Analysis Of Using Firewall And Single Honeypot In Training Attack On Wireless Network

Tengku. Mohd. Diansyah\textsuperscript{1}, Ilham Faisal\textsuperscript{2}, Adidtya Perdana\textsuperscript{3}, Boni Octaviani Sembiring\textsuperscript{4}, and Tantri Hidayati Sinaga\textsuperscript{5}

\textsuperscript{1,2,3}Informatics Engineering and \textsuperscript{4,5}Information System of Sekolah Tinggi Teknik Harapan Jl. H. M. Joni No. 70 C Medan, Indonesia
dia.10.22@gmail.com

Abstract: Security issues become one of the important aspects of a network, especially a network security on the server. These problems underlie the need to build a system that can detect threats from parties who do not have access rights (hackers) that are by building a security system honeypot. A Honeypot is a diversion of intruders' attention, in order for intruders to think that it has managed to break down and retrieve data from a network, when in fact the data is not important and the location is isolated. A way to trap or deny unauthorized use of effort in an information system. One type of honeypot is honeyd. Honeyd is a low interaction honeypot that has a smaller risk compared to high interaction types because the interaction with the honeypot does not directly involve the real system. The purpose of the implementation of honeypot and firewall, firewall is used on Mikrotik. Can be used as an administrative tool to view reports of Honeyd generated activity and administrators can also view reports that are stored in the logs in order to assist in determining network security policies.

Keywords: Honeypot, low interaction, firewall, Mikrotik, wireless

1. Network Security System

Network security systems are often at the moment still seen as the result of several factors. Factors related to the safety of this network vary, depending on the basic ingredients, but normally there are at least some things in the concept of security such as securities, integrity, and availability. In network security, there is also the risk of computer networks that are all forms of threats both physical and logic that directly or indirectly disrupts the ongoing activities within the network. The Risks in computer network caused by several factors such as weakness of network operating system, weakness of network communication system and weakness of computer hardware. This security can be combined with non-repudiation, authenticity, possession, utility.
The purpose of network security can be achieved by a network security method that can protect the system both from outside and outside the network, but not only protect but also must be able to overcome network attacks. If you want to determine what you want to protect then it should have a good and sound security plan from procedures to network security policies. Because if not planned then it will not be as expected in network protection.

![Figure 1. Security Level 1](image1)

2. Honeypot mechanism

A Honeypot is a system or computer that is deliberately "sacrificed" to be the target of attacks from hackers. The computer serves every attack done by hackers in the penetration of the server. This method is intended for the administrator of the server to be attacked to know the penetration tricks that hackers do and can anticipate in protecting the real server. Any action was taken by an intruder trying to connect to the honeypot, then the honeypot will detect and record it. A Honeypot is a source of information systems that are usually designed to detect, trap, in an attempt penetration into the system. Generally, the honeypot consists of computers, data, and network segments that look Honeypot also have a monitoring feature to monitor attacker activity when Enter into the honeypot system. Known activities include ports being attacked, commands typed by attackers, and alterations by attackers on a fake server honeypot. This can be exploited by the Network Administrator as input to patch the actual system, configuring the original network segment for early prevention (Tambunan, et al, 2013). The picture of honeypot as follows.

![Figure 2. Attacker mechanism](image2)

A Honeypot is a computer system on the Internet that can manage to attract and trap people who are trying to penetrate other computer systems. A Honeypot is a server-installed forensic application specifically designed to monitor potential activities to attack and observe intruders how they get into the server computer system. (Aye Thu, 2013)
3. Honeyd

Honeyd is a type of Open Source Honeypot application written by NielProvos. Honeyd is a simple daemon that keeps virtual hosts on the network. The host can then be configured to run various services. TCPnya Personality Can run as a particular operating system, to fool scanner fingerprints like Nmap or probe. Actually honeyd powerful enough and Provides a complete feature, but the configuration is not easy because it does not have a GUI (Mustofa & Aribowo, 2013). Honeyd is a low interaction honeypot type honeypot that performs network simulation as a whole like service FTP, SSH, HTTP, router in one machine / PC and can add multiple hops, packet losses, and latency (Tambunan, et al, 2013).

4. Firewall

In the computer network is very important for network security, especially related to applications involving various interests, there will be many things that can disrupt the stability of the computer network connection, whether related to hardware (physical security, power resources) and related to software (System, configuration, access system, etc.). Disruption of the system can occur due to accidental factors performed by the manager (human error), but not least also caused by a third party. Disturbances can include destruction, infiltration, theft of access rights, misuse of data or systems, to criminal acts through computer network applications. Security of the system should be done before the system is enabled. The use of the system should be done before the actual system is enabled. Overall.

Figure 3. Firewall concept and using honeypot (Aye Thu, 2013)

Figure 4. Firewall mechanism
5. Implementation

In this test the authors will conduct trials using low orbit applications as an attack testing application attack attack, this attack testing will conduct a direct attack to the server so that in the presence of this test will go into the trap honeypot.

![Low Orbit Application](image1)

Figure 5. Low orbit application

Table 1. Honeyd implementation and firewall

| IP Address | User Computer | Operating System | Port Applied          |
|------------|---------------|-------------------|-----------------------|
| 10.0.2.16  | Real Server   | Linux Ubuntu      | 135,139,445,1028      |
| 10.0.2.15  | Server Shield Honeypot | Microsoft Windows SP1 | 135,139,445,1028 |
| 10.0.2.18  | Client Intruder | Microsoft Windows Server | 135,139,80,445,1028 |

The table is a scenario that will be tested in this honeypot test port used is port 135,139,445,1028 and windows SP 1 is acting as a shadow server used in this trial. The function of this shadow server is to perform manipulation so it is expected that the Microsoft server is hosted and active.

![Honeyd Config](image2)

Figure 6. honeyd config

The above view is the result of the use of honeydconfig is the configuration file name that has been created before, this honeypot does not run in the background, in honeypot it is automatically given information about IP DHCP, mac address of the shield already built from honeyd application.
In this test directly to attack the server, the purpose of this attack is to make the server down so it can not be accessed, after this attack will not be able to directly attack the actual server but stuck in the fake server or shield server so the server does not directly down But the attacker seems to be successful in attacking as shown below.

Display above after configuration and if port scanning successfully executed on at zenmaphoneyd will do the response from the result of scanning. In the above honeyd experiment will know the IP address that tries to communicate with the shadow host so that with the honeyd we can find the IP address of Intruder.

The attack is a type of port scanning attack so that the attacked port can be prevented following the attacker using IP 10.0.2.18 proved that honeyd is able to reduce attacks performed for the scanning port of the orbit application. Port scanning results can be seen as shown below In Implementasi test scenario using this honeyd. Is done to determine the network condition of the gap of a network security testing using ubuntu 12.04 as a trial operating system and create a trap for honeyd application by utilizing the above configuration.
Table 2. Testing online

| No. | Ip Address Scanned | Detected Address |
|-----|-------------------|------------------|
| 1   | 192.168.68.XXX    | 192.168.1.XXX    |
| 2   | 10.0.2.XXX        |                  |
| 3   | 172.192.85.XX     | 172.168.XX       |

In this test scenario using orbit tools as an application for port scanning and Flooding, in this study conducted experiments for 3 times so it can conclude new types of network than before, so that honeypot can accept new types of attacks and can learn the types of attacks that occur and stored In the folder ubuntuhoneydtmp/honeyd log file so will author can classify the type of attack.

6. Conclusion

At the time of this test the author get the conclusion that the honeypot and firewall can cooperate in restraining the incident that occurred so the attacker can’t enter easily because the attacker into the trap honeypot that has been made, so the server can work safely, and honeypot is successful in Detects suspicious activity and captures the attacker's IP and is stored in a separate folder on the server trap honeypot.

REFERENCES

[1] Adam brown, Todd Andel 2016 “What’s Is Your Honeypot?” (Universty of South Alabama), Mobile, USA
[2] Ariyus, Dony 2005. Computer Security Yogyakarta: Penerbit Andi
[3] Aye Aye Thu, 2013. “Integrated Intrusion detection and Prevention System With Honeypot on Cloud Computing Environment” (International Journal of Computer Applications) Volume 64 Number 4
[4] Gray Plant Mooty, 2014. A. Legal guide to privacy and data security.
[5] Muh Masruri Mustofa, Aribowo Eko 2013 “Penerapan system keamanan honeypot dan ids pada jaringan nirkabel (hotspot)” (Jurnal Sarjana Teknik Informatika) e-ISSN : 2338-5197 Vol 1
[6] Mohd Diansyah, Tengku 2015 “Analisa Pencegahan Aktivitas Ilegal didalam Jaringan Menggunakan Wireshark” (Journal Time) Vol 2 No 2
[7] Pidie Wiyanto, et al 2014 “Aplikasi Monitoring Keamanan Jaringan menggunakan IDS dan Router Mikrotik” (Jurnal Jarkom Institut Sains & Teknologi AKPRIND Yogyakarta) e-ISSN : 2338-6312 Vol 2 No 1
[8] Project Honey Pot, 2015. Project Honey Pot Statistic. Available at: https://www.projecthoneypot.org/statistic.php
[9] Zhan, Z., Xu, M. & Xu, S., 2013. Characterizing Honeypot-Captured Cyber Attack: Statistical Framework and Case Study. (IEEE Transactions on Information Forensics And Security), 8 (11), pp. 1775-1789.