*Prosiding*
**ANNUAL RESEARCH SEMINAR 2016**
*6 Desember 2016, Vol 2 No. 1*

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

# Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means

Eko Arip Winanto
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera Indonesia
ekoaripwinanto@gmail.com

Ahmad Heryanto
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera Indonesia
hery@unsri.ac.id

Deris Stiawan
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera Indonesia
Deris.stiawan@gmail.com

***Abstract— Visualisasi merupakan salah satu teknikuntuk meningkatkan akurasi deteksi serangan yang terjadi di jaringan. Visulisasi bertujuan untuk mempermudah dalam mengenali dan menyimpulkan serangan terjadi. Clustering k-means dapat digunakan untuk mendeteksi paket serngan dan paket normal. Serangan remote to local adalah serngan yang dilakukan oleh attacker untuk mendapatkan akses akun ke sebuah sistem yang sebelumnya tidak memiliki akun ke sistem tersebut. Pola serangan R2L pada dataset DARPA dapat dikenali dengan beberapa paramer seperti sourceaddress, destination address, flags, ip length, dan tcp length***

.

***Kata Kunci—Visualisasi, Clustering, K-Means, R2L***

## I. PENDAHULUAN

Menurut [1] visualisasi dapat membantu *user* untuk mendeteksi pola serangan dengan lebih cepat, dan apabila dikombinasikan dengan teknologi seperti *datamining* atau*machine learning,* sistem visualisasi akanlebih efektif dalam mendeteksi pola serangan. Teknik yang diterapkan untuk mendeteksi serangan dapat menggunkan *clustering,* menurut [2] *clustering* dapat membantu mendeteksi serangan ketika data *trainingunlabeled,* serta untuk mendeteksi serangan baru atauserangan yang tidak diketahui.

Pada penelitian [3], [1] [4] , membahas tentang permasalahan visualisasi serangan menggunakaan teknik visualiasi *parallel coordinates. Parallelcoordinates* menampilkan *traffic* jaringan kedalambidang kordinat dua dimensai dan mempresentasaikan informasi seperti *source address, destination address,port source, port destination, ip length, tcp length.*

Penelitian [4], membahas bagaimana mendeteksi serangan menggunakan algoritma *clustering k-means.*

Serangan yang umum dilakukan oleh seorang *attacker* adalah mengeksploitasi *vulnerability* dari suatusistem. Menurut [5] R2L adalah ketika *attacker* dapat mengirim paket ke sistem melalui jaringan tetapi tidak memiliki akun kedalam sistem tersebuat dan mencoba mengeksploitasi *vulnerability* untuk mendapatkan akses *user* ke sistem.

Pada naskah ini terdiri dari beberapa bagain, bagian pertama pendahuluan menjelaskan latar belakang dari penelitian. Bagian 2 menyajikan tentang dasar teori.

Bagian 3 mengambarkan tentang metodologi yang dilakukan. Bagian 4 menyajikan hasil dari percobaan yang telah dilakukan. Terakhir, bagian 5 berisi kesimpulan dan penelitian selanjutnya.

## II. TINJAUAN PUSTAKA

1. *Intrusion Detection System*

*Intrusion Detection System* adalah kombinasi dari perangkat lunak atau perangkat keras yang berjalan pada suatu mesin untuk melakukan *monitoring* aktivitas pengguna dan program untuk mencari kemungkinan ancaman dari *insider,* serta memeriksa *traffic* jaringan yang terhubung dengan mesin dari jaringan luar [6].

*2. Feature Extraction*

Menurut [7], *feature extraction* sebuah pendekatan yang memungkinkan seseorang untuk mengidentifikasi pola yang tersembunyi atau yang tidak biasa karena pada *raw data* asli tidak mengandung informasi yang cukup untuk mengenali untuk paket serangan.

*C. Clustering*

*Clustering* merupakan teknik untuk mengklasifikasi

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

data yang tidak diketahui ke dalam satu grup untuk eksplorasi dan analisis data. Tujuan utama dari *clustering* meliputi antara lain memperoleh informasidari data (deteksi *anomaly*, identifikasi *feature*), *classification* data dan *compressing* data [8]. Menurut[9] *data mining* memiliki beberapa peran dalam *intrusion detection system* :

A Menghilangkan paket normal dari alarm dan fokus pada analisis data *attack.*
B Mengidentifikasi *false alarm* dan "*bad*" sensor *signature.*
C Menemukan aktivitas anomali yang tidak diketahui.
D Mengidentifikasi panjang dan pola yang berkelanjutan (beda *ip adderss,* aktivitasnya sama).

*D. Visualisasi*

Visualisasi adalah sebuah proses interaktif yang berulang terus-menerus antara visualisasi dan knowledge discovery, dan berfungsi mengumpulkan data [1]. Teknik untuk visualisasi menggunakan *parallel coordinates.* Menurut [3][1], *parallel coordinates* adalah salah satu teknik visualisasi yang dapat mempresentasikan *raw data* dengan multiple dimensions (parameter) kedalam bidang dua dimensi.

## III. METODOLOGI PENELITIAN

Langkah-langkah yang dilakukan pada percobaan ini ada beberapa langkah utama. Pertama melakukan *feature extraction* untuk mengekstrak dataset. Keduamelakukan *clustering* untuk mendeteksi serangan. Ketiga adalah memvisualisaikan serangan *remote tolocal* dalam bentuk grafik. Pada percobaanmenggunakan dataset DARPA 99 pada minggu ke-4 yang terdiri dari 5 hari percobaan. Ada beberapa tahapan yang dilakukan pada percobaan ini.

*[6] Feature Extraction*

Tahapan pertama adalah melakukan *feature extraction* pada dataset. Tujuan dari *feature extraction* adalah untuk mendapatkan informasi yang sebelumnya tidak diketahui pada dataset *traffic.* Atribut-atribut yang diekstrak pada paket *header* berupa nomor paket, *timestamp*, *service, source address, destination address, port source, port destination, sequence, acknowledgment, window, flags, ttl, ip length, ip ceksum, ip id, ip offset, tcp length,* dan *protocol.*

*B. Pola Serangan*

Kedua adalah mencari pola serangan *remote tolocal* berupa serangan *ftp_write, snmpget, named, netbus* dan *imap.* Pola serangan berupa atribut- atributdari hasil *feature extraction.* Langkah awal untuk mencari pola serangan adalah memasukkan *file capturedataset* ke *tool IDS snort,* hasil *alert* dari *snort* kemudian dibandingkan dengan hasil *feature extraction* untuk mencari atribut yang dapat dijadikan pola serangan R2L.

*C. Clustering*

Pada tahap ketiga ialah melakukan *clustering k- means.* Tujuan dari tahap ini adalah mengelompokkanserangan *remote to local* kedalam *cluster-cluster,* pada percobaan ini akan menghasilkan enam *cluster* yaitu *cluster ftp_write, cluster snmpget, cluster imap, cluster named, cluster netbus* dan *cluster* normal. Padapercobaan *clustering* ditetapakan bahwa *centroid* awal berupa pola serangan *remote to local* yang sudah didapatkan.

*D. Visualisasi*

Tahapan terakhir adalah bagaimana visualisasi dari hasil *clustering* kedalam bentuk grafik yang mudah dipahami oleh user. Teknik untuk visualisasi menggunakan *parallel coordinates,* dimana setiap cordinat yang berupa garis vertikal mempresentasikan setiap parameter dari pola serangan. Parameter yang divisualisasikan, pertama *ip source,* kedua *ipdestination,* ketiga *source port,* keempat *destination port,* kelima *ip length* dan keenam adalah *tcp/udp length.* Keenam parameter ini memungkinkanmembentuk aliran garis yang akan diplot pada parallel coordinates.

## IV. HASIL DAN PEMBAHASAN

*a) Pola Serangan*

Pada gambar 1 (b) adalah bagaimana cara unutkmendapatkan pola serangan *remote to local.* Dari hasil percobaana tribut -atribut unik yang dapat digunakan untuk mendeteksi serangan *remote to local* dapat dilihat pada tabel 2.

**TABEL 2**

Pola Serangan *Remote to Local*

| **Jenis Serangan** | **Atribut** | | | | |
|---|---|---|---|---|---|
| | **Sport** | **Dport** | **Flags** | **IPLen** | **PaketLen** |
| *Snmpget* | √ | 161 | - | 132 | 112 |
| *Imap* | √ | 143 | PA | 1336 | 1316 |
| *Ftp_write* | √ | 21 | - | 56 | 36 |
| *Named* | √ | 53 | PA | 42-45 | 22-25 |

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

| | | | | | |
|---|---|---|---|---|---|
| *NetBus* | √ | √ | PA | 48 | 28 |

*b) Clustering*

Tahap *clustering* bertujuan untuk mengelompokkanserangan R2l kedalam *cluster-cluster.* Pada tabel 3 dapat dilihat hasil *clustering* dari dataset DARPA pada minggu ke-4, dimana serangan *ftp_write* adalah serangan yang paling banyak terjadi pada setiap harinya.

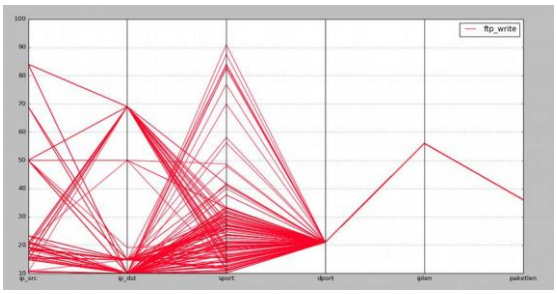
**TABEL 3**

*Pola Serangan Remote to Local*

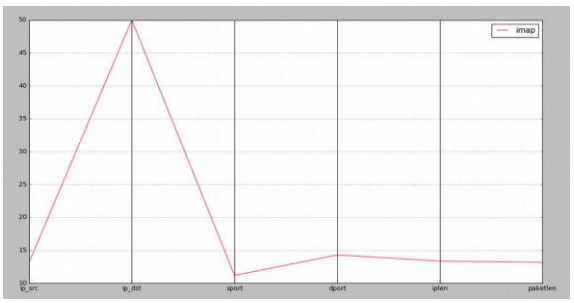
| **Hari_** | ***imap*** | ***ftp_write*** | ***named*** | ***snmpget*** | ***Cluster*** ***netbus*** | ***other*** |
|---|---|---|---|---|---|---|
| Hari ke-1 | 0 | 207 | 0 | 0 | 0 | 1580545 |
| Hari ke-2 | 0 | 126 | 0 | 231 | 0 | 1231399 |
| Hari ke-3 | 1 | 222 | 8 | 163 | 0 | 1237432 |
| Hari ke-4 | 0 | 154 | 1 | 1216 | 4 | 1557874 |
| Hari ke-5 | 0 | 146 | 4 | 0 | 3 | 1241638 |

*c) Visualisasi Serangan Remote to Local*

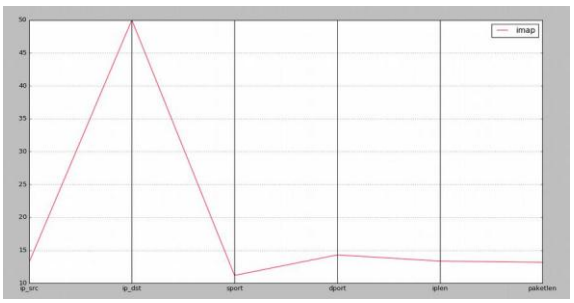
*Parallel coordinates* merupakan salah satu teknik yang dapat digunakan untuk visualisasi, kelebihan dari *parallel coordinates* dapat memprentasikan beberapaparameter kedalam bidang dua dimensi. Pada gambar 2 merupakan hasil visualisasi gabungan beberapa serangan *remote to local,* dimana setiap serangan membentuk aliran pola yang berbeda. Gambar 3 menunjukkan pola serangan *ftp_write* dimana dari banyak *source address* menuju ke port 21 dan besar paketnya kurang dari 60 byte. *Imap* adalah serangan *remote to local* yang paling sedikit terjadi dalam datasetDARPA, gambar 4 memgambarkan pola dari serangan *imap.* Pada gambar 5 adalah pola serangan *named,* dimana serangan ini mengeksploitasi *vulnerability* pada server BIND dan pada gambar 6 merupakan hasil visualisasi serangan *netbus, netbus* adalah sebuah program *backdoor* untuk *remote* komputer korban. Terakhir, *snmpget* ialah serangan *remote to local* yang mencoba untuk mengakses sebuah perangkat *router,* pada gambar 7 adalah hasil visualisasi serangan *snmpget* yang ada dataset DARPA.



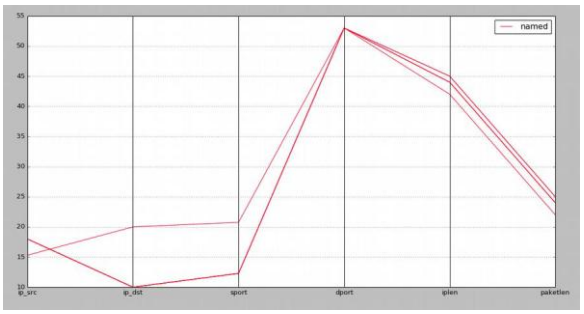

Gambar 2. Serangan *remote to local*




Gambar 3. Serangan *ftp_write*

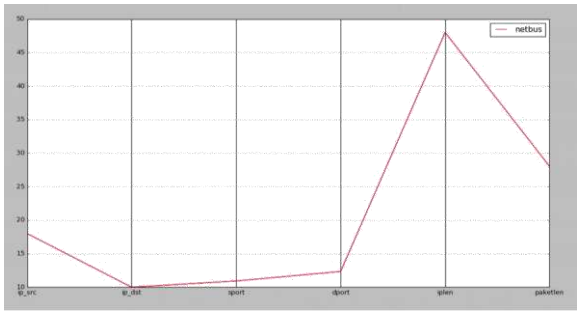



Gambar 4. Serangan *imap*

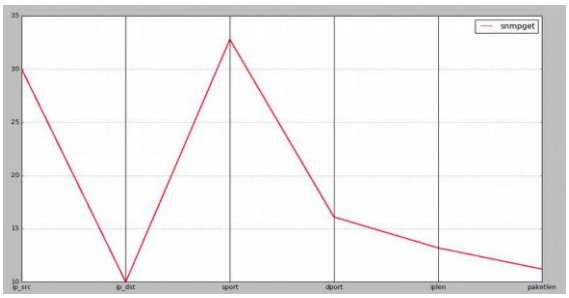



Gambar 5. Serangan *named*

ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id




Gambar 6. Serangan *netbus*




Gambar 7. Serangan *snmpget*

## V. KESIMPULAN DAN SARAN

Pada naskah ini mempresentasikan tentang bagaimana memvisualisasikan serangan *remote to local,* dengan menggunakan teknik *clustering k-means* untuk mendeteksinya. Kesimpulan dari hasil percobaan yaitu sebagai berikut :(i) Algoritma *clustering k-means* dapat diterapkan pada IDS untuk mendeteksi serangan *remoteto local.* (ii) Atribut-atribut unik pada paket *header* dapat digunakan sebagi pola serangan untuk mengenali paket serangan *remote to local* berupa *port destination,flags, ip length* dan *packet length.* (iii) Visualisasi dapatmempermudah untuk menggenali serangan *remote tolocal.*

Percobaan selanjutnya yang dapat dilakukan antara lain : (i) menerapkan teknik visualisasi kelingkungan *real-time.* (ii) menerapkan teknik deteksi yang lainuntuk mencari yang terbaik.

## DAFTAR PUSTAKA

[1] H. D. Yanping Zhang, Yang Xiao, Min Chen, Jingyuan Zhang, "A survey of security visualization for computer network logs," *Secur. Commun. NETWORKS*, vol. 9, no. 22, pp. 5:404–421, 2012.

[2] V. Kumar, H. Chauhan, and D. Panwar, "K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detectionm Dataset," *Int. J. Soft Comput. Eng.*, vol. 3, no. 4,pp. 1–4, 2013.

[3] H. Choi, H. Lee, and H. Kim, "Fast detection and visualization of network attacks on parallel coordinates," *Comput. Secur.*, vol. 28, no. 5, pp. 276–288, 2009.

[4] R. Sánchez, Á. Herrero, and E. Corchado, "Visualization and Clustering for Snmp Intrusion Detection," *Cybern. Syst.*, vol. 44, no. 6–7, pp. 505–532, 2013.

[5] A. Mohammed, M. Ghaleb, and S. A. Talab, "Assembly Classifier Approach to Analyze Intrusion Detection Dataset in Networks by Using Data Mining Techniques," vol. 4, no. 4, pp. 742–748, 2015.

[6] Z. Dewa and L. A. Maglaras, "Data Mining and Intrusion Detection Systems," vol. 7, no. 1, pp. 62–71, 2016.

[7] H. T. SONG, Jungsuk, "A Generalized Feature Extraction Scheme to Detect 0-Day Attacks via IDS Alerts," *Int. Symp.Appl. Internet A*, pp. 55–61, 2008.

[8] M. E. Celebi, H. A. Kingravi, and P. A. Vela, "A comparative study of efficient initialization methods for the k-means clustering algorithm," *Expert Syst. Appl.*, vol. 40, no. 1, pp. 200–210, 2013.

[9] M. N. Mohammad, N. Sulaiman, and O. A. Muhsin, "A novel intrusion detection system by using intelligent data mining in weka environment," *Procedia Comput. Sci.*, vol. 3, pp. 1237–1242,2011.