Sistem Deteksi HTTP menggunakan HTTP *Inspect Preprocessor* and *Rule Options*

M. Ridwan Zalbina, Deris Stiawan
Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya
zalbinaridwan@gmail.com
deris@unsri.ac.id

Abstract* – Penelitian ini membahas mengenai *Web Application* atau *HTTP Attack Detection System* dengan memanfaatkan *Network Intrusion Detection System* untuk mendeteksi aktivitas mencurigakan pada sistem *realtime traffic*. Salah satu yang dapat digunakan pada penelitian ini adalah Snort, dengan kemampuan dan modularitas pada *Preprocessor* dan *Detection Engine* seperti *HTTP Inspect Preprocessor* dan *Rule Options* yang dimanfaatkan sebagai bagian dari metode penelitian. Sebagai sistem berbasis *Knowledge NIDS*, Snort dapat digunakan untuk mendeteksi beberapa jenis serangan seperti XSS dan SQL *Injection*. *Alert* yang muncul di klasifikasi berdasarkan *request* dan *content* serangan. Hasil dari penelitian berupa, jumlah *alert* yang terdeteksi, *network traffic,* kemudian evaluasi dari hasil pengujian dengan *confusion matrix.

LATAR BELAKANG

Intrusion Detection System merupakan setiap perangkat keras, perangkat lunak atau kombinasi dari keduanya yang memiliki fungsi untuk memonitor suatu sistem atau jaringan dari segala aktivitas yang sifatnya *malicious* [1]. Pada saat melakukan monitoring, IDS pada dasarnya menerapkan *General Method Detection* seperti *Signature Analysis, Artificial Intelligence* dan *Computational Method* [2].

IDS diklasifikasikan berdasarkan penempatan sumber data dan sisi fungsional. IDS yang digunakan untuk memantau trafik jaringan dikenal dengan *Network Intrusion Detection System* [3]. NIDS bekerja pada *promiscous mode* agar dapat memberikan suatu *alert* apabila terjadi intrusi yang mengarah ke sistem. *Alert* muncul pada *realtime traffic* dari sistem deteksi yang menerapkan *Signature Based* sebagai metode deteksi.

Signature Based, *Misuse Detection* or *Detection by Appearance* [4] menerapkan mekanisme yang menyerupai perangkat lunak *antivirus* yang bergantung pada pengetahuan perangkat tersebut terhadap pola dari suatu paket data yang diindikasikan sebagai serangan. Jenis dari serangan atau intrusi dapat dibedakan berdasarkan protokol maupun layanan. Terdapat jenis serangan yang tergolong sebagai *web application attack* yang berjalan melalui *Hypertext Transfer Protocol* (HTTP) seperti *Cross Site Scripting, SQL Injection, Command Execution, File Inclusion, Cross Site Request Forgery, Path Traversal* dan beberapa jenis serangan lain. Serangan yang melalui protokol HTTP pada dasarnya sulit untuk dideteksi karena keragaman dan fleksibilitas serangan, kemampuan suatu NIDS sangat terbatas. Untuk itu perlu dilakukan pengkajian seputar hal tersebut.

Pada penelitian [5], membahas permasalahan mengenai SQL *Injection Attack* yang didasarkan pada *textual manipulation* pada *sql query* dan pengaruh penggunaan mekanisme tersebut pada beberapa web dan penggunaan Snort NIDS sebagai *Network Level Detection,* dimana pengujian dilakukan menggunakan *custom dataset.* Hasil penelitian tersebut juga dibandingkan dengan penelitian terdahulu yang memiliki relevansi seputar SQL *Injection Attack.* Sama halnya pada penelitian yang dilakukan [6], membandingkan beberapa *detection tools* seperti Snort, SCALP, PHP-IDS, ICD dan SQLADS.

Pada penelitian lain [7], membahas secara keseluruhan beberapa Snort *rules* dan bagaimana *rules* tersebut dapat meningkatkan keamanan pada suatu website dengan beberapa jenis serangan seperti XSS, SQLI dan *Command Injection Attack.* Selanjutnya, [8] melakukan penelitian dengan menerapkan *opensource* Snort NIDS untuk mendeteksi SQL Injection Attack pada beberapa DBMS seperti ORACLE, MS-SQL *Server,* MySQL dan *Cross Site Scripting* (XSS), dengan membuat *rules* berdasarkan *regular-expression.* Dari beberapa ulasan diatas, penggunaan *rules* dan *preprocessor* pada Snort dapat dimanfaatkan sebagai salah satu cara untuk mendeteksi serangan pada protokol HTTP. Beberapa pola serangan tersebut dapat direferensi sehingga dapat dijadikan *rules* untuk digunakan pada sistem *realtime traffic.*

HASIL SEMENTARA

Pada penelitian terdahulu, tidak dilakukan pengujian secara berulang dan evaluasi terhadap *rules* yang dibangun dan bagaimana proses pengujian dilakukan. Pada penelitian ini, pengujian dilakukan sebanyak 3 kali dengan durasi pengujian selama ± 60 menit yang bertujuan untuk melihat konsistensi dari rules yang dibangun, kemudian data secara kuantitatif dianalisis dan diklasifikasikan berdasarkan layanan dan jenis serangan, hingga dilakukan proses penghitungan berdasarkan *confusion matrix*.

Pengujian dilakukan dengan menggunakan 4 *endpoint*, 1 unit Server (DVWA), 1 unit PC untuk *realtime monitoring system,* 2 *notebook* PC yang digunakan untuk uji serangan, dengan menggunakan sistem operasi berbasis linux dan windows. Pengujian dilakukan pada pukul 12.45 sampai 14.00 WIB pada 7 Agustus 2015 pada laboratorium *Communication Network and Computer Security* (COMNETS) Fakultas Ilmu Komputer Universitas Sriwijaya. Uji serangan dilakukan 2 *endpoint* dengan IP : 10.100.206.12/24 dan 10.100.206.36/24 mengarah pada web DVWA dengan IP : 10.100.206.13/24, selanjutnya *realtime monitoring system* digunakan untuk memonitor secara langsung *alert* yang muncul.

Berdasarkan data pada tabel 1 berupa *alert, priority* dan jumlah serangan, terdapat total 340 *alert* yang muncul, terindikasi sebagai serangan dan sisanya merupakan normal *alert* dengan prioritas rendah pada metode *request* GET dan POST, dan yang lain merupakan *alert* dengan prioritas tinggi seperti XSS keyword dan SQL Injection query. Dari hasil pengujian tidak ada indikasi adanya unknown attack yang muncul sebagai *false negative*. Tabel2 merupakan tabel hasil kalkulasi *confusion matrix* berupa TP, FP, TN DAN FN. Terdapat total 6 *alert* terdeteksi sebagai FP dan 2 *alert* sebagai TN. Tingkat PPV dari pengujian pertama mencapai 98%

Dengan menggunakan *packet analyzer* seperti grafik 3, 4, 5 dan 6 merupakan hasil tes yang meliputi *Total Traffic, Top Local* IP, TCP *port* dan *matrix connection*.

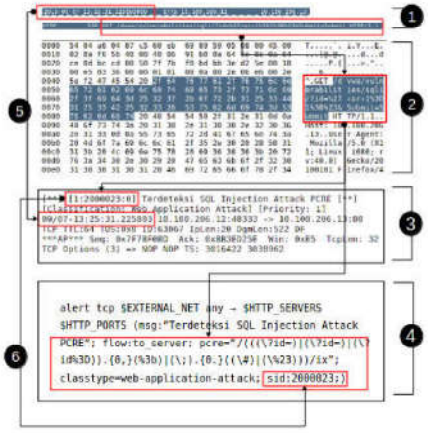
REFERENSI

[1] J. Koziol, *Intrusion Detection with Snort*. IndianaPolis: Sams Publishing, 2003.
[2] J.C. Shaik Akbar, K.Nageswara Rao, "Intrusion Detection System Methodologies Based on Data Analysis," *Int. J. Comput. Appl.*, vol. 5, no. 2, pp. 10–20, 2010.
[3] R. Bejtlich, A. Reviewer, S. Northcutt, and C. Hill, *About the First Edition of Snort Intrusion Detection*. Rockland, 2004.
[4] P. Patel, C. Langin, F. Yu, and S. Rahimi, "Network Intrusion Detection Types and Computation," vol. 10, no. 1, 2012.
[5] H. Alnabulsi, M. R. Islam, and Q. Mamun, "Detecting SQL Injection Attacks Using SNORT IDS," *IEEE*, p. 7, 2014.
[6] A. Majkowska, D. Zydek, and L. Koszałka, "Evaluation of Various Technique for SQL Injection Attack," *Springer*, vol. 226, pp. 763–772, 2013.
[7] M. Dabbour, I. Alsmadi, and E. Alsukhni, "Efficient Assessment and Evaluation for Websites Vulnerabilities Using SNORT," *Int. J. Secur. Its Appl.*, vol. 7, no. 1, pp. 7–16, 2013.
[8] K. K. Mookhey and N. Burghate, "Detection of SQL Injection and Cross-site Scripting Attacks," *Symantec*, 2010.

```
[**] [1:2000004:0] Terdeteksi XSS script [**]
[Classification: Web Application Attack] [Priority: 1]
09/07-13:01:47.168464 10.100.206.12:48041 -> 10.100.206.13:80
TCP TTL:64 TOS:0x0 ID:38180 IpLen:20 DgmLen:632 DF
***AP*** Seq: 0x2DEB8D1B  Ack: 0x89A0810  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2660408 2682948

[**] [1:2000024:0] Terdeteksi keyword SQLi [**]
[Classification: Web Application Attack] [Priority: 1]
09/07-13:18:16.433533 10.100.206.12:48270 -> 10.100.206.13:80
TCP TTL:64 TOS:0x0 ID:1335 IpLen:20 DgmLen:662 DF
***AP*** Seq: 0x89BD5B7A  Ack: 0xAC9B698F  Win: 0xE5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 2907724 2930264
```

Gambar 1. *Sample* Alert Hasil Pengujian



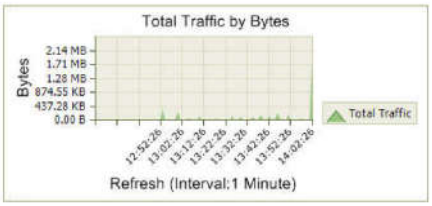
Gambar 2. Ekstraksi dan Korelasi Data Hasil Pengujian

TABLE 1. Jumlah *Alert* dari Pengujian ke-1

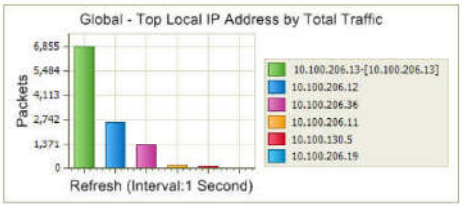
No	Klasifikasi Alert Terdeteksi	SID	Prioritas	Total
1	GET	2000001	2	258
2	SQLiA *keyword*	2000024	1	33
3	POST	2000002	2	17
4	XSS *script keyword*	2000004	1	14
5	XSS *script keyword 2*	2000008	1	7
6	SQLiA PCRE	2000025	1	4
7	XSS *image*	2000006	1	4
8	XSS *iframe keyword*	2000005	1	3

TABLE 2. Hasil dari *Confusion Matrix* Pengujian ke-1

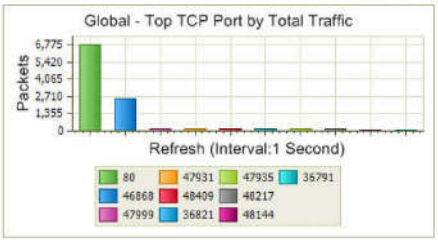
No	Hasil Deteksi	Total	Tingkat Akurasi Hasil Deteksi	Nilai	Persentase (%)
1	TP	334	TPR	1	100 %
2	FP	6	FPR	0.75	75 %
3	TN	2	TNR	0.25	25 %
4	FN	0	FNR	0	0 %
5			PPV	0.9823	98 .23%
6			NPV	1	100%



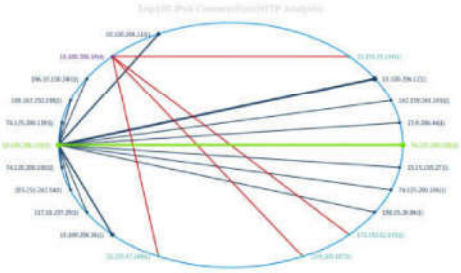
Gambar 3. HTTP *Traffic Analysis* Pengujian ke-1



Gambar 4. HTTP *Analysis Top Local* IP Pengujian ke-1



Gambar 5. HTTP *Analysis Top* TCP *Port* Pengujian ke-1



Gambar 6. *HTTP Analysis Matrix Connection* Pengujian ke-1

ISBN: 979-587-573-6