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 Brute Force Menggunakan Metode K-Means dan Naïve Bayes

Sari Sandra
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera, Indonesia
09121001005@students.ilkom.unsri.ac.id

Deris Stiawan
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera, Indonesia
deris@ unsri.ac.id

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

Abstrak—Penelitian ini menyajikan visualisasi dalam bidang two dimensional (2D) untuk mengkategorikan paket ISCX dan DARPA dataset. Paket data akan dibedakan dalam dua kategori yaitu paket data attack dan paket data normal berdasarkan pattern serangan brute force. Serangan bruteforce melakukan penyerangan pada beberapa layananprotokol seperti secure shell (SSH) dan telecommunicationnetwork (Telnet). Pada ISCX dataset serangan brute force terjadi pada layanan SSH , sedangkan DARPA dataset terjadi pada layanan TELNET. Metode K-Means dan metode Naïve Bayes diimplementasikan pada penelitian ini untuk mendapatkan hasil pengkategorian yang efektif Hasil akhir dari penelitian menunjukkan metode yang digunakan mendapatkan hasil yang baik dalam hal accuracy dengan mengurangi false alarm yang terjadi.

***Kata Kunci—Visualisasi, ISCX dataset, DARPA dataset,Brute force, Metode K*-Means dan Metode Naïve Bayes**

I. PENDAHULUAN

Salah satu teknik, serangan yang paling umum digunakan oleh para penyerang *(attacker)* adalah *brute force attack* dengan persentase serangan mencapai 25% dibawah serangan *Denial ofService* (DoS) [1], [2], [3]. Pada serangan *brute force, attacker* mencoba untuk *login* menggunakan protokol SSH dan telnet untuk mengungkapkan *password login* [2]. Protokol ini memungkinkan pertukaran data antara dua perangkat jaringan, yang banyak digunakan pada sistem berbasis *Linux* dan *Unix* [4].

Secara garis besar *brute force* dapat diklasifikasikan dalam dua kategori dalam menganalisa pola paket serangan, yaitu kategori paket data *attack* dan kategori paket data normal. Kategori pola *brute force attack*, dapat dilakukan dengan memanfaatkan metode K-Means dan metode Naïve Bayes yang berasal dari algoritma *data mining* untuk *intrusion detection* [5]. Metode K-Means dan metode Naïve Bayes akan mengkategorikan data dari himpunan data yang ada dengan tujuan akhir memberikan hasil visual terhadap serangan yang terjadi pada *dataset*.

Paper ini berisi beberapa bagian antara lain, bagian 2 memberikan penjelasan berupa penelitian terkait bidang yang dibahas. Bagian 2, memberikan penjelasan berupa metodologi penelitian. Bagian 3, menjelaskan hasil dari penelitian, dan bagian 4 menyimpulkan hasil penelitian serta memberikan saran untuk penelitian selanjutnya.

II. PENELITIAN TERKAIT

Pada penelitian [6] tahun 2013, membahas mengenai pendeteksian serangan *brute force* SSH dalam lalu lintas jaringan

Lawrence Berkeley National Laboratory (LBNL), sebuahlaboratorium penelitian nasional US. Penelitian tersebut menunjukkan terdapat perubahan secara signifikan dalam protokol SSH ketika serangan *brute force* terjadi.

Dalam studi lain [7], membahas mengenai *intrusiondetection dataset* menggunakan algoritma K-Means *clustering*.Penelitian ini mencoba untuk *clustering dataset* menjadi kategori normal dan kategori serangan yaitu DOS, Probe, R2L dan U2R. Akan tetapi, penelitian ini hanya menggunakan NSL-KDD *dataset* untuk *clustering dataset.*

Selain penggunaan algoritma K-Means, terdapat algoritma Naïve Bayes yang dapat digunakan dalam mengidentifikasi *intrusion detection*, seperti pada penelitian [8]. Penelitian ini membahas mengenai penggunaan algoritma K-Means dan Naïve Bayes untuk mengatasi *false alarm* dengan menggunakan ISCX *dataset.*

Pada penelitian [9], membahas mengenai pendeteksian secara otomatis suatu *attack* menggunakan *Parallel CoordinateAttack Visualization (PCAV).* Penelitian ini, mendeteksi *attack internet* dalam skala besar seperti *internet worms, DDOS* dan *network scanning.*

Selanjutnya penelitian [10], membahas pendeteksian serangan untuk mengevaluasi kinerja sistem tanpa *monitoring* dalam mendeteksi anomali. Penelitian ini menggunakan KDD Cup 1999 *dataset* dengan algoritma K-Means *clustering.*

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

Namun, penelitian ini memanfaatkan *cluster 3.0 tool* dan *TreeViewvisualization tool.*

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode K-Means dan Naïve Bayes dalam mengkategorikan pola paket berupa pola paket serangan atau pola paket normal pada ISCX dan DARPA *dataset.* Penggunaan kedua metode tersebut, diharapkan dapat mewujudkan sistem dengan memberikan gambaran visual dalam mengkategorikan serangan *brute force* dengan akurasi pendeteksian serangan yang baik.

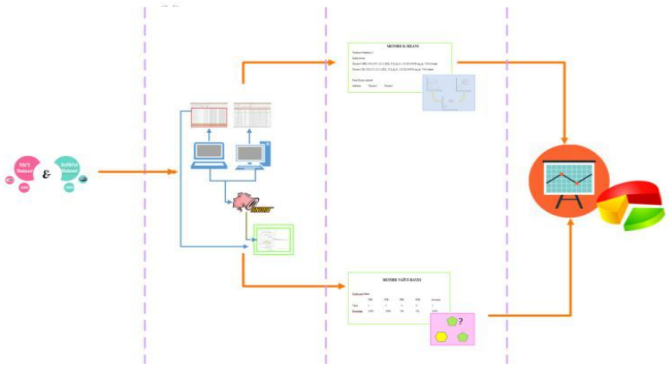
Selain itu, penelitian ini menggunakan perangkat lunak untuk mendukung sistem yang dipakai pada penelitian. Berikut, spesifikasi kebutuhan perangkat lunak yang dijelaskan pada tabel 1.

Tabel 1. Spesifikasi Kebutuhan Perangkat Lunak

Sistem	***Tools***	**Keterangan**
NIDS SSH dan TELNET	Snort	Versi 2.9.8.0
Attack Pattern dan *Normal Pattern*	Visual Studio	2012
Visualisasi	Visual Studio	2012

Pada tabel 1, diketahui bahwa perangkat lunak yang digunakan berupa snort dan visual studio. Snort digunakan sebagai NIDS (Network Intrusion Detection System) dalam mendeteksi serangan brute force pada layanan SSH dan TELNET, sedangkan visual studio digunakan sebagai sistem Attack Pattern dan NormalPattern serta digunakan untuk visualisasi paket data.

Kami memberikan gambaran dalam memvisualisasikan serangan brute force pada gambar 1, berikut ini.



Gambar 1. Tahapan Penelitian, dengan label (A)*dataset*, (B)*attack pattern* dan *normal pattern,* (C) metode K-Means dan Naïve Bayes dan (D) visualisasi

Pada gambar 1, diketahui bahwa tahapan awal pada penelitian ditunjukkan pada label (A), berupa penelitian pada dataset, kemudian dataset tersebut akan diolah pada tahapan attack pattern dan normal pattern yang ditunjukkan pada label (B). Padatahapan attack pattern dan normal pattern digunakan tool snort dan traceroute untuk validasi dataset. Tahapan selanjutnya merupakantahapan pada label (C) berupa penggunaan metode K-Means dan Naïve Bayes pada dataset sehingga, didapatkan hasil visualisasi dengan akurasi pendeteksian yang baik pada tahapan penelitian dengan label (D). Berikut merupakan penjelasan lebih terperinci dari setiap tahapan penelitian yang dilakukan :

3.1. Dataset

Dataset yang digunakan dalam penelitian adalah ISCX *dataset* dan DARPA *dataset* dalam format CSV (*Comma Separated Values*). ISCX *dataset* merupakan *dataset* yangdigunakan untuk meng-*capture* lalu lintas jaringan yang dikembangkan oleh Fakultas Ilmu Komputer, Universitas New Brunswick [11]. ISCX *dataset* mensimulasikan skenario serangan *infiltrating the network from the inside,* HTTP *denial of service, distributed denial of service an* IRC *Botnet* dan *brute force* SSHpada tanggal 11-17 Juni 2010.

ISCX *dataset* dalam penelitian hanya berfokus pada satu skenario serangan yaitu *brute force* pada tanggal 17 Juni 2010 di layanan *secure shell* (SSH) yang terdiri dari 20 *features* dengan 5540 *packets*. SSH menyediakan *service remote log-in* yang cukup aman serta memiliki sistem otentikasi dan otorisasi, sehingga untuk mengakses *service* ini dibutuhkan *log-in* yang dapat menyebabkan terjadinya serangan dengan teknik *brute force.* Layanan SSH merupakan bagian dari protokol TCP.

Berbeda pula, dengan DARPA *dataset* dimana serangan *brute force* terjadi pada layanan *telecommunication network*

(TELNET) *detection* yang terdiri dari 42 *features* dengan 1234 *packets*. Telnet tidak menggunakan mekanisme keamanan berupasistem otentikasi dan teknik enkripsi serta transfer data dalam bentuk *plain-text,* sehingga informasi menjadi ancaman besar dalam jaringan.

DARPA *dataset* dikumpulkan pada tahun 1998 dan 1999 oleh *Information Systems Technology group of MIT LincolnLaboratory,* dibawah *Defense Advanced Research Projects Agency (DARPA)* dan *Air Force Research Laboratory (AFRL/SNHS) sponsorship* [12]. DARPA diciptakan guna mensimulasikan *traffic* di pangkalan Angkatan Udara AS untuk mengevaluasi sistem *intrusion detection.*

3.2. Attack Pattern dan Normal Pattern

Attack pattern dan *normal pattern* pada penelitian,menggunakan suatu program *matching* dalam menentukan *bruteforce pattern.* Hasil dari program *matching* berupa paket dominan *attack* dan normal dalam *dataset* yang akan menjadi *preprocess* pada penelitian selanjutnya.

Tool snort juga digunakan pada tahapan ini untukmembuktikan bahwa benar pada ISCX dan DARPA *dataset* terdapat serangan *brute force. Snort* dapat bekerja

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

dalam 4 mode, yaitu *sniffer, packet logger, Network Intrusion Detection System*

(NIDS) dan *Intrusion Prevention System* (IPS) [13]. Snort mode NIDS yang digunakan dalam penelitian ini, dengan *setup* dari berbagai *rules* berdasarkan *rule options* untuk mendeteksi serangan sehingga dapat membedakan sebuah paket normal dan paket serangan.

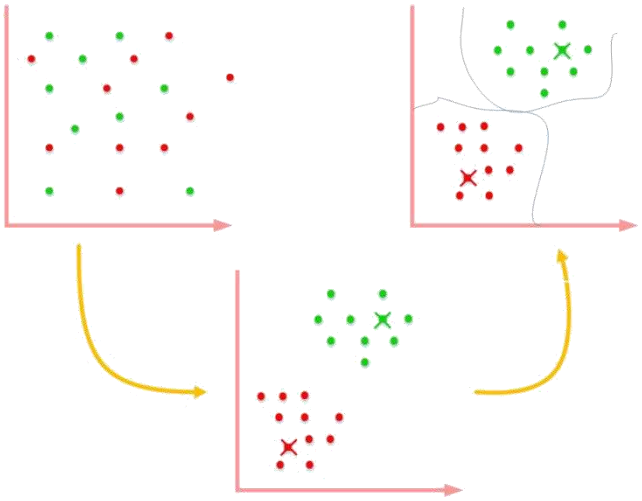
Selain program *matching* dan *tool* snort, pada tahapan ini dilakukan *traceroute* untuk mengetahui rute yang dilalui oleh *attacker* untuk mencapai *server* dalam melakukan aksiserangannya. *Traceroute* juga berguna dalam membuktikan bahwa benar pada ISCX dan DARPA *dataset* terdapat host *client* dan *server* tertentu.

3.3. Metode K-Means dan Naïve Bayes

Metode K-Means merupakan salah satu metode data *clustering* non-hirarki yang mengelompokkan data dalam bentuksatu atau lebih *cluster* [14]. Pada metode K-Means, dihitung jarak tiap data ke tiap *cluster* dengan menggunakan *Euclidean Distance* sebagai berikut:

$$(,) = \sqrt{\sum =1(\ - \ )2 \ ; } = 1, 2,3, \ldots \quad \ldots\ldots..(1)$$

Pada penelitian ini, banyaknya jumlah *cluster* (k) adalah dua, untuk membedakan kategori paket data *attack* dan kategori paket data normal. Berikut gambar 2, yang menunjukkan ilustrasi dari metode K-Means.



Gambar 2. Ilustrasi Metode K-Means (A) banyak*cluster*dari*dataset*, (B) inisialisasi *centroid*, (C) pengkategorian *dataset*

Metode *Naïve Bayes* juga digunakan pada penelitian ini, untuk mengelompokkan paket data dalam pengenalan pola (patternrecognition). *Naïve Bayes* memiliki kecepatan dan akurasi yangtinggi ketika diaplikasikan pada sebuah data yang besar [15]. Naïve Bayes didasarkan pada teorema *Bayes* memiliki persamaan sebagai berikut.

$$P (H \mid X) = \frac{P (H) P (X \mid H)}{P(X)} \quad \ldots\ldots..(2)$$

Metode *Naïve Bayes* akan mengkategorikan suatu data kedalam kategori tertentu berdasarkan probabilitas posterior P(H | X) tertinggi. Klasifikasi suatu data akan terjadi jika dan hanya jika *posterior probability* data H berdasarkan kondisi X {P (H | X)} lebih kecil dariposterior probabilitydata Hberdasarkan kondisi X { P (H | X }

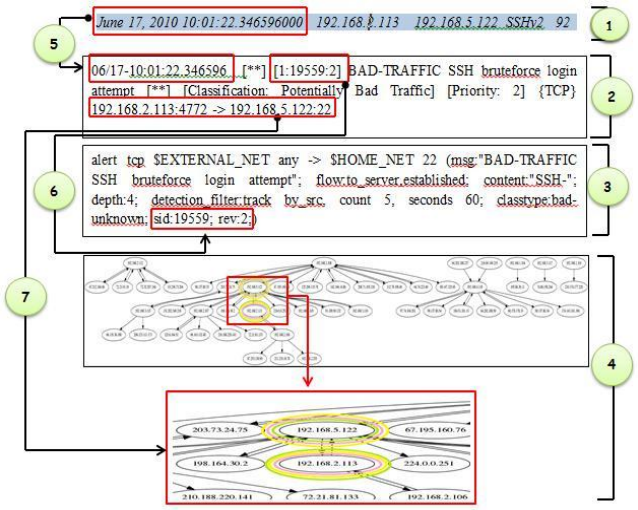
$$P (H \mid X) > P (H \mid X) \quad \ldots\ldots..(3)$$
dimana, j ≥ 1 dan j≠ i

3.4. Visualisasi

Pada penelitan, visualisasi akan menggambarkan suatu pola *(pattern)* dari paket *attack* dan paket normal pada ISCX dan DARPA *dataset* dengan desain visualisasi *parallel coordinate.* Visualisasi *parallel coordinate* menggambarkan suatu informasi dalam bidang *two dimensional* (2D).

IV. HASIL DAN PEMBAHASAN

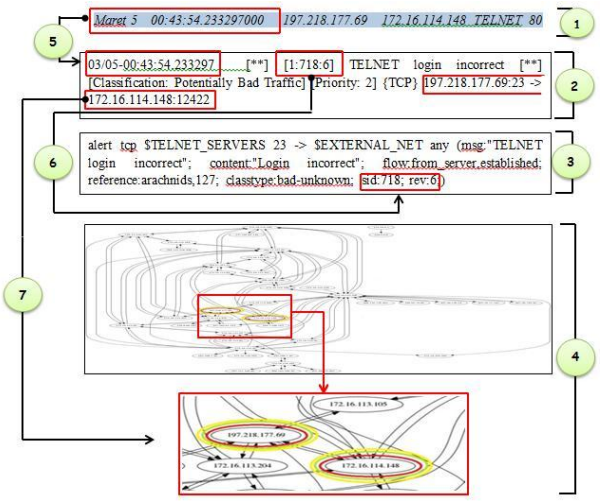
Pada awal penelititan, dilakukan proses validasi setiap *dataset* (ISCX dan DARPA *dataset*) dalam mendeteksi paket data *attack* dan paket data normal yang membentuk suatu korelasi data
terhadap paket data dengan *engine* IDS serta *traceroute*. Hasil dari proses validasi data tersebut, ditampilkan pada gambar 3 dan gambar 4 berikut ini.



Gambar 3. Korelasi ISCX*Dataset*

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

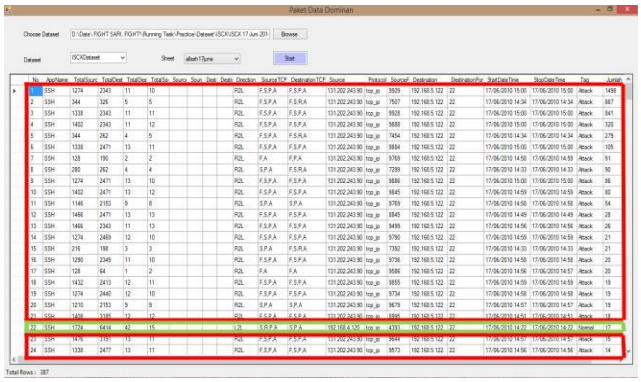
ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id



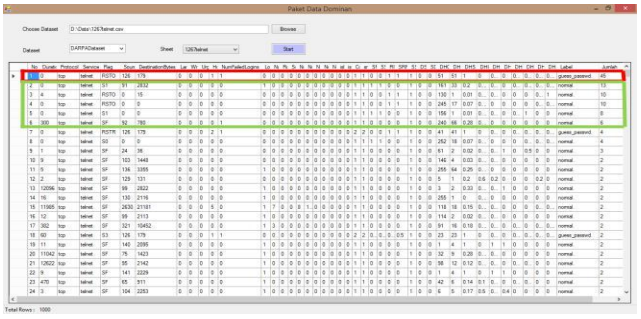
Gambar 4. Korelasi DARPA*Dataset*

Pada gambar 3 dan gambar 4, bagian pertama mendeskripsikan packet list dengan data packet capture (pcap) yang berisi informasi mengenai time, source, destination, protocol dan data length. Bagian kedua merupakan contoh alert dari snort engine IDS yang mendeskripsikan hasil deteksi serangan. Bagianketiga menunjukkan salah satu model rules yang digunakan dalam mendeteksi serangan. Bagian keempat mendeskripsikan traceroute berupa host source dan host destination. Bagian kelima membuktikan korelasi dari data pengujian berdasarkan kecocokkan time antara paket data dengan alert yang terdeteksi pada hasilpengujian. Bagian keenam menunjukkan korelasi data dari alert yang terdeteksi pada hasil pengujian dengan salah satu model rules berdasarkan GID (Generator ID), SID (Signature ID) dan revision number dan bagian ketujuh merupakan korelasi data antara alert snort dengan traceriutr berdasarkan kecocokkan host.

Hasil penelitian selanjutnya merupakan hasil penelitian dari tahapan attack pattern dan normal pattern. Berikut, gambar 5 dan gambar 6 yang memberikan hasi dari penelitian attack pattern dan normal pattern pada setiap dataset.



Gambar 5.*Attack Pattern*dan*Normal Pattern*ISCX*Dataset*



Gambar 6.*Attack Pattern*dan*Normal Pattern*DARPA*Dataset*

Gambar 5 menunjukkan attack pattern dan normalpattern dominan pada ISCX dataset yang memiliki nilai dominanberjumlah 1498 dan 17 paket data. Attack pattern dominan memiliki features “TotalSourceBytes” bernilai 1274, features“TotalDestinationBytes” bernilai 2343 features “TotalDestinationPackets” bernilai 11 features “TotalSourcePackets” bernilai 10 dengan features “Direction” adalah R2L serta features“SourceTCPFlagsDecription” dan features “Destination-TCPFlagsDecription” adalah F,S,P,A. Selain itu, pada “Tag” attack diketahui bahwa source IP yang dominan merupakan IP 131.202.243.90 dengan tujuan IP server adalah 192.168.5.122, dimana IP server tersebut merupakan IP dari main server ISCX yang bertanggung jawab untuk memberikanlayanan e-mail sehingga memungkinkan terjadinya serangan bruteforce pada IP server tersebut.

Sedangkan, normal pattern pada gambar 5 memiliki data dominan dengan features “TotalSourceBytes” bernilai 1724, features “TotalDestinationBytes” bernilai 6414 features “TotalDestinationPackets” bernilai 42 features “TotalSourcePackets” bernilai 15 dengan features “Direction” adalah L2L dan features“SourceTCPFlagsDecription” adalah S,R,P,A serta features “Destination-TCPFlagsDecription” adalahS,P,A dengan IP source berasal dari 192.168.4.120 dan IP destination 192.168.5.122.Gambar 6 menunjukkan attack pattern dan normalpattern pada DARPA dataset. Attack pattern dominan dengan“Label” guess_passwordmerupakan data denganfeatures“Protocol” adalah TCP, features “Service” adalah TELNET, features “Flags” adalah RSTO, features “DurationBytes” bernilai179 serta features“Num_Failed_logins” bernilai 1. Data dominan ini, merupakan data yang akan menjadi pola dari serangan bruteforce TELNET dengan jumlah dominan data mencapai 45 rows. Sedangkan, normal pattern dominan memiliki nilai dominan berjumlah 13. Data tersebut merupakan data dengan features“Protocol” adalah TCP, features “Service” adalah TELNET, features “Flags” adalah S1, features “DurationBytes” bernilai 2832 serta features“Num_Failed_logins” bernilai 0.

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

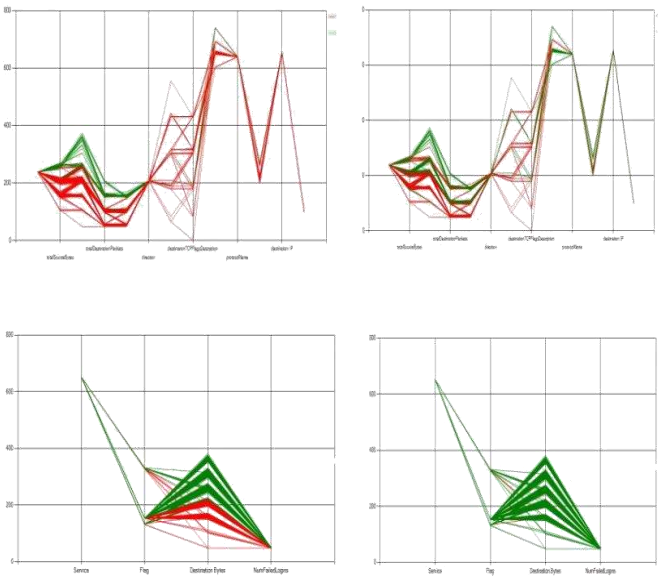
Tahapan penelitian selanjutnya merupakan tahapan pengunaan metode K-Means dan Naïve Bayes pada dataset. Hasil penelitian berdasarkan metode pada setiap dataset, didapatkan suatu serangan yang dikategorikan normal oleh metode K-Means dan Naïve Bayes. Berikut, merupakan hasil penelitian penggunaan metode K-Means dan Naïve Bayes dalam bentuk confusion matrix yang ditunjukkan pada Tabel 2.

Tabel 3. *Confusion Matrix*dengan*Attack*dan*Normal Pattern*

Metode	*Dataset*	Hasil Kategori				
		TP	**TN**	**FP**	**FN**	***Accuracy***
K-Means	*ISCX*	5197	92	245	6	95.46
	DARPA	52	857	325	1	73.60
Naïve Bayes	*ISCX*	5185	337	18	0	99,68
	DARPA	51	1169	13	2	98,79

Dari tabel 3, dapat diketahui bahwa hasil kategori paket dataset dengan menggunakan metode Naïve Bayes mendapatkan accuracy lebih besar dibandingkan dengan metode K-Means. Accuracy netode Naïve Bayes pada ISCX dan DARPA dataset didapatkan persentaste accuracy 99,68% dan 98,779%, sedangkan, metode K-Means pada ISCX dan DARPA dataset didapatkan persentaset 95,46 % dan 73,60% Selain itu, metode Naïve Bayes mendapatkan false alarm yang lebih kecil dibandingkan dengan metode K-Means.

Selanjutnya. pembentukan visualisasi parallel coordinate dapat diimplementasikan kedalam program attack dan normalpattern pada ISCX dan DARPA dataset, ketika tahapan penelitianmenggunakan metode telah dilakukan . Berikut screenshot aplikasi visualisasi parallel coordinate yang disajikan pada gambar 8.



Gambar 8. Visualisasi*Parallel Coordinate*

Gambar 8 menunjukkan visualisasi parallel coordinate dengan label (A) merupakan visualisasi parallel coordinate ISCX dataset dengan menggunakan metode K-Means clustering. Line berwarna merah merupakan attack dengan kategori termasuk cluster 0, sedangkan line hijau merupakan kategori cluster 1 yaitunormal. Label (B) merupakan visualisasi DARPA dataset menggunakan metode Naïve Bayes dengan line merah merupakan kategori cluster 0 yaitu attack dan line hijau merupakan normal yang termasuk kedalam kategori cluster 1. Label (C) memberikan hasil visualisasi parallel coordinate ISCX dataset dengan menggunakan metode Naïve Bayes. Line yang berwarna hijau merupakan paket data yang termasuk kedalam kategori normal, sedangkan line berwarna merah merupakan paket data attack. Label (D) menunjukkan hasil visualisasi DARPA dataset dengan menggunakan metode Naïve Bayes dengan paket data yang dominan termasuk kedalam kategori normal.

V. KESIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa serangan *brute force* pada ISCX *dataset di* layanan SSH membentuk suatu pola serangan dimana satu IP *source* yang fokus melakukan serangan ke satu *server, dengan* port *destination* yang akan di-*exploit* adalah port 22 Sedangkan,serangan *brute force* pada layanan TELNET didapatkan suatu bentuk pola serangan dimana IP *attackers* mengalami *failed logins* dengan nilai minimal 1 dengan port

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

destination yang akan di-*exploit* adalah port 23 serta *destination bytes* yang terjadi adalah179 *bytes*.

Metode K-Means dan metode Naïve Bayes dapat diimplementasikan pada *dataset* dalam mengkategorikan sejumlah paket data *attack* atau paket data normal berdasarkan *attack* dan *normal pattern*. Hasil akhir dari implementasi kedua metode dapatmemberikan visualisasi dalam bidang *two dimensional* (2D), berupa visualisasi *scatter plot* atau *parallel coordinate,* dengan *accuracy* pengkategorian yang baik. Metode K-Means dan metode Naïve Bayes yang diimplementasikan pada ISCX *dataset* mendapatkan hasil *accuracy* hingga 95,46% dan 99,68%, sedangkan pada DARPA *dataset* didapatkan nilai *accuracy* 73,60% dan 98,79%.

Penelitian selanjutnya, dapat melakukan visualisasi serangan secara *real time* dengan penambahan jenis serangan seperti SQL *injection, probe, internet worms* dan *networkscanning.*

VI. PENGHARGAAN

Penelitian ini didukung oleh Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya serta laboratorium COMNETS research.

DAFTAR PUSTAKA

1 D. Dede, “Most Common Attacks Affecting Today ’ s Website,” *Sucuri Blog*, 2014. [Online]. available:https://blog.sucuri.net/2014/11/most-common-attacks-affecting-todays-websites.html. [Accessed: 20-May-2016].

2. M. M. Najafabadi, T. M. Khoshgoftaar, C. Kemp, N. Seliya, and R. Zuech, “Machine learning for detecting brute force attacks at the network level,” *Proc. - IEEE 14th Int. Conf. Bioinforma. Bioeng.BIBE 2014*, pp. 379–385, 2014.

3. Calyptix, “Follow us ork Attack Types in 2015,” 2015. [Online]. Available: http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/. [Accessed: 20-May-2016].

4. E. Haryanto, “Meningkatkan Keamanan Port SSH dengan Metode Port Knocking Menggunakan Shorewall Pada Sistem Operasi Linux,” *Journal of Chemical Information and Modeling*, vol. 53, no. 9. pp. 1689–1699, 2013.

5. V. Kumar, H. Chauhan, and D. Panwar, “K-Means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset,”*Int. J.Soft Comput. Eng.*, vol. 3, no. 4, pp. 1–4, 2013.

6. W. Brute and F. Report, “WordPress Brute Force Attacks,”*SucuriBlog*, 2016. [Online]. Available: https://sucuri.net/security-reports/brute-force/. [Accessed: 29-Feb-2016].

7. M. Kumagai, Y. Musashi, D. A. L. Roma??a, K. Takemori, S. Kubota, and K. Sugitani, “SSH dictionary attack and DNS reverse resolution traffic in campus network,” *Proc. - 3rd Int. Conf. Intell.Networks Intell. Syst. ICINIS 2010*, pp. 645–648, 2010.

8. W. Yassin, N. I. Udzir, and Z. Muda, “Anomaly-Based Intrusion Detection Through K- Means Clustering and Naives Bayes Classification,” *Proc. 4th Int. Conf. Comput. Informatics, ICOCI2013*, no. 49, pp. 298–303, 2013.

9. 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.

10. a M. Riad, I. Elhenawy, A. Hassan, and N. Awadallah, “V Isualize N Etwork a Nomaly D Etection B Y U Sing K- Means C Lustering a Lgorithm,” vol. 5, no. 5, pp. 195–208, 2013.

11. R. Zuech, T. M. Khoshgoftaar, N. Seliya, M. M. Najafabadi, and C. Kemp, “A New Intrusion Detection Benchmarking System,” *Proc.Twenty-Eighth Int. Florida Artif. Intell. Res. Soc. Conf.*, no.McHugh, pp. 252–255, 2015.

12. H. H. Jebur, M. A. Maarof, and A. Zainal, “Jurnal Teknologi Full paper Identifying Generic Features of KDD Cup 1999 for Intrusion Detection,” vol. 1, pp. 1–9, 2015.

13. K. S. A. Kahtani, “Improving Snort performance under Linux,” no. April, 2009.

14. Y. Agusta, “K-Means - Penerapan, Permasalahan dan Metode Terkait,” *J. Sist. dan Inform.*, vol. 3, no. Februari, pp. 47–60, 2007.

15. A. Jananto, “Algoritma Naive Bayes untuk Mencari Perkiraan Waktu Studi Mahasiswa P (H | X) P (X | H) P (H),” vol. 18, no. 1, pp. 9–16, 2013.