Background

The development of information technology in increasingly advanced computer networks still has serious problems, namely the security factor. Computer network security systems are very important in today's technological era, as is the case with wireless networks. The security of data is vital and requires extra supervision. The value of data within a particular institution or company can be very valuable if the information contained therein can result in benefits for one or several other parties (Wiyanto et al, 2014).

In this case, computer network security is divided into 2 parts, namely physical security (hardware) and non-physical security (software). These disturbances can be in the form of disturbances from within (internal) or disturbances from outside (external). Internal interference is interference that originates from within the infrastructure network. External interference is interference that originates from outside parties who want to try or deliberately want to penetrate existing security. Computers connected to the internet network are also very likely to be attacked by disturbances to the security of the network system, so it is necessary to build a system that can study the types of attacks that often occur on the network.

With the need to control access to available services. One solution is that a firewall security system is not enough to minimize attacks on a computer network. Many attacks that occur on computer networks can be discovered after strange events occur on the network. Administrators cannot know for sure what happened, so it takes quite a long time to audit the system to find problems that have occurred. In research conducted by Mustofa and Aribowo, 2013, published in the information engineering undergraduate journal at Ahmad Dahlan University, discussing the application of Honeypot and IDS security systems on wireless networks, in this journal Honeyd is a tool that is able to detect early the occurrence of intruders or detrimental activities. a network. So in theory the honeypot will not record legal traffic. So it can be seen that those interacting with the honeypot are users

who use system resources that are used illegally. So the honeypot seems to be a system that has been successfully infiltrated by the attacker. even though the attacker did not enter the real system, but entered a fake system.

1.2. Problem Formulation

From the background description given above, the problem can be formulated:

1. There is an attack from outside the network system that cannot be prevented so that it manages to enter the network system which results in the server going down.
2. Implement Honeypot and IPS to prevent attacks by detecting intruder detection and deflection.

1.3. Problem Limitations

In order for this research to be more focused and easier to understand in its discussion, the author provides problem limitations, namely as follows:

1. The attack pattern displayed is the attack pattern from the IP entering the honeypot installed on the server.
2. Honeypot development is designed using the honeyd application.

1.4. Research Objectives

The objectives of this research can be concluded as follows:

1. Understand and secure wireless networks from Intruders.
2. Understand honeypots and IPSs against new types of attacks.

1.5. Benefits of Research

The benefits that can be concluded in this research are:

1. Implement Honeypot for the server security system using honeyd.
2. Become a reference for further research and improve network security with honeypots and IPS

2. Theoretical Basis

2.1. IP Addresser.

IP addresses are used as addresses in connections between hosts on the internet so that it is a universal communication system because it is an addressing method that has been accepted throughout the world. By determining the IP address, we have provided a universal identity for every computer interface. If a computer has more than one interface (for example using two Ethernet) then we must give the computer two IP addresses for each interface (Nurwijianto, 2012).

Internet Protocol (IP) is also known as "best effort" where IP only provides a guarantee to make the best effort so that the datagram can reach its destination (Iwan Sofana, 2010). The IP protocol has five main functions, namely:

1. Defines a packet which is the smallest unit of data transmission on the internet.
2. Moving data between the Transport Layer and the Network Interface Layer.
3. Define the Internet addressing scheme or IP address.
4. Determine packet routing.
5. Perform packet fragmentation and reordering.

IP Addressing (IP Addressing) The Internet (International Network) is a "giant network" consisting of computers connected to each other. To be able to communicate with each other, each computer must have a network card. The network card has a unique identification number. For example, the network card ID number is 00:50:FC:FE:B1:E9. The ID is difficult to remember. Imagine if to communicate with other computers on a network you had to memorize each network card ID. To make this easier, the TCP/IP protocol is used on each computer. Every computer that uses this protocol must have a number called an IP address, so to connect we just need to use the computer's IP number, which of course is easier than using the network card ID number.

2.2. Network Security System

Network security systems are often currently viewed as the result of several factors. Factors related to network security vary, depending on the basic materials, but normally there are at least several things in the network security concept, including confidentiality, integrity and availability. In network security there are also computer network risks which are all forms of threats, both physical and logical, that directly or indirectly disrupt ongoing activities on the network. Risks in computer networks are caused by several factors including weaknesses in the network operating system, weaknesses in the communication network system and weaknesses in computer hardware. This security can be combined again with nonrepudiation, authenticity, possession, utility.

Network security goals can be achieved with a network security method that can protect the system both from outside and outside the network, but not only protects but must also be able to overcome network attacks. If you want to determine what you want to protect, you must have a thorough and good security plan from procedures to network security policies. Because if it is not planned it will not be as expected in network protection.

Computer network security has many branches. In security matters, considerations for securing the system must be taken into account, such as database

security, data security, computer security and information security. Information security is very important because without information almost everything cannot be done properly. Computer network security system methodology is something that is very important in computer network security issues because all elements are interrelated.

2.3. Honeypot Mechanism

A honeypot is a system or computer that is deliberately "sacrificed" to become a target for attacks by hackers. This computer serves every attack carried out by hackers in penetrating the server. This method is intended so that the administrator of the server that will be attacked can know the penetration tricks used by hackers and can anticipate how to protect the actual server. Every action taken by an intruder who tries to connect to the honeypot, the honeypot will detect and record it. A honeypot is an information system source that is usually designed to detect, trap, and attempt to penetrate the system. Generally, a honeypot consists of computers, data, and visible network segments. Honeypot also has a monitoring feature to monitor attacker activity when entering the honeypot system. Activities that can be identified include the ports attacked, commands typed by the attacker, and changes made by the attacker to the fake honeypot server. This can be used by Network Administrators as input for patching the actual system, configuring the original network segment for early prevention (Tambunan, et al, 2013).

2.4. IPS (Intrusion Prevention System)

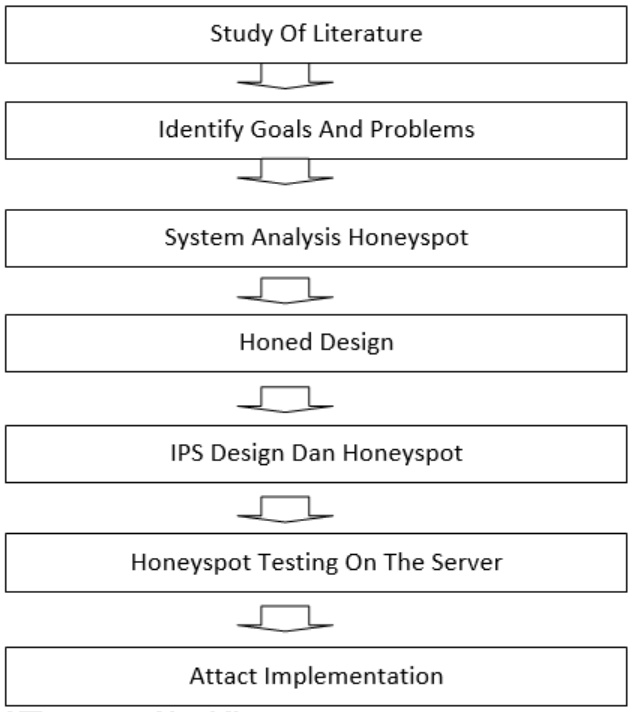
Intrusion Prevention System (IPS), is an approach that is often used to build computer security systems, IPS combines firewall techniques and Intrusion Detection System (IDS) methods very well. This technology can be used to prevent attacks from entering the local network by checking and recording all data packets and recognizing packets with sensors. When an attack has been identified, IPS will deny access (block) and record (log) all identified data packets. So IPS acts like a Firewall which will allow and block combined like IDS which can detect packets in detail. IPS uses signatures to detect traffic activity on the network and terminals, where the detection of incoming and outgoing packets (inbound-outbound) can be prevented as early as possible before they damage or gain access to the local network. So early detection and prevention are the emphasis in this IPS (Jutono, 2012).

3. Research Methods.

3.1. Research Framework

This chapter will describe the problem analysis process and analysis of the need for Honeypot implementation to improve the server security system from intruders/attackers. The following is a general overview of the steps in this research framework which is shown in Figure 3.1 below:

Figure 3.1. Framework



3.2. System Design Analysis.

In this chapter the author will discuss analysis and design in implementing the Honyepot application to improve the server security system from attack activities. The target of this analysis is how to secure a computer network from syn flood attacks. To facilitate design in securing computer networks, there are several existing mechanisms, so a flowchart of system use is needed.

The reason the author uses a system flowchart and UML is because by using a honeypot system flowchart the flow of the process of using a honeypot to secure a computer network can be clearly depicted.

3.2.1. Analysis of Honeyd Security on the Network

Analysis of the Honeyd security system on the network for network security is an open source application that can be used only on the Linux operating system. This chapter will describe the process of analyzing problems and analyzing the need for Honeypot implementation to improve the server security system using the Honeyd and Nmap applications as tools for recording. port that has been set in the honeyd. conf file. Creating a Honeyd Configuration file is used to determine the operating system as well as open ports or services provided by the Honeyd honeypot. Honeyd is configured to impersonate a trapping host with IP address 10.0.2.11. By emulating the Microsoft Windows XP

SP1 operating system,. The purpose of this configuration is to trick attackers as if there is an open server with various services (open ports). Because the attacker's stage in carrying out an attack is usually by scanning to look for the entrance or place where the attack will be carried out. An attacker through this activity tries to find security holes through which attacks can enter. From this process it can be seen that the operating system and open ports of this IPS will be built using NIPS so that the IPS system is not directly installed on the host. The following is the topology that will be used to implement a honeypot in the network.

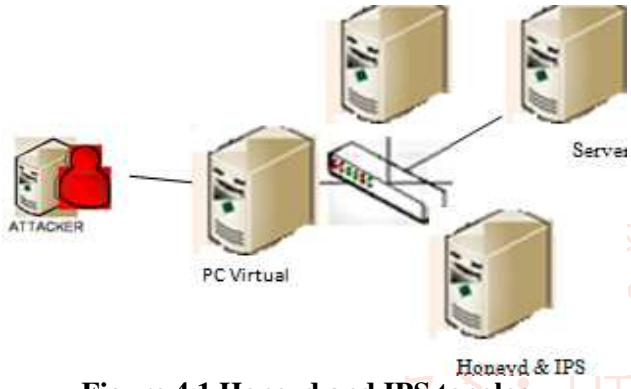


Figure 4.1 Honeyd and IPS topology

The image above is the topology that will later be built by the author in the IPS design and IP addressing honeypot carried out on the interface on the computer. Attackers will carry out attacks based on the techniques they master against existing vulnerabilities. After the installation process and creating the honeyd configuration script are complete, the next stage is to simulate the system to find out whether the system can run as expected. Honeyd runs as desired if the following conditions are met.

The IP address of the host impersonated by honeyd can be reached or accessed by other hosts on the network.

A. Scanning carried out on hosts imitated by Honeyd using Nmap produces open operating systems and ports according to the Honeyd configuration file.
B. The services that honeyd emulates can be accessed by other hosts in the network.
C. Every traffic to honeyd is recorded in the log file.

3.2.2. System Requirements Analysis (Requirements Analysis)

The requirements analysis stage aims to define the requirements of the system to be developed. In the process of analyzing the needs of the system to be developed, the author uses UML modeling to describe the existing needs of the network.

In the world of network security, many techniques or systems have been used that generally function to secure firewall networks. Firewalls are designed to bypass, stop intruders who try to enter the server network. Implementing a honeypot system using honeyd is expected to be able to secure data stored on the server by observing the attacker's activities with the logs displayed by honeyd. With the implementation of this honeypot, it can increase the security system against attack activities that occur by scanning the ports on Zenmap/Nmap. Nmap testing can be seen in the test below.

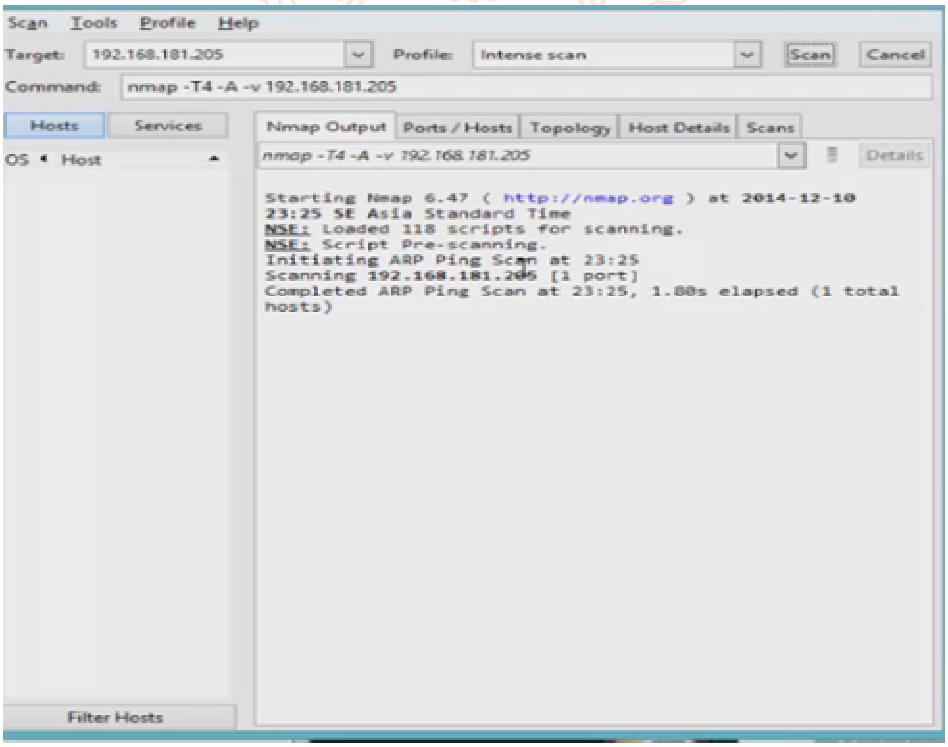


Figure 4.2 Nmap Testing

In the picture above, it is a test of Nmap in detecting activity on the network. In this activity experiment, the attack test was not carried out in the Nmap experiment above. It only checks the communication that is taking place. Using Nmap, you can also find out the port usage used. Then the next stage is

The requirements analysis stage is the stage of intensive interaction between system analysts and system users (end-users). The use of UML modeling in implementing the honeypot system is expected to be more dynamic and able to increase security on the server.

to ward off intruders/attackers who try to infiltrate the company's server network.

At this stage there is also a weakness in the running system, namely that the honeypot is not a system that can be fully used as a security system. The firewall security system implemented is not strong enough to ward off attackers who try to infiltrate existing network servers.

Based on this, a honeypot security system is needed. Development of the existing system is to create a honeypot system using the honeyd application and to be able to secure the data on the server, so that an intruder or attacker can be distracted by creating a fake server that is installed into the honeypot via a port.

3.2.3. Process Design

At this system design stage, we will explain the development of the Honeypot system using Ubuntu so that the process is easier to understand and clearer in accordance with the Flowchart and Unified Modeling Language (UML) standards that will be created.

3.2.4. Flowcharts

Flowcharts are used to clarify the development design that will be made. The following is a flowchart of developing a honeypot system for server security.

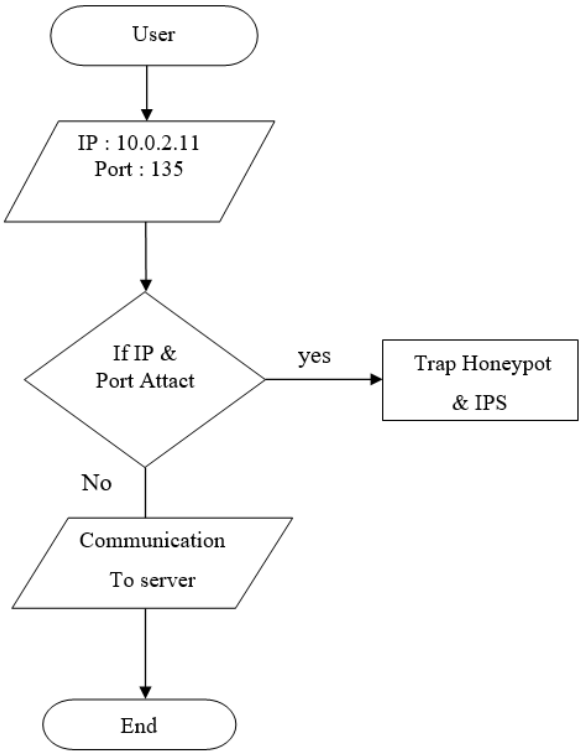


Figure 4.3 *Flowchart* Sistem

3.2.5. Use Case Diagram

Usecase Diagrams are used to textually describe the steps in system interaction with its use. There are 2 types of actors in the designed system, namely User and admin. In this case, visitors act as users and admins act as system data managers.

3.2.6. Arrange for Port Security

The port number can be specified using several methods, such as "any" for all ports, any is an arbitrary value, theoretically meaning all ports on the computer without exception.

To be more focused and maximize network security, it is indicated by a single port number, for example 80 for HTTP, 23 for TELNET and other ports. The range operator can be applied in a number of ways to convey different meanings such as

udp log any any -> 192.168.1.0/24 1:1024 udp log

the purpose and objective is traffic coming from any port and destination ports in the range 1 to 1024. Other examples such as to ensure ports less than port 1024 can be written in this way

add windows tcp port 135 open

add windows tcp port 139 open

add windows tcp port 445 open

add windows ftp port 20 open

add windows http port 80 open

So that this honeypot can run as the author wants, the author created a configuration file for port security. The aim and objective is that traffic coming from any port and destination ports in 135,139,445,20,80 can be processed by those who have user authority. Virtual operating systems are also used for virtual communication by attackers. . The port used by this researcher has been specified in the configuration file to be used as a trap for attackers. The following ports have been set in this research so that this research matches the results expected by the author.

4. Implementation and Testing

4.1. System Implementation

The implementation of the system developed will be explained in the form of test scenarios and the implementation of test scenarios for honeypot networks and Intrusion Prevention Systems (IPS) on wireless networks. It is carried out here based on the scenarios developed and this is a form of implementation. In the test, only one test scenario is carried out, and to find out the condition of the network, identify gaps in network security. In this test, a test will be carried out using the port scanning mentioned above and the test will use a type of flooding attack. In carrying out this test scenario the author will set up the honeyd application. So that later you can learn about the type of attack that will be carried out and the results will be as desired in that scenario, the author will build a fake server and a real server.

4.2. Testing Scenario Results

In the test scenario, this test was carried out to determine network conditions regarding gaps in network security. This test used Ubuntu 12.04 as a test operating system and created a trap in the Honeyd application by utilizing the configuration file above.

In this test scenario, the Zenmap tool is used as an application for port scanning and flooding. In this research, an experiment was carried out for 3 days, the experiment was carried out 4 times so that it could conclude a new type of network from before, so that honyepot could receive new types of attacks and be able to learn about the types. attacks that occur and are stored in the Ubuntu Honed Logfile folder so that later the author can classify the type of attack. As in the following table :

Tabel 5 Testing Scenario Results

User Komputer	Ip Addres	Port yang digunakan
Server asli	10.0.2.16	135, 139, 445, 1028
Server Bayangan	10.0.2.15	135, 139, 445, 1028
Client Intruder	10.0.2.18	135, 139, 445, 1028

The table above is the result of testing using online and public IPs so that Honeyd caught him attempting an attack on the original server, so the original server provided a port that had been deliberately provided and a fake IP to the intruder (attacker).

5. Conclusion and Recommendation

5.1. Conclusion

This chapter is used to provide conclusions and suggestions from research results from analyzing the Honeypot mechanism in attacker attacks. Several things can be concluded from this research as follows:

1. Improve the security system using a honeypot by redirecting intruders to the honeydew.
2. From the test results using honeypot, Honeypot is able to recognize attacks with new rules. And create a fake server for intruders.

5.2. Suggestions

Meanwhile, during the testing and implementation of the snort mechanism in dealing with flooding attacks, there are still many weaknesses, so suggestions are needed that can be developed to continue research in preventing attacks that arise. The suggestions that the author hopes to obtain from this research are:

1. Need an administrator who is proficient in Linux, for security by implementing honeypot and IPS.
2. Need to test with a large network such as a WAN.

BIBLIOGRAPHY

[1] Adelia, (2011). "*Implementasi Customer Relationship Management*"(CRM) pada Sistem Reservasi Hotel berbasisi Website dan Desktop**"**.*STMIK Yogyakart*.

[2] Dony A., (2005). "*Computer Security"*. *Yogyakarta: Penerbit Andi.*

[3] Raden S., (2015). "Pengembangan Sistem Presensi Mahasiswa".

[4] Yulius C.,(2014). "Penerapan *Virtual Private Network* Menggunakan MikrotikRouter Pada RS Immanuel Bandung".

[5] Haviluddin, (2011). "Memahami Penggunaan UML (*Unified Modelling Language*)". *UniversitasSurabaya*.

[6] Hadianastuti L., (2014). "Rancang bangun system Informasi persediaan Raw Material dan Packaging Material dengan Menggunakan Java 2 Platform Standard *Edition* (J2SE) dan Mysql 5.0.6.7 Pada PT Cedefindo".

[7] Herlambang L,.(2008). "Menguasai Router Masa Depan Menggunakan Mikrotik RouterOS". *Yogyakarta: Penerbit Andi.*

[8] Diansyah T,. (2015). "Analisa Pencegahan Aktivitas Ilegal didalam Jaringan Menggunakan *wireshark*".

[9] Mustofa M,. (2013). "Penerapan Sistem Keamanan *Honeypot* Dan IDS Pada Jaringan *Nirkabel*" (*Hotspot*). *Universitas Ahmad Dahlan.*

[10] Naisuty, (2012). "Analisa Kinerja Protokol TCP/IP dan DTN Pada Jaringan Multi Jalur".

[11] Pratama Y,. (2013). "Aplikasi Virtual LAN (VLAN) Dalam Mengatur *Bandwith* Pada Jaringan".

[12] Prasetyo U,. (2013). "Analisa dan Perancangan Sistem Informasi Parkir Di Universitas Mutiara Kudus".

[13] Setyo R,. (2013). "Membangun Aplikasi *Autogenerate* Script Ke*Flowchart* Untuk Mendukung *Business Process Reengineering*".

[14] Sugeng W,.(2015). "Jaringan Komputer Dengan TCP/IP". *Bandung: Penerbit Modula*.

[15] Sulindawati,(2010). "Pengantar Analisa Perancangan Sistem". *Jakarta: AMIKOM.*

[16] Tambunan M,.(2013). "Desain dan Implementasi *Honeypot* dengan *Fwsnort* dan PSAD sebagai *InstrusionPrevention System*".*Universitas Kristen Duta Wacana*.

[17] Taufik K,.(2013). "Pembuatan Aplikasi Anbiyapedia Ensiklopedi Muslim Anak Berbasis Web"**.** *UIN Sunan Gunung Djati Bandung*.