ISSN 2356-4407

www.STIKI.ac.id

Bersama memajukan ICT Indonesia

PROCEEDING

IC - ITECHS 2014

The 1st International Conference on Information Technology and Security

Malang, November 27, 2014

Published by:

Lembaga Penelitian dan Pengabdian pada Masyarakat

Sekolah Tinggi Informatika dan Komputer Indonesia

PROCEEDING

The 1st International Conference on Information Technology and Security (IC-ITechs)

November 27, 2014

Editors & Reviewers:

Tri Y. Evelina, SE, MM Daniel
Rudiaman, S.T, M.Kom Jozua
F. Palandi, M.Kom

Layout Editor:

Eka Widya Sari

LEMBAGA PENELITIAN & PENGABDIAN KEPADA MASYARAKAT
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
Website: itechs.stiki.ac.id E-mail: itechs@stiki.ac.id

PROCEEDING

The 1st International Conference on Information Technology and Security (IC-ITechs) November 27, 2014

ISSN 2356 - 4407

viii + 276 hlm; 21 X 29,7 cm

Reviewers & Editors:

Tri Y. Evelina, SE, MM
Daniel Rudiaman, S.T, M.Kom
Jozua F. Palandi, M.Kom

Layout Editor:

Eka Widya Sari

Published by:
LEMBAGA PENELITIAN & PENGABDIAN KEPADA MASYARAKAT
Sekolah Tinggi Informatika & Komputer Indonesia (STIKI) – Malang
Jl. Raya Tidar 100 Malang 65146, Tel. +62-341 560823, Fax. +62-341 562525
Website: itechs.stiki.ac.id E-mail: itechs@stiki.ac.id

GREETINGS

Head of Committee IC-Itechs

For all delegation participants and invited guest, welcome to International Conference on Information Technology and Security (IC-Itechs) 2014 in Malang, Indonesia.

This conference is part of the framework of ICT development and security system that became one of the activities in STIKI and STTAR. this forum resulted in some references on the application of ICT. This activity is related to the movement of ICT development for Indonesia.

IC-Itechs aims to be a forum for communication between researchers, activists, system developers, industrial players and all communications ICT Indonesia and abroad.

The forum is expected to continue to be held continuously and periodically, so we hope this conference give real contribution and direct impact for ICT development.

Finally, we would like to say thanks for all participant and event organizer who involved in the held of the IC-Itechs 2014. We hope all participant and keynote speakers got benefit from this conference.

ISSN 2356 - 4407
The 1st International Conference
on Information Technology and Security

LIST OF CONTENT

Analisys Design Intrusion Prevention System (IPS) Based Suricata

Dwi Kuswanto
Universitas Trunojoyo Madura
dwikuswanto@if.trunojoyo.ac.id

Abstract

Network security is a very important thing. Technological developments have an impact on the security of the computer network with the rise of attackers. It is very threatening the existence of data on storage media from the actions of people who are not responsible. To maintain confidentiality, originality and availability of these data, we need a system to detect the presence of intruders in computer networks that can run in real time. Intrusion Prevention System (IPS) is a method that can monitor the network and can provide a particular action on a computer network. IPS is the development of IDS, which is using Suricata IPS as intruder detection is connected with IPTables as a deterrent to intruders. IPS is equipped with a display guide user interfaces for easy admin to monitor the network from intrusion action to the server using open source (Linux Ubuntu 12.04 Precise Pangolin) at a operating system. Suricata create alerts when intrusions are detected on the network and stored in log files Suricata. At the same time WebAdmin can display the alert dialog that is accompanied by an alarm signal to instruct IPTables block IP addresses identified as an intruder, so the attacker access to the server is lost. Hopefully design is done optimally capable of detecting attacks.

Key words: *IPS (Intrusion Prevention System), Suricata, IPTables*

INTRODUCTION

The need internet on a computer network is required to accelerate activity in all respects. This has an impact on the development of a global computer network. Security in computer networks is very important, especially for maintaining the validity and integrity of the data and assurance services for users. Many methods are carried out to infiltrate the network. Starting from a mere attempt to try to destroy or steal important information on the server.

To assist in the monitoring of data packets on the network and analyze packet traffic in order to prevent from things that are harmful to the network, it takes a suppression system attacks and can display / give a warning when there is an intrusion that is commonly referred to as Intrusion Prevention System or IPS. IPS itself is a system that can prevent and provide action as it happens infiltration. Based on the literature study by Bayu Wicaksono (2012) "Design and Implementation of IPS (Intrusion Prevention System) Using Web-Based Snort and IPTables" in research discussed how to both build Intrusion Prevention System using snort with accompanying web-based interface to set the IPS system. Meanwhile, according Tamsir Ariyadi (2012). "Implementation of Intrusion Prevention System (IPS) On Campus Computer Network B Universitas Bina Darma" discusses IPS on a computer network utilizing the Cisco 1700 Series Routers and Switches Catalyst 2950. The study explains that attacks or network intrusions can prevented the implementation of the Intrusion Prevention System (IPS) depending on the pattern of the attack in the IPS rule or not. Research conducted by Bahrul Ulum (2013). "Design of Network Intrusion Prevention System In the TCP / IP Using Snort and iptables" discusses the reliability of IPS in analyzing packets and issuing alerts, which carried out the test as much as 50 times more than attack the attacker 1. Results of testing can be analyzed through webmin interface.

Based on previous studies we concluded that they were using Snort as an attack detection. Suricata is one attack detection products other than snort. Suricata features multi-threaded which serves to improve the performance of Suricata. Suricata is expected to become the next generation of intrusion detection engine. Research studies of this analysis is intended to design Intrusion Prevention System (IPS) Suricata by combining IPTables based on computer networks, in which the system can prevent and monitor network computers automatically so as to reduce the threats on the computer network. IPS can be built in a Linux Precise Pangolin Ubuntu 12.04.

METHODS

Intrusion Prevention System (IPS) is a type of network security software and hardware that can monitor the activity of unwanted or intrusion and can react immediately to prevent such activity. IPS is the development of IDS. As the development of technology firewall, IPS can take control of a system based on the application of content or pattern, not only based on port or IP address such as firewalls generally. In addition to monitoring and monitoring, IPS can also take a policy to block packets that pass by way of "report" to the firewall. Rule-based detection method known as signature-based detection is a method of detection by assessing whether the transmitted data packets are dangerous or not. A packet of data will be compared to the existing list. This method can protect the system from the types of attacks that are already known in advance. Therefore, to maintain the security of computer network systems, the data existing signature must remain Replaces. Suricata is an intrusion detection system (IDS) high performance developed by a non-profitOpenInformation foundation Security Foundation (OISF). Suricata developed by OISF and its supporting vendors.

In this study Intrusion Prevention System (IPS) as a bridge between the local network server so that the server is protected by IPS. Topology Intrusion Prevention System (IPS) in this study is quite simple. Suricata IPS device installed on a computer that also functioned as a bridge to protect the server from any activity that threatens the server. Pamasangan Intrusion Prevention System (IPS) as Figure 1 is an attempt to prevent any activity that may threaten the server from another network.

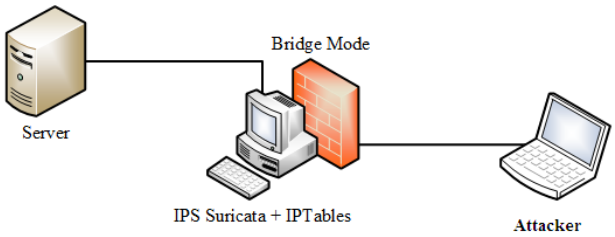

Figure 4. Design Intrusion Prevention System Based Suricata

Design Intrusion Prevention System (IPS) is constructed based on the incorporation of several components ie:

1.Suricata detection engine running in inline mode, so it can work as an examiner and packet analyzer indicated as an attack and create alerts to log file Suricata.
2.IPTables blocking or forwarding the packet on the network.
3.WebAdmin read and process the log file and stored in a MySQL database.
4.MySQL database keeps a record of events for subsequent analysis.
5. WebAdmin displays events in the form of real-time web.

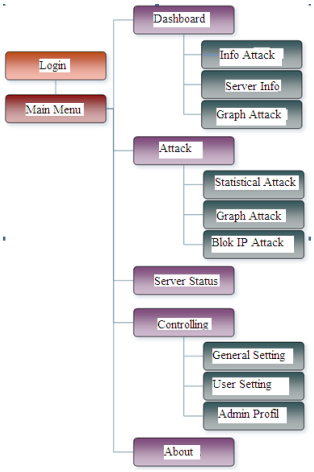

Figure 5. Design WebAdmin

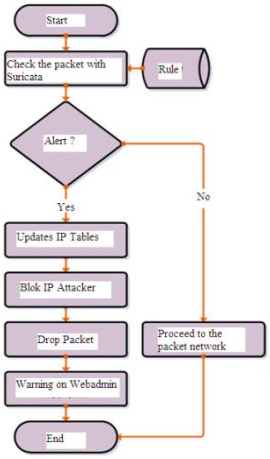

Figure 6. *Flowcart* IPS based Suricata

Flowcart above explains the workings of the system as a whole Suricata IPS. The data packet to the server to be checked beforehand by Suricata. The data packets are then matched with the rules Suricata. If the packet is indicated as an attack, then Suricata create alerts. Further update the firewall rule to block attackers IPTables then dropping the packet data. After that WebAdmin displays a warning with sound

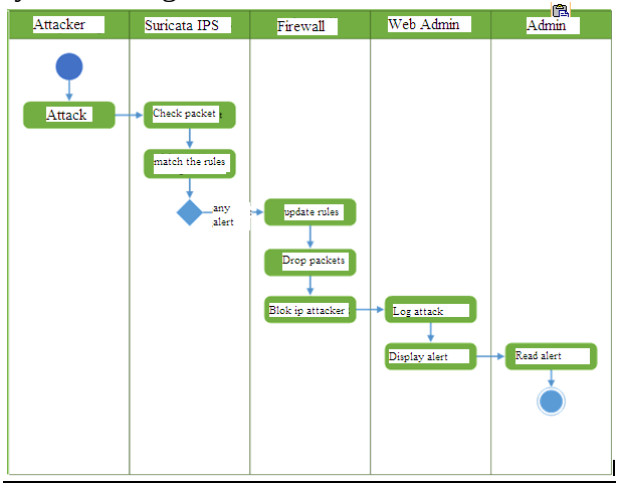

Figure 7. *Activity* IPS Diagram

RESULTS AND ANALISYS

In the study of these analyzes can be tested on Suricata attack detection system, accompanied by WebAdmin to monitor the results of the attack. The trial aimed to ensure that Suricata IPS system that has been built in accordance with its objectives. The test is done between the client and server are focused on the internal network.

After installation and configuration on Suricata, further testing to ensure that Suricata IPS IPS Suricata can run well.

To run Suricata in inline mode using the command sudo suricata –c /etc/suricata/suricata.yaml –q 0. And if you want to dismiss it by pressing Suricata ctrl + c on the keyboard. To find out the status *chain* IPTables can use the command sudo iptables –vnL

After the configuration steps and test Suricata IPS function is complete, then Suricata ready to be tested detection and function *drop* packets from the attacker. In the trials can attack using software such as superscan, nmap, dan nikto.

After the attack launched by the Suricata will check on each packet to the server. If the package is considered to be an attack, then Suricata will issue alerts and kept on file *log* suricata. The alert will then be read by WebAdmin to be displayed on the web and make a warning sound accompanied by admin easier to check the condition of the network.

Conclusion

Results of analysis of design intrusion prevention system (IPS) based Suricata produce some conclusions are:

1. Suricata and IPTables that has been configured to be the inline mode can work well.
2. The system is capable of connecting between Suricata WebAdmin and IPTables well so that it can block the attacker's IP through the web.
3. Implementation of Intrusion Prevention System can protect servers from threats, because the IPS can prevent suspicious attacks on the network.
4. WebAdmin allows a network administrator to observe the state statistics and computer attacks IPS. WebAdmin can also be a warning to raise the alert sound when the attack occurred.

Reference

[1] Wicaksono, Bayu. Perancangan Dan Implementasi IPS (Intrusion Prevention System) Berbasis Web Menggunakan Snort Dan IPTables. 2012.

[2] Aryadi, Tamsir. Implementasi Intrusion Prevention System (IPS) Pada Jaringan Komputer Kampus B Universitas Bina Darma. Vol 14: 1-14. 2012.

[3] Ulum, Bahrul. Rancang Bangun Intrusion Prevention System Pada Jaringan TCP/IP mengunakan Snort dan IPTables. 2013.

[4] Stiawan Deris, "Intrusion Prevention System(IPS) dan Tantangan dalam pengembangannya," FASILKOM, UNSRI, Palembang, Indonesia.

[5] Purbo, Onno, 2010. Keamanan Jaringan Komputer. Handry Pratama. Jakarta.

[6] Open Information Security. Open Information Security Foundation. URL: http://www.openinfosecfoundation.org, diakses tanggal 1 Desember 2013.

[7] Aldeid Foundation. Suricata/Introduction. 5 April 2011. URL: http://www.aldeid.com/wiki/Suricata/Introduction#Description, diakses tanggal 3 Desember 2013.

[8] Suricatayaml - Suricata - Open Information Security Foundation. URL: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricatayaml, diakses tanggal 20 Mei 2014.