Advances in Social Science, Education and Humanities Research, volume 410
1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)

Implemetation of Snort IPS Using PfSense as Network Forensic in Smk XYZ

1st Saleh Dwiyatno
Program Studi Rekayasa Sistem Komputer
Fakultas Teknologi Informasi
Universitas Serang Raya
Kota Serang Indonesia
salehdwiyatno@gmail.com

2nd Widya Ayu Andriani
Program Studi Rekayasa Sistem Komputer
Fakultas Teknologi Informasi
Universitas Serang Raya
Kota Serang Indonesia

3rd Ayu Purnama Sari
Program Studi Sistem Informasi
Fakultas Teknologi Informasi
Universitas Serang Raya
Kota Serang Indonesia

4th Sulistiyono
Program Studi Informatika
Fakultas Teknologi Informasi
Universitas Serang Raya
Kota Serang Indonesia

***Abstract*—The rise of attack software that can be easily accessed from the internet, makes anyone who doesn't ability to hack can do it. SMK Negeri 2 Pandeglang has a server that is used as a learning for all students. This encourages vulnerability to e-learning server attacked using software from the internet. So that a security system can detect attacks and take preventive actions and can carry out an investigation. This study aims to prevent any attempt to attack, detect and take preventive action against the attacker to carry out an investigation of the attack's log. This research was conducted using survey methods. The study was conducted for four months from April 1, 2019 to July 31, 2019. The result of this research is a security system that can detect an attack attempt and block the attacker's IP Address and conduct investigations using network forensic.Based on the result of the study it can be concluded that by using Snort with IPS mode stored on PfSense can detect attack aimed at e-learning servers and PfSense automatically takes preventive measures in the form of blocking of the attacker's IP Address. From the alert generated by Snort, investigative action can be taken using network forensics so that reporting if the effects of the attack are detrimental.**

Keywords: network forensic, Snort, PfSense

I. INTRODUCTION

The very rapid development of technology demands an increase in the quality of network security. Especially with the increasingly open knowledge about hacking and cracking which is supported by tools that can be obtained easily and for free. Tools that are used can be a network tool that is commonly used and tools used to carry out attacks.

Network forensic is one of the methods used to carry out network security. When an attack occurs on a computer network, an investigation is needed. An investigation was conducted to find and collect evidence related to the attack.

The potential for an attack to be directed at the SMK Negeri 2 Pandeglang server is very large because there is important data on a server and there is a server that often needs to be accessed by both teachers and students. In the event of an attack and not handled properly will cause obstruction of teaching and learning activities. After an attack, it is necessary to identify the attack in order to maximize the infrastructure in the network.

Therefore, a network-based IPS (NIPS) based security system is needed using Snort installed on PfSense to block and investigate alerts for network forensic purposes.

II. METHOD

The problem that occurs at SMK Negeri 2 Pandeglang is the emergence of vulnerability to e-learning servers that have data about learning material and some teaching and learning activities shared through that server. The rise of software on the internet that is used to carry out attacks makes someone who does not have the expertise to do attack techniques. This resulted in the vulnerability of SMK Negeri 2 Pandeglang servers in these activities.

Alternative solutions that can be done are by implementing a network security system using Snort tools to detect every activity that is on the network, installing Snort tools on the PfSense open source firewall in order to take preventive measures, namely blocking IP Addresses to attackers and conducting investigative activities against attacks using a branch of network forensic science.

III. RESULT AND DISCUSSION

The network at SMK Negeri 2 Pandeglang is complex but has vulnerabilities due to servers that can be accessed from outside. From this vulnerability an attack can occur which can be detrimental. For this reason, the authors make a proposal by adding a forensic network server using the PfSense open source firewall and Snort tools in the network infrastructure. It serves to analyze and investigate the source of the attack and can take preventive measures in the form of blocking IP Address against the IP Address that is indicated as an attacker.

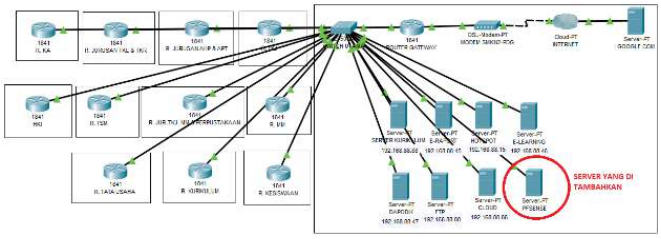

Fig.1. Proposed Network Topology

In the initial test carried out is to attack using Denial of Services using Low Orbit Ion Cannon (LOIC) tools when Snort installed on PfSense has not been activated. The results obtained are:

- Network traffic provided by PfSense has not shown any suspicious activity or is still under normal circumstances.

Fig.2. Network Traffic Before Active Snort

- No alerts appear on the PfSense dashboard or on the Snort Services menu.

In the final test carried out by activating Snort installed on PfSene as a forensic server and will be tried by conducting several attack experiments. And analyze the Alert tab and the Blocked tab for network forensic purposes.

Testing Stages :

- The reporting stage is carried out to write a report about the inspection process and information obtained from the previous stages.

1) HTTP Inspect. Testing using HTTP inspect is carried out by client computers that try to exploit forensic server websites. The result is that Snort detects an HTTP inspect and makes an alert and PfSense automatically blocks the attacker's IP Address.

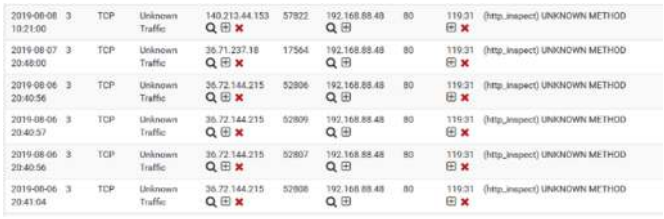

Fig.3. HTTP Inspect Alert

The approach taken in conducting network forensic processes is the forensic process model.

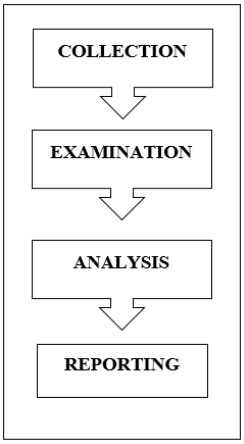

Fig.4. Forensic Process Model Approach

The analysis of the alerts generated by Snort is as follows.

- The collection stage is the stage of collecting evidence carried out by Snort because it has detected an attack in the form of HTTP Inspect.
- Examination stage is the examination of evidence that has been collected at the collection stage. Checks are made on the alerts that are generated as well as on the file alerts that have been downloaded.
- The analysis phase is the stage to study the results of the examination. This stage serves to answer forensic questions.

TABLE 1 SUMMARY OF FORENSIC QUESTIONS (1)

Forensic question	The answer
What attack happened?	HTTP Inspect
When did the attack occur?	08-08-2019 jam 10.21, 07-08-2019 jam 20.48, and 06-08-2019 jam 20.41
What is the attacker's IP Address?	140.217.55.153, 36.71.237.18, and 36.72.144.215
What is the destination IP Address?	192.168.88.48 (IP Address server forensic)
What protocol is used?	TCP
How many ports were attacked?	80
What is the classification of assault?	Trafik dan metode yang digunakan tidak diketahui

2) Denial of Services (DoS). Denial of services is done to disable the e-learning server with IP Address 192.168.88.46. *DoS is done from a client PC that uses the Debian Server operating system.*

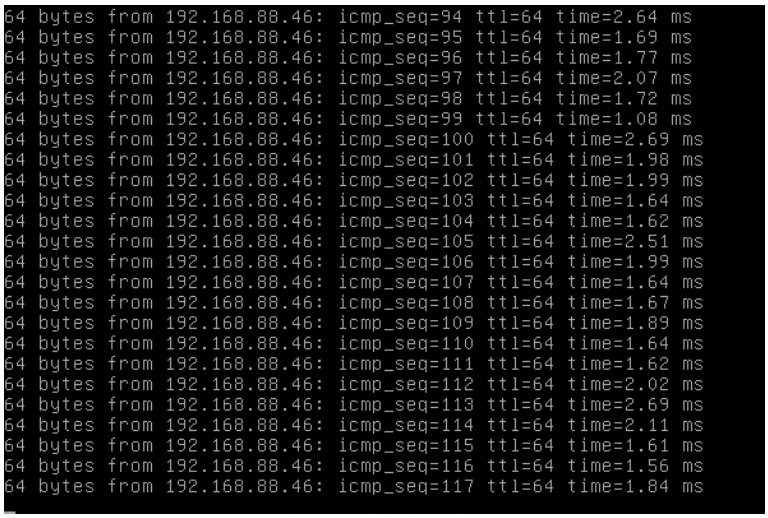

Fig.5. Denial of Services

The alerts generated by Snort are used as material for conducting forensic networks by summarizing forensic questions.

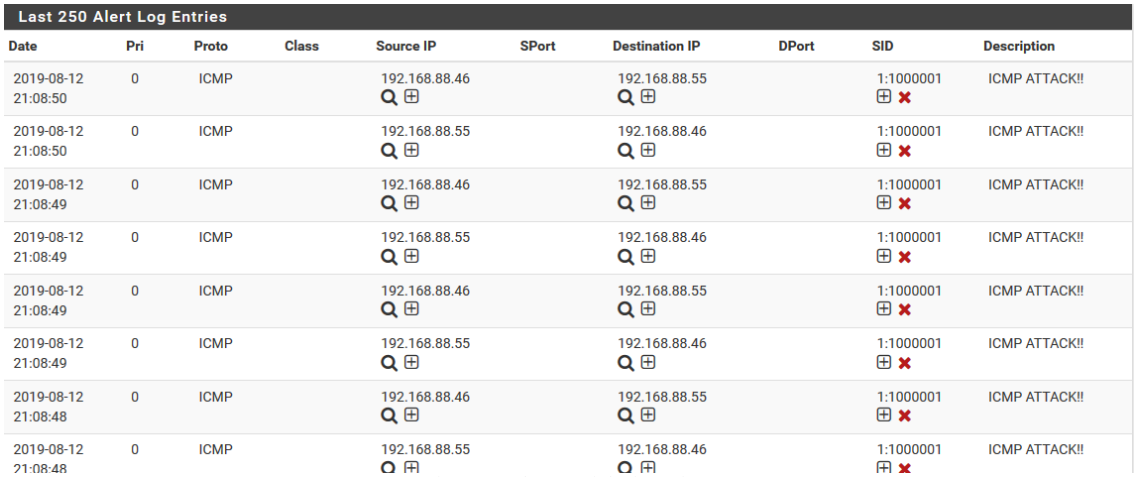

Figure 6. Alert Denial of Services

TABLE 2 SUMMARY OF FORENSIC QUESTIONS (2)

Forensic question	The answer
What attack happened?	12-08-2019 jam 21.08
When did the attack occur?	ICMP
What is the attacker's IP Address?	192.168.88.55 and 192.168.88.50
What is the destination IP Address?	192.168.88.46 (IP Address server e-learning)
What is the meaning of the message generated?	"ICMP ATTACK" provide information that an attack occurred using the ICMP protocol with a large size

3) Port Scan is performed to detect several open ports so that they are vulnerable to an attack. Port scans are performed using Zenmap software installed on the client PC. Port scans are for forensic servers.

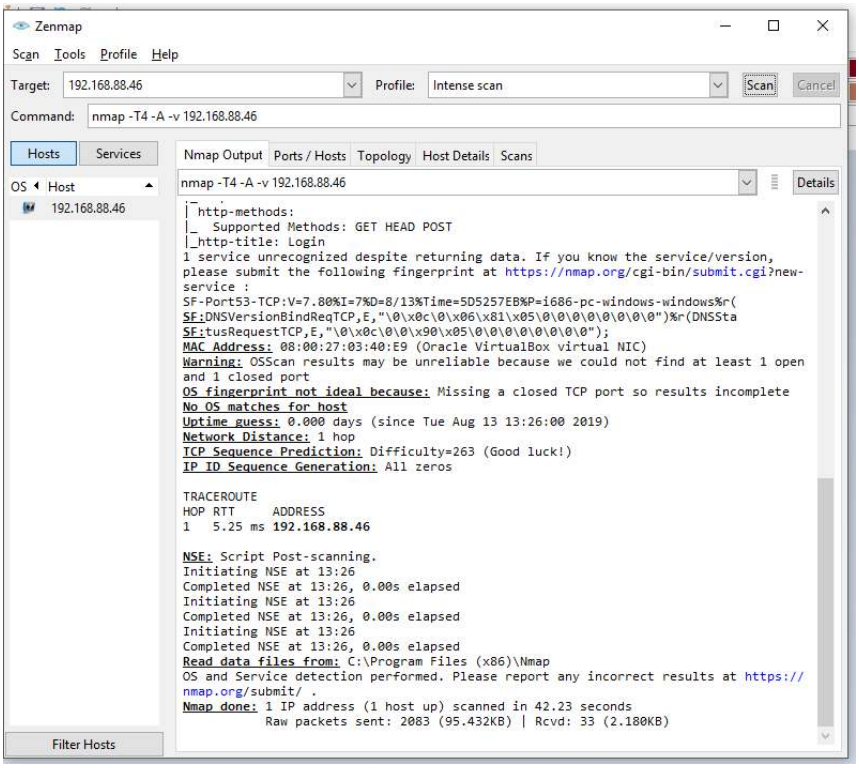

Fig.7. Port Scan

Alerts generated by Snort are used as material for analysis using network forensics.

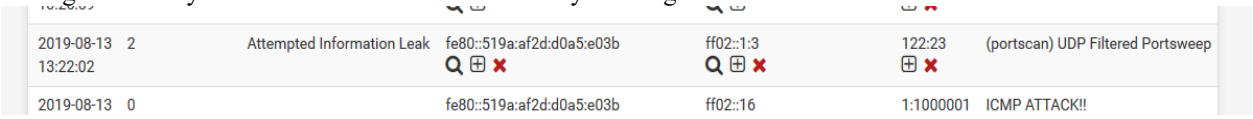

Fig. 8. Alert Port Scan

TABLE 3 SUMMARY OF FORENSIC QUESTIONS (3)

Forensic question	The answer
What attack happened?	13-08-2019 jam 13.22
When did the attack occur?	Fe80:519a:af2d:d0a5:e03b
What is the attacker's IP Address?	Ff02::1:3
What classification is given by Snort?	An attempt was made to leak information using a port scan
What is the meaning of the message generated?	There was an attempt to leak information using the port scan on the UDP protocol.

4) ARP Spoofing is done for sniffing data packets intended for victim PCs from client PCs. In this test, Snort provides rules preprocs and has provided rules for detecting ARP spoofing. ARP spoofing is done from a PC client with the Ubuntu operating system using the Ettercap application.

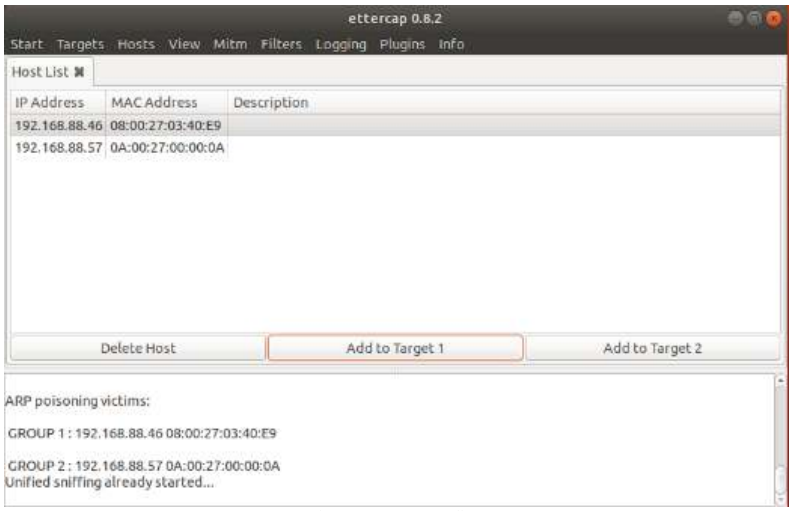

Fig.9. ARP Spoofing

The alerts generated by Snort do not have an attacker's identity because the rules provided by PfSense do not include the attacker's identity.

Fig.10. Alert ARP Spoofing

Fig.11. Rules ARP Spoofing

When Snort alerts an attack attempt, PfSense will automatically take preventive measures in the form of blocking.

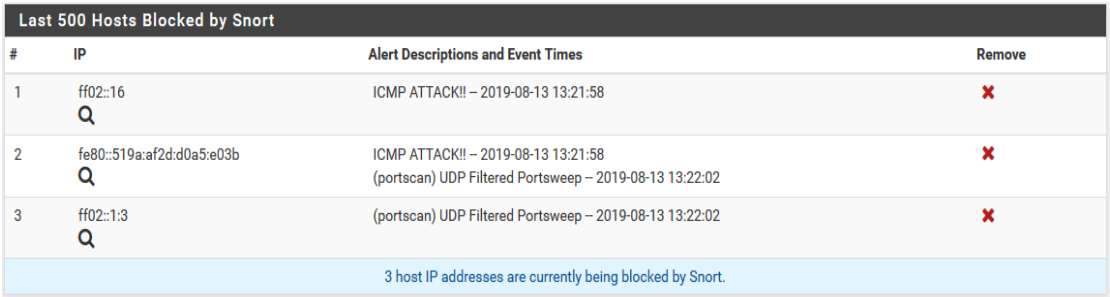

Fig.12. Log Blocked Snort

The results obtained in the Snort test that the alerts generated by the Snort log have detected every packet of data that made an attack attempt or carried out an attack. PfSense will automatically block both the attack IP Address. Log alerts and blocked logs on Snort can be downloaded for network forensic purposes.

Every attack or assault attempt made from a PC client affects traffic on PfSense. The traffic is appropriate from the attack source interface.

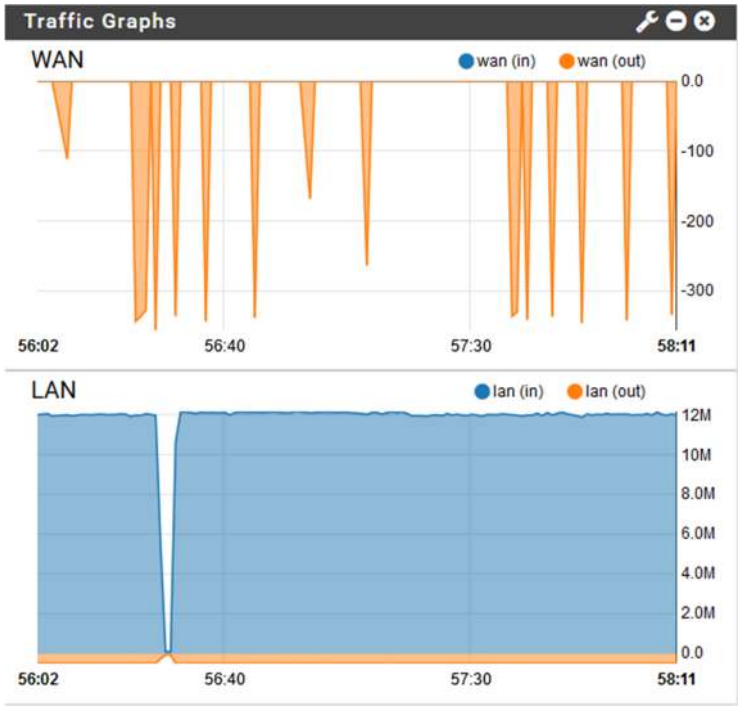

Fig.13. Attack Traffic

Attempts to attack made from the client come from the LAN interface which means it is still in the school network. Seen on the LAN graph, traffic reaching 12 Mbps indicates an activity on the interface. The traffic also experienced a noticeable increase until finally it was constant at 12 Mbps. When compared with normal traffic which means that there is not a large activity or an attack attempt, the resulting traffic will not reach 12 Mbps.

The alerts generated by Snort are material for network forensic investigations. From this information, an administrator can find out what is happening on a computer network so that he can track the data of the attack and attack attempt.

IV. Conclusion

The construction of a forensic server using PfSense and Snort is able to prevent and investigate attacks and take preventive actions on the network because it has a package manager to detect attacks. By activating the rules that suit your needs, Snort is able to identify each attack and PfSense will automatically take preventive measures in the form of blocking and alerts generated by Snort that can be used as an analysis for the network forensic investigation process.

Acknowledgments

Researchers realized that during the process of this research found many difficulties. These difficulties will not be resolved by researchers without the help and encouragement of various parties.

References

[1] Bintara, Hengky. (2017). Mengenal Snort Sebagai Network Intrusion Detection System (IDS). [Online]. Tersedia: https://netsec.id/snort-nids/ [22 April 2018]

[2] Budiharjo, Suyatno, et al. (2014). "Forensik Jaringan Pada Lalu Lintas Data Dalam Jaringan Honeynet di Indonesia Security Incident Respone Team On Internet Infrastructure/ Coordination Center". Akademi Telkom Sandhy Putra Jakarta. Vol V, No. (9). 16-23

[3] Caswell, Brian. dan Beker, Andrew. (2007). Snort IDS and IPS Toolkit. USA: Syngress

[4] Clarke, Justin. (2012). SQL Injection Attack And Defense. British: Elsevier

[5] Dewi, Kusuma, et al. (2017). "Analisis Log Snort Menggunakan Network Forensic". Jurnal Ilmiah Penelitian dan Pembelajaran Informatika. Vol. 2, No. (2). 72-79

[6] Dewi, Kusuma, et al. (2017). "Snort IDS Sebagai Tools Forensik Jaringan Universitas Nusantara PGRI Kediri". Seminar Nasional Inovasi Teknologi.

[7] Diansyah, Mohd. (2015). "Analisa Pencegahan Aktivitas Ilegal Di Dalam Jaringan Menggunakan Wireshark". Jurnal Times Medan. Vol. IV, No. (2). 20-23

[8] Erza, Muhammad. (2013). Menangani Serangan Intrusi Menggunakan IDS dan IPS. [Online]. Tersedia: https://keamanan-informasi.stei.itb.ac.id [14 November 2018]

[9] Fadlil, Abdul, et al. (2017). "Pengembangan Sistem Pengaman Jaringan Komputer Berdasarkan Analisis Forensik Jaringan". Jurnal Ilmu Teknik Elektro Komputer dan Informatika .Vol. 3, No. (1)

[10] Fahrianah. (2019). Backhaul. [Offline]. Tersedia: www.scribd.com/backhaul [26 Januari 2019]

[11] Hypernet. (2018). Jenis-jenis Router. [Online]. Tersedia: https://hypernet.co.id [14 November 2018]

[12] PFire. (2018). Features. [Online]. Tersedia: www.ipfire.org [14 November 2018]

[13] Kurniawan, Agus. (2012). Network Forensic Panduan Analisis & Investigasi Paket Data Jaringan Menggunakan Wireshark. Yogyakarta: Penerbit Andi

[14] Komputer, Teori. (2017). Topologi Jaringan Extended Star. [Online]. Tersedia: www.teorikomputer.com/2017/02/topologi-jaringan-extended-star.html [26 Januari 2019]

[15] Komputer, Wahana. (2006). Menginstalasi Perangkat Jaringan Komputer. Jakarta: PT. Elex Media Komputindo

[16] Komputer, Wahana. (2010). Tutorial Lima Hari Belajar Hacking Dari Nol. Yogyakarta: Penerbit Andi

[17] Knowledge, Raf. (2010). Trik Monitoring Jaringan. Jakarta: PT. Elex Media Komputindo

[18] Mikrotik. (2019). Interkoneksi Jaringan Dengan Tunnel. [Online]. Tersedia: http://www.mikrotik.co.id/artikel_lihat.php?id=91 [08 April 2019]

[19] Netgate. (2019). Configuring the Snort Package. [Online]. Tersedia: docs.netgate.com [29 Mei 2019]

[20] Netgate. (2019). Virtualizing PfSense with Proxmox. [Online]. Tersedia: docs.netgate.com [10 Juni 2019]
[21] PfSense. (2018). Getting Start Overview. [Online]. Tersedia: www.pfsense.org [14 November 2018]
[22] Pratama, Eka. (2014). Handbook Jaringan Komputer Teori dan Praktik Berbasiskan Open Source. Bandung: Penerbit Informatika
[23] Putri, Utami, et al. (2012). "Analisis Forensik Jaringan Studi Kasus Serangan SQL Injection pada Server Universitas Gadjah Mada". Indonesian Journal of Computing and Cybernetics Systems. Vol. 6, No. (2). 101-112
[24] Rafiudin, Rahmat. (2010). Mengganyang Hacker Dengan Snort. Yogyakarta: Penerbit Andi
[25] Sutarti, et al. (2018). "Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal". Jurnal PROSISKO. Vol. 5, No. (1)
[26] Umar, Husein. (2003). Metode Riset Bisnis. Jakarta: Gramedia Pustaka Utama
[27] Wijaya, Irtanto. (2018). Bedah Total Server: Referensi Lengkap Teknologi Server, Data Center, Virtualization, Cloud Computing & Enterprise Sistem. Jakarta: M&C Gramedia
[28] Winarno, Edi. Zaki, Ali. (2015). Belajar Hacking dari Nol untuk Pemula. Jakarta: PT. Elex Media Komputindo