AUTOMATION SNORT RULE FOR XSS DETECTION WITH HONEYPOT

Syaifuddin
Faculty of Engineering
School of Information Technology
University of Muhammadiyah Malang
Indonesia, Malang
Email: saifuddin@umm.ac.id

Diah Risqiwati
Faculty of Engineering
School of Information Technology
University of Muhammadiyah Malang
Indonesia, Malang
Email: risqiwati@umm.ac.id

Hanugra Aulia Sidharta
Faculty of Technology and Design
Computer Science Program Study
Bina Nusantara Institute of Creative Technology Malang
Indonesia, Malang
Email: hanugra.sidharta@binus.edu

***Abstract*— In modern era, data has become precious and important, data leak can lead to high damage to business, impact on losing profit. To avoiding those problems, organization need equip with updated security tools to protecting data and network. As computer network growing rapidly, currently security become important to prevent from attack, both from outside and inside the network. In line with that, new vulnerability grown on everyday basis and resulting increment number of intrusion and attack. Unfortunately, each intrusion and attack have a different pattern and unique behavior, continuous development and research on intrusion detection is mandatory. By statistic, in 2017 attack associated with XSS attack is grew 39% compared with 2015**

Keywords: Network attack, IDS, XSS

I. INTRODUCTION

Number of device connected and tethered to computer network growing every day. With technology explosion, almost every person has a PC, laptop or smartphone that starve to connect with internet. This led with increment number of attack on computer network. estimated reaching 580 million number of occurrence. [1] Cyber-attack can spread fast on computer network, on 2004 some researcher found swarm of botnet with estimated roughly up to 25.000 bots with capability transmit junk data around 5 Gbps, sufficient to make computer network on several company become offline. [2]

Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) have been used thoroughly on industrial network. Intrusion Detection is processing to monitor and observe on computer network for unrecognize threat, illegal activities. IDS also can inspect network traffic, to preventing system being target from attacker, such as DDOS attack.[3] IDS/IPS used to identify malicious activity and abnormal activity in network system. With effective IDS, should be have knowledge to detect several type of attack, its variant, several possible technique to evasion attack. [4]

With current IDS/IPS, system just can handle passive intrusion, but with adding honeypot, system can act as an active defender, or act as a decoy, so when there is intrusion, intruder is attack on honeypot as decoy, not real server or real network.[5]

XSS or Cross Site Scripting in one of most common technique used to hack with exploiting application layer. In 2017, attack to web is associate with XSS is grew 39% compared with 2015[6]. XSS also origin of many other attack, such as information disclosure, credential stolen, and content spoofing. XSS attack is simple but yet effective, just by insert malicious script exploit on URL parameter, cookies, database query [7]

II. BACKGROUNDS

This section expounds the details of the relevant information relating to the paper's topic.

A. Concept of Intrusion Detection System (IDS)

IDS or Intrusion Detection System is specific device or software with capability to monitor and observe network activity inbound and outbound through system, and recognize compromising pattern that may indicate system is under attack by someone, or someone attempt to compromise network. [8]

Snort is a popular open source IDS/IPS which can utilize for protecting system from attacker. Developed by Martin Roesch in 1998 with C language. Snort can run on almost every computer architecture and OS (Operating System). Snort IDS is real time-based alerting, it monitors and observe anomalies in traffic packet comparing it with rules. Rules in Snort IDS is user friendly and easy to modify. With basic component such as : Packet Decoder, Preprocessor, Detection Engine, Logging and alerting system, and output module. [9]

Snort utilizing rules and compare it with data packet from traffic onto network. Figure 1 is shown basic rule Snort IDS, which divided into two logical part: rule header, and rule option. Figure 2 is shown each field from rule header part, that contain criteria definition. Criteria definition use for comparing data between rule and data packet from network. Rule option following rule header and they are within pair of parentheses. Or in simple word, each option of rule contains 2 parts: keyword and argument. Keyword option extract from arguments with emblem colon. And argument is option inside the emblem double quote, each rule separated with semicolon

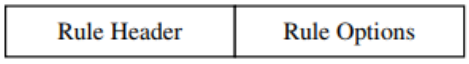

Fig. 1. Snort IDS rule structure

978-1-5386-8402-3/18/$31.00 ©2018 IEEE

Action	Protocol	Source Address	Source Port	Direction	Destination Address	Destination Port

Fig. 2. Snort IDS rules header structure

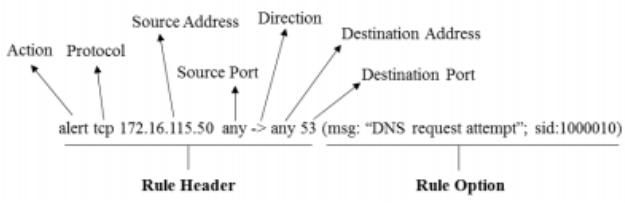

Fig. 3. Example snort IDS

Example of snort IDS rule shown on Figure 3, this rule will triggered general alert with condition: if there is tcp protocol request from source IP address: 172.16.115.50 with any port sent to any IP address with destination port is 53. If this rule triggered will show message: "DNS request attempt", this rule will have saved as sid:1000010

Advantage using IDS can summarize as [10]

1. IDS can detect attack and variant security breech flawlessly
2. Identify harm and affected system.
3. IDS do not suffer with harmful security.
4. Act as quality control for security model and implementation
5. On each suspected attack, IDS will save pattern and behavior for future prevention system.
6. IDS can observe and analyze activity on computer or network.
7. IDS could check system configuration even through vulnerabilities for integrity system.
8. Estimate and analysis abnormal or irregular service.

B. *Honeypot*

Honeypot develop by Lance Spitzner, founded in 1999 as honeynet project in nonprofit research. Honeynet design to attract intruder, act as a trap for unauthorized communication on network. Honeypot also can used to learn intruder behavior and intrusion pattern.[11]. Besides that, honeypot can dig various tools used by hacker, even can examine social network of intruder.

Main feature of honeypot is on accuracy from data collection. Unlike most IDS system, honeypot examine only on known attack. Honeypot cannot directly protect on system, unlike IDS that can by pass interception techniques to monitor entire network[5]

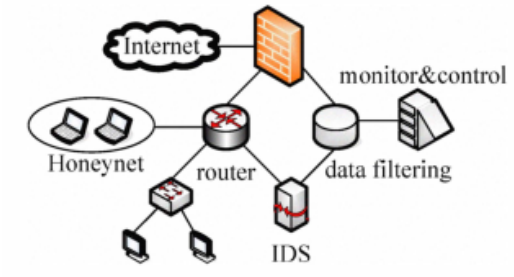

Fig. 4. Honeypot system structure

In Figure 4 shown honeypot system structure, honeypot not really protect network, this system act as a decoy. So, hacker is attack honeypot, not the real system. Unfortunately, honeypot can't be running standalone on system, honepot need defense with firewall also IDS. Honeypot server act as security policy core, access control, provide security protection through security check, such as traffic analysis, hole detection, pattern matching. Meanwhile IDS support on rapid transform from static to dynamic protection.

Advantages of honeypot

1. Data collection: normally honeypot collect most data, this system provides a lot of useful information. With these data we can know hacker profile, pattern, how they interact with system.
2. Resource: with honeypot sysadmin can studying on hacker without exposing real system, and minimalizing compromised system
3. Honeypot provide prevention compromised system.

Disadvantages:

1. Honeypot is worthless if there is no attack on system
2. While there is no activity, honeypot essentially have no use.
3. Honeypot can have misused to attack another machine on another network
4. While honeypot can act as decoy, but there is varying level of risk compromised on security

To overcome those issue, author suggested develop honeypot to dynamic and hybrid model.[12]

C. *Cross Site Scripting (XSS)*

According to Web Hacking Incident Database, most popular attack is SQL Injection, XSS (Cross Site Scripting) and DoS (Denial of Service) [7]. XSS attack first discussed in Computer Emergency Respond Team (CERT) back on 2002. [13]

Cross Site Scripting (XSS) is application level code injection type security vulnerability. It may occur while server program uses unrestricted input through HTTP request, or database without any validation. With these vulnerability, hacker can get sensitive data, such as cookies, session log. On figure 5, illustrated sequence XSS attack to some server program. Example on untrusted blog, some user wants to check latest command, legitimate user sent HTTP request for view latest command. Site will respond those request, but due database server already infected with XSS, sensitive information leak to attacker web server.

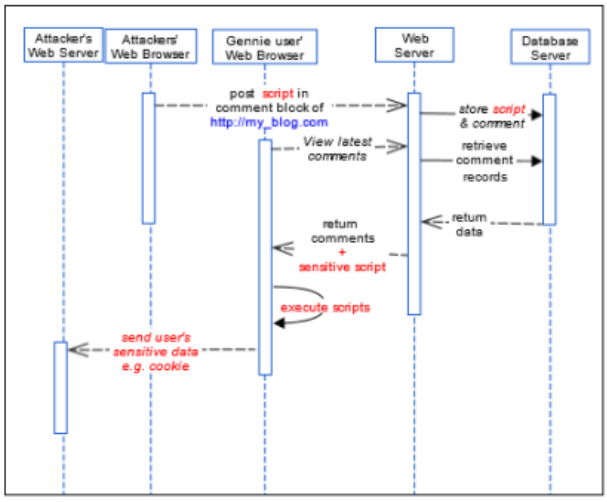

Fig. 5. Sequence diagram to represent XSS attack scenario

III. Related Works

Previously, there were several researchers that focused on snort IDS to detect network probe attack, with snort IDS can detect 100% network probe attack based on MIT-DARPA 1999. [9] Khamphakdee et all suggest improving snort IDS with other attack, such as: DOS, U2R, R2L, XSS.

Garg et all research IDS detect attack using signature from malicious and harmful attack. Signature base IDS used to detect known attack, and unknown attack detect with Anomaly based IDS. Garg emphasize due IDS need update frequently due system need to familiar with new attack and threat. [10] Alam et all investigate possibility splitting traffic between snort sensor using policy based splitting mechanism. System will adapt adjusting with incoming traffic dynamically, with this policy will shift traffic load from one sensor to another sensor for improving system performance. [14] Zhai et all, successfully implement IPS based on snort on windows platform. Snort successfully implement by utilize between snort and IPSec [15]

Chawda et all introduce novel dynamic and hybrid model for analyze pattern, characteristic, and track internet thread, such as worm. Data collected from passive fingerprint tools (POf) and active probing such as Nmap [12]. From survey conducted by Cambell et all shown since 2006 honeypot research begin in line with increment number of PC or laptop connected with network, but since 2013 there is another device begin to hook up with internet, smartphone begin to replace PC or laptop. [1] Comparing with other defense strategy and mechanism, honeypot is superior due simple, more flexible during configuration, and consume less resource.[5]

IV. Simulation Scenario

On our research, we use several PC with different OS on each PC as figure 6. Attacker PC user OS Back Box. Second PC act as honeypot server, this PC also can listen to network. Third PC as IDS server to filter all packet on network between all PC.

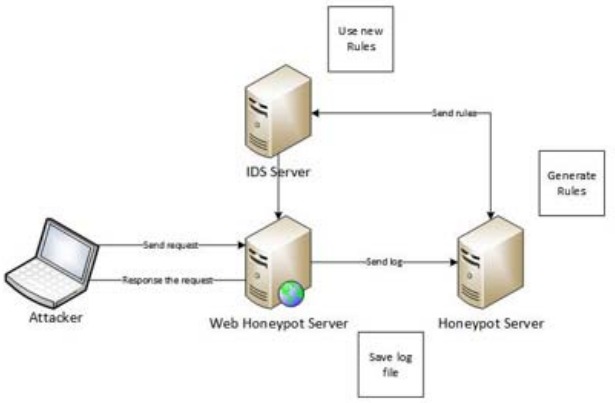

Fig. 6. Honeypot and IDS server topology

In these research IDS server will tell another server if there is breach on server. Rule will continuously update while there is attack on server while current attack is not on list of rules. Assume attacker already succeeded brake into server, all activities record on honeypot log. Malicious script that run on honeypot will become reference for making new IDS rule. Several data also gathered as part new rule, such as: IP address, port number, port protocol service requested, url request from attacker. To manage all of those data we develop program, with those programs will make IDS rule automatically

Step per step algorithm we use to make auto generate IDS rules

1. When honeypot receive HTTP request, honeypot server will listen to specific service and port. To help detect illegal script we filter URL request packet converted to hex. Example, “<script></script>” will be converted to ”%3Cscript%3E %3C%2Fscript%3E”.
2. Program will check whether those request packet contain illegal activities or not. It there is no illegal suspect than packet will redirect to normal web page. But if there is detected anomalies, honeypot will record log and URL request.
3. URL and tag from XSS will separate and save on another log file
4. Those log file will compare with snort rule, if there are new illegal activities, system will add new rule automatically. IDS server will update that information gradually.

V. Simulation Results

In this research we simulate with 200 XSS attack samples, each attack will record on honeypot. XSS attack list method collected from xxsed.com, owasp.org andcyclist github sample. From each attack we check whether those logs can use to generate rule for XSS attack. But due special character limitation, and there is too many variate XSS attack not all attack succeed generate automatic rule. Below several rule that succeed make by system.

TABLE I. SNORT RULE

No	*Rules Snort*
1	*Alert* tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"XSS attempt: script injection detected "; flow:to_server,established; content:"*Alert*(%22XSS_BY_C37HUN%22)"; classtype:attempted-admin; sid:1000001;)
2	Alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"XSS attempt: script injection detected "; flow:to_server,established; content:"Alert%281%29"; classtype:attempted-admin; sid:1000002;)
3	Alert tcp $EXTERNAL_NET any -> $HOME_NET any (msg:"XSS attempt: script injection detected "; flow:to_server,established; content:"Alert(document.cookie)"; classtype:attempted-admin; sid:1000003;)

Data on table 1 is example of rule that succeed generate by system. But not all rules can succeed generate automatically. This suspect due rules on snort server is case sensitive.

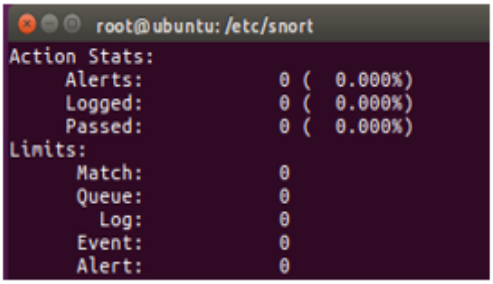

Fig. 7. Snort report on first attack

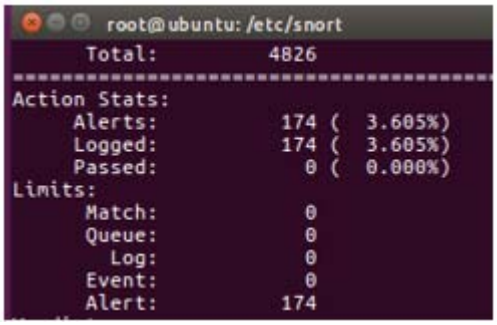

Fig. 8. Snort report on second attack

We conduct 2 phase XSS attack, first attack is occurred when snort data is blank, meanwhile on second attack snort data already updated with data form first attack. From figure 7, when IDS not have information about XSS attack, IDS not alerting if there is XSS attack. But this anomaly detected from honeypot log. From this data IDS data updated for XSS attack. After updated with data from first attack, on figure 8 as second attack, snort already know there is an attack. Snort alerting IDS if there is occur XSS attack, and IDS filtering packet from those attack. From 200 XSS attack, 174 attempts is blocked by IDS, but there is 26 attack miss but from snort stat cannot detect it. Suspect this occur due another variant of XSS attack or due case sensitive on snort rule

VI. CONCLUSIONS

According to the experiment result, automatic rule for XSS attack is succeed. From 2 phase XSS attack, snort rule succeeds generated base on first phase XSS attack. Comparing between 2 phase, on first phase there is no XSS attack succeed blocked, from 200 XSS attack attempt, not single attack is succeeding to block. On second phase IDS succeed blocked 174 XSS attack from 200 XSS attack, its mean 87% attack succeed blocked by IDS. Automatic rule is succeeding generated base on honeypot log data based on first attack

Although automatic rule is succeeding to generate, there is 13% attack is slip from IDS, suspect this caused by case sensitive snort rule. We propose for attack testing do numerous time, also need to develop rule for another attack, such as DOS, U2R, R2L

REFERENCES

[1] R. M. Campbell, K. Padayachee, and T. Masombuka, "A survey of honeypot research: Trends and opportunities," *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 208–212, 2016.

[2] Y. Al-Nashif, A. A. Kumar, S. Hariri, G. Qu, Y. Luo, and F. Szidarovsky, "Multi-level intrusion detection system (ML-IDS)," *5th Int. Conf. Auton. Comput. ICAC 2008*, pp. 131–140, 2008.

[3] S. Bajpai and A. Gupta, "A genetic annealing based new approach for IDS," *Proc. 2017 Int. Conf. Intell. Comput. Control Syst. ICICCS 2017*, vol. 2018–Janua, pp. 42–45, 2018.

[4] S. Roschke, C. Willems, and C. Meinel, "A security laboratory for CTF scenarios and teaching IDS," *ICETC 2010 - 2010 2nd Int. Conf. Educ. Technol. Comput.*, vol. 1, pp. 433–437, 2010.

[5] J. Bao, C. P. Ji, and G. Mo, "Research on network security of defense based on honeypot," *ICCASM 2010 - 2010 Int. Conf. Comput. Appl. Syst. Model. Proc.*, vol. 10, no. Iccasm, 2010.

[6] Guy Podjarny, "XSS Attacks: The Next Wave | Snyk." [Online]. Available: https://snyk.io/blog/xss-attacks-the-next-wave/. [Accessed: 02-Aug-2018].

[7] B. Jacob, "Automatic XSS detection and Snort signatures / ACLs generation by the means of a cloud-based honeypot system," no. December, 2011.

[8] J. Xi, "A design and implement of IPS based on snort," *Proc. - 2011 7th Int. Conf. Comput. Intell. Secur. CIS 2011*, pp. 771–773, 2011.

[9] N. Khamphakdee, N. Benjamas, and S. Saiyod, "Improving intrusion detection system based on Snort rules for network probe attack detection," *2014 2nd Int. Conf. Inf. Commun. Technol. ICoICT 2014*, pp. 69–74, 2014.

[10] A. Garg and P. Maheshwari, "Performance analysis of Snort-based Intrusion Detection System," *ICACCS 2016 - 3rd Int. Conf. Adv. Comput. Commun. Syst. Bringing to Table, Futur. Technol. from Arround Globe*, pp. 0–4, 2016.

[11] M. Baykara, "A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems," *Int. J. Comput. Networks Appl.*, vol. 2, no. 5, pp. 203–211, 2015.

[12] K. Chawda and A. D. Patel, "Dynamic & hybrid honeypot model for scalable network monitoring," *2014 Int. Conf. Inf. Commun. Embed. Syst. ICICES 2014*, no. 978, 2015.

[13] I. Yusof and A. S. K. Pathan, "Preventing persistent Cross-Site

Scripting (XSS) attack by applying pattern filtering approach," *2014 5th Int. Conf. Inf. Commun. Technol. Muslim World, ICT4M 2014*, 2014.

[14] M. S. Alam, Q. Javed, M. Akbar, M. R. U. Rehman, and M. B. Anwer, "Adaptive Load Balancing Architecture for SNORT," pp. 48–52.

[15] J. Zhai and K. Wang, "Research on applications of honeypot in Campus Network security," *Proc. 2012 Int. Conf. Meas. Inf. Control. MIC 2012*, vol. 1, no. Mic, pp. 309–313, 2012.