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 *Denial Of Service* Dengan *Clustering* Menggunakan *K-Means Algorithm*

Napsiah
Computer Engineering Department
Faculty of Computer Science
Sriwijaya University, Inderalaya 30662
South Sumatera Indonesia
09121001065@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*—Visualisasi menjadi salah satu solusi dalammenampilkan serangan di *network*. Dengan memvisulisasikan serangan, akan lebih mudah dalam mengenali dan menyimpulkan pola dari gambar visual yang komplek. Target serangan *DoS* bisa ditujukan ke berbagai bagian jaringan, bisa ke *routing, web, electronic mail* atau *server DNS* (*Domain NameSystem*). Tujuan dari serangan DoS membuat *server shutdown, reboot, crash* atau *not responding*. Pola serangan DoS padadataset ISCX membentuk sebuah pola dimana banyak nya *IPhost* yang hanya meng-*exploit* ke satu *server. Snort* mendeteksiadanya serangan *DoS* pada dataset ISCX *testbed* 14 juni sebanyak 42 *alert HttpDoS attac*k. Persentasi akurasi dari program*clustering* menggunakan algoritma *k-means* sebesar 97,83%, untuk *detection rate* nya sebesar 98,63%, dan *false alarm* dari program sebesar 0,02%. Sedangkan, nilai persentase akurasi dari *clustering* menggunakan algoritma *k-means* dengan *tool WEKA* sebesar 99,69%, *detection rate* 99,01% dan *false alarm* sebesar 3,70%.**

Keywords— Visualisasi; DoS; *Clustering; K-means Algoritthm*

I. PENDAHULUAN

Teknik serangan yang sering dilakukan oleh attacker dalam melumpuh-kan sistem terbagi dalam beberapa macam, salah satu teknik serangan yang umum digunakan oleh *attacker* adalah *Denial of Service (DoS*). Serangan *DoS* menghasilkan kerusakan yang sifatnya persisten, artinya kondisi *DoS* akan tetap terjadi walaupun *attacke*r sudah berhenti menyerang, dan *serve*r akan kembali normal setelah di *re-start/reboot* [1].Serangan DoS mudah untuk diimplementasi, akan tetapi sulit untuk mencegah dan melacaknya.

Pada penelitian [2], [3], [4], [5] membahas permasalahan terhadap visualisasi serangan secara otomatis menggunakan *parallel coordinate attack visualization (PCAV).* Penelitian ini,mendeteksi serangan internet dalam skala besar yang tidak diketahui seperti internet *worms, DoS attack* dan aktifitas *network scanning*. *PCAV* menampilkan *traffic* jaringan padabidang koordinat paralel menggunakan informasi seperti *source IP address, destination IP address, source port* danpacket length. Penelitian [2], [5] menjelaskan, bahwa setiap jenis serangan secara signifikan membentuk pola yang unik. Pada penelitian [6], melakukan penelitian terhadap serangan *DoS* dengan cara mengklasifikasikan serangan menggunakan jaringan syaraf tiruan *LVQ (Learning Vector Quantization),* dengan menghasilkan tingkat keberhasilan yang tinggi untuk kondisi normal, *PING flood dan UDP flood*. Dengan demikian, penelitian akan difokuskan pada salah satu pendekatan yaitu *attack visualization* terhadap serangan *Denial of Service (DoS)* dengan *clustering* menggunakan *K-Means Algorithm*.

Dataset yang digunakan pada penelitian ini yaitu dataset *(Information Security Center of eXcellence) ISCX* yangdikembangkan oleh fakultas ilmu computer, *universitas newBrunswick* dari tahun 2009 sampai tahun 2011. Kumpulan datasimulasi yang terdapat pada dataset ISCX adalah infiltrasi jaringan dari dalam, *HTTPDoS, DDoS* menggunakan *IRCbotnet*, dan *brute-force SSH*.

II. METODOLOGI PENELITIAN

A. Pengenalan Pola Paket Data

Langkah pertama dalam pengenalan pola paket data adalah menganalisa antara skenario serangan dari dataset dengan hasil *traceroute*. Selanjutnya, akan dibandingkan dengan programperhitungan paket data yang dominan disetiap baris paketnya. Program perhitungan paket data dilakukan secara *off-line*, menggunakan dataset dalam format *csv* sebagai data inputan. Acuan perhitungan pada program berdasarkan daftar *features* yang terdapat pada dataset *ISCX* (tabel 1), dimana *features* ini diperoleh dari *extraction raw* paket data kedalam bentuk csv.

TABLE I. DAFTAR*FEATURES DATASET ISCX*

No	Nama *Features*	No	Nama *Features*
1	*appName*	11	*Source TCP flags*
2	*Total source bytes*	12	*Destination TCP flags*
3	*Total destination bytes*	13	*Source*
4	*total destination packet*	14	*Protocol name*
5	*Total source packet*	15	*Source port*
6	*Source payload as base 64*	16	*Destination*
7	*Source payload as base UTF*	17	*Destination port*
8	*Destination payload as base 64*	18	*Start date time*
9	*Destination payload as base UTF*	19	*Stop date time*
10	*Direction*		

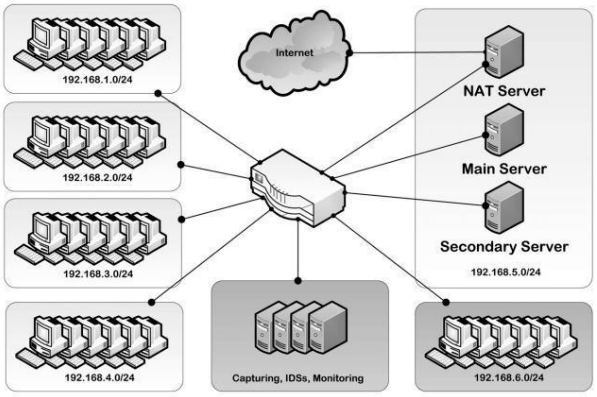
ISBN : 979-587-626-0 | UNSRI http://ars.ilkom.unsri.ac.id

B. Skenario Dataset ISCX

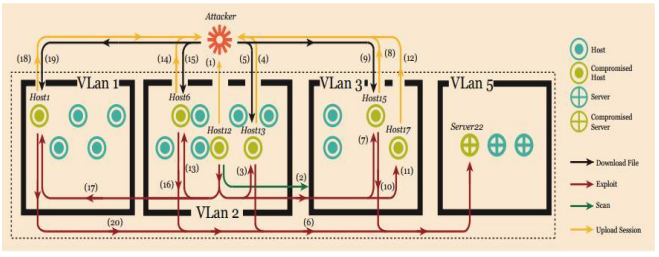
Dataset ISCX memiliki arsitektur jaringan testbed (gambar 1) yang terdiri dari 21 *windows workstation* yang saling berhubungan, dua mesin berbasis *linux Ubuntu* dan satu mesin diinstal *windows server* 2003. Tahapan dalam menghasilkan dataset ISCX terdiri dari empat elemen :

6.*Probe,* yang bertujuan untuk mengumpulkan informasi
7.*Identifikasi vulnerability*
8.*Mempertahankan* akses dengan menciptakan *backdoors*
9.*Kemampuan* untuk secara efektif menutupi jalur penyerangan.

Dataset ISCX yang digunakan dalam penelitian ini adalah hasil testbed 14 juni yang merupakan serangan *HTTPDoS*. Skenario serangan *HTTPDoS* (gambar 2) dirancang tanpa membanjiri jaringan, sehingga *bandwitdth* yang dibutuhkan rendah. ISCX memanfaatkan *slowloris* sebagai alat utama dalam skenario seranga *HTTPDoS*.



Gambar 1. Arsitektur Jaringan Testbed ISCX [7]



Gambar 2. Ilustrasi Skenario HTTPDoS Dataset ISCX [7], [8]

C. Perhitungan Paket Data Dominan

Pada tahapan pengenalan pola dari perhitungan paket data dominan menggunakan sebuah program yang akan melakukan *string matching* terhadap setiap paket data. Dari program inidapat dilihat bagaimana pola paket normal dan pola paket serangan *DoS*. Berikut *pseudocode* programnya :.

***Pseudocode** : Perhitungan Probability dari serangan Denial of Service (DoS) pada Dataset ISCX*

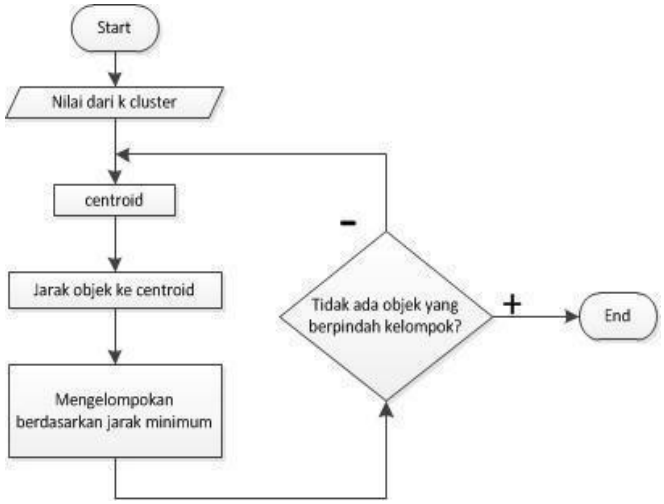
```
Input : dI
Output : Banyaknya kemungkinan
         HttpDoS attack

Step 1: Connect to
Database
for dataset connect with
   Microsoft Access
   P ←Microsoft.Jet.OLEDB.4.0
                pc = p + ds + ep + E
          End for

   Od conn = new Od(pc)

Step 2: proses data
if features= A
read dI
query ←SELECT*
count(StartDateTime)as
Jumlah from dI
where   appName=HTTPWeb
groupBy features
orderBy count DESC
End if

Step 3: fill data gridview
ODA myDA = new ODA(query,conn) DT
          dt ← new DT
myDA.fill(dt) dG.DS = dt
```

D. Clustering K-Means Algorithm

Langkah awal dari *k-means clustering* adalah menentukan nilai k sebagai jumlah *cluster* yang ingin dibentuk, kemudian mengasumsikan *k centroid* (titik pusat *cluster*) awal secara *random*. Langkah selanjutnya dari algoritma *k-means* yangharus dilakukan sampai objek benar-benar stabil (tidak ada objek yang berpindah kelompok) yaitu :

4 Menentukan koordinat *centroid*
5 Menentukan jarak dari masing-masing objek ke *centroid*
6 Mengelompokan objek berdasarkan jarak minimum (sampai menemukan *centroid* terdekat).

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



Gambar 3. Proses *Clustering K-means*

Dari pengolahan dataset ISCX 14 juni menggunakan program pengenalan pola paket data dominan, maka dari data tersebut diambil secara acak *centroid* awal untuk data normal dan data serangan sebagai pola dalam meng-*cluster* data pada algoritma *K-means.* Selanjutnya dilakukan perhitungan jarak antara paket satu dan paket lainnya menggunakan rumus *Euclidean distance* [9], [10]. Berikut pseudocode dari program *clustering* menggunakan algoritma *K-means* :

Pseudocode : Program clustering menggunakan algoritma k-means pada Dataset ISCX 14 juni

```
Input : F = {m1,m2,…mn} #dataset ISCX
        K = banyak cluster
        pola={p1,p2,….,pn}
Output : dos = cluster attack
           normal = cluster normal
for p1€ pola do
           p1 ← mn€ F
end
  def kmeans do
          a (m1) ← sqrt (mn - p1)2 n € {1…n}
                    return a
  end

  def hitung centroid baru do
              h (m1) ← i/len (cluster)
                    return h
  end

centroidbaru  ←  none
cluster ← [ ]
i77 ← none
  while pola !=centroidbaru
                 i77+1
                 i++
  for i in range (len(F))
      for h in range (len(cluster_atttack))
      for k in range(len(cluster_normal))
jarak ← kmeans (m1, p1)
if jarak = min(jarak) then
           cluster ← m1
end
polaupdate ← newcentroid(clusterattack)
          matrikattack ← polaupdate
polaupdate ←newcentroid(clusternorm)
          matriknormal ← polaupdate
end
```

Langkah berikutnya setelah melakukan *clustering* paket data adalah memvisualisasikan paket data tersebut kedalam dua *cluster* yaitu paket data *attack* dan paket data normal. Berikut *pseudocedo* p rogram visualisasi nya :

Pseudocode : Program visualisasi di *Dataset ISCX* 14 juni

```
Input:F
        cluster
Output : plot
  for cluster € Fdo
       cluster ← F
      cluster=attack   and   clsuter=normal
           Return plot
           Plot.show
end
```

III. HASIL DAN PEMBAHASAN

Visualisasi serangan DoS menggunakan clustering dengan algoritma k-mean diterapkan untuk mempermudah dalam mengenali pola serangan DoS. Sehingga, dengan cara memvisualisasikan akan lebih mudah dalam mengatasi serangan yang ada.

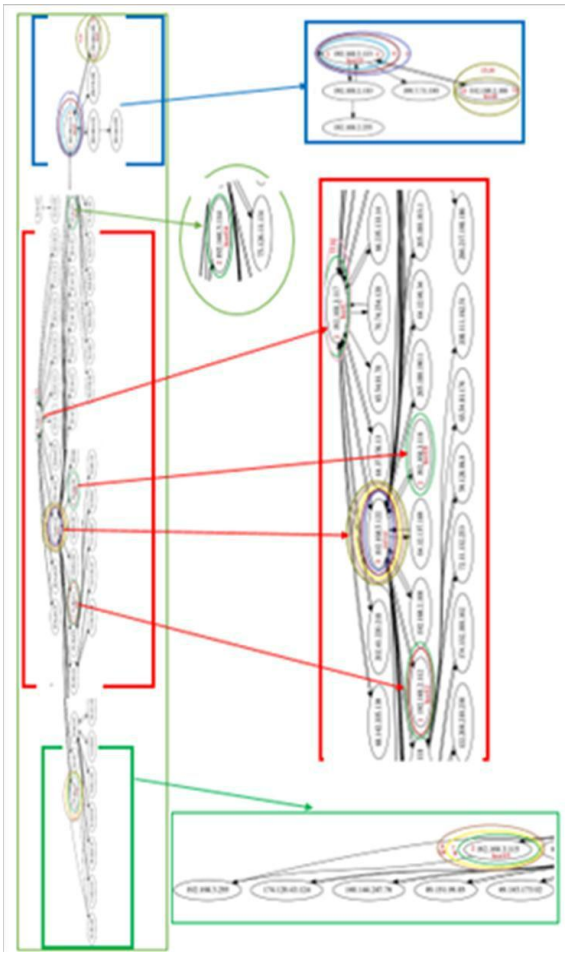
3.1. Pengujian Traceroute Dataset ISCX

Berikut gambar 4 akan menampilkan hasil dari *trace routedataset ISCX testbed* 14 juni. Hasil dari *traceroute* padagambar 4 beikut menunjukan, bahwa skenario dataset ISCX :

1. Dalam melakukan skenario serangan *HTTPDoS,attacker* memanfaatkan koneksi dari *host*
   a. 192.168.2.112, 192.168.2.113, 192.168.3.115,
   b. 192.168.3.117, 192.18.1.101 dan 192.18.2.106 yang bertindak sebagai penyerang untuk melakukan *exploitke IP server* 192.168.5.122 melalui backdoor.
2. Kemudian *attacker* melakukan koneksi dengan cara *upload session ke host*.

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

3. Selanjutnya host 192.168.2.112 melakukan scan terhadap host 192.168.2.113, 192.168.3.115 dan 192.168.3.117. Scan dilakukan untuk mengetahui vulnerability dari sistem agar dapat di exploit.
4. Setelah mengetahui vulnerability, maka attacker akan me-remote sistem yang kemudian dengan leluasa attacker dapat meng-exploit serangan ke sistem.
5. Dan setelah attacker melakukan serangan terhadap server, maka host yang telah digunakan oleh attacker akan men-download file mailicious dari remote server yang telah dikendalikan oleh attacker.

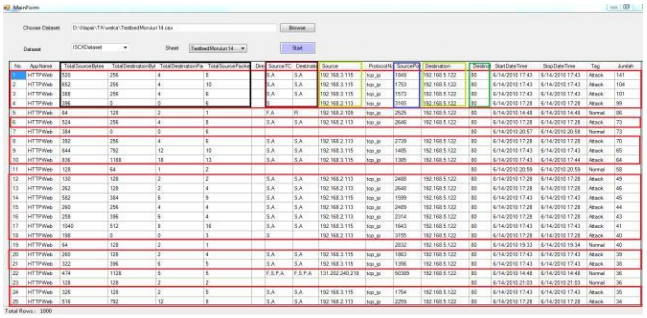


Gambar 4. Hasil *Traceroute* Dataset ISCX Testbed 14

B. Pengujian Program Perhitungan Paket Data Dominan

Dilihat dari hasil pengujian program perhitungan paket data yang dominan pada gamabar 5 berikut, Pola baris paket data pada dateset ISCX mengacu pada karakteristik serangan *Denial of Service* [6], [7] :

[1] *Attacker* memanfaatkan koneksi dari *IP source* sistem melalui backdoor untuk meng-exploit server.
[2] *Port numbers* yang digunakan secara acak darijumlah paket palsu.
[3] Ukuran *window* dan *packet length* yang tetap selama serangan dilakukan.
[4] *Flags* dalam *protocol TCP* dimanipulasi hanyamelakukan *SYN* dan *ACK*.
[5] HTTP *requests* dibanjiri melalui port 80.



Gambar 5. Hasil Perhitungan Paket Data Dominan Pengujian Menggunakan Snort

Sebagai dasar untuk memvalidasi apakah benar hasil dari pengenalan pola dari program diatas adalah serangan DoS, maka akan dibandingkan dengan hasil dari engine IDS yang dapat membedakan antara paket data normal dan paket data serangan DoS. Berikut hasil pengujian :

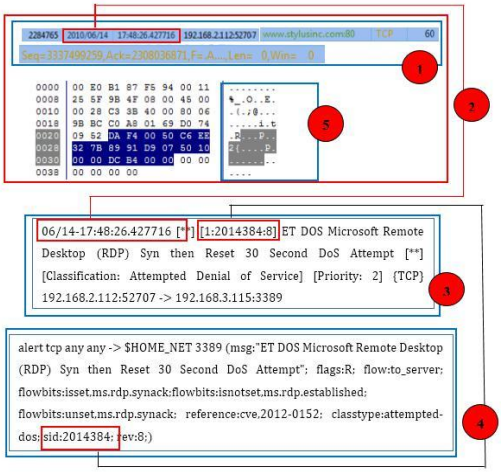
TABLE II. JUMLAH ALERT TERDETEKSI PADA PENGUJIAN ISCX DATASET (14 JUNI 2010)

No.	Klasifikasi *alert Terdeteksi*	*SID*	*Priority*	*Total*
1	*Misc activity*	*1:2925:3*	*3*	*18264*
2	*Generic protocol command decode*	*1:1748:8*	*3*	*7310*
3	*Attempted adm privilege gain*	*1:2546:14*	*1*	*3582*
4	*Attempted information leak*	*1:1201:13*	*2*	*770*
5	*Access to potentially vulnerable web*	*1:1721:18*	*2*	*284*
6	*Attempted DoS*	*1:2014384:8*	*2*	*42*

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

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

Berikut ekstraksi dan korelasi data hasil pengujian untuk dataset ISCX :



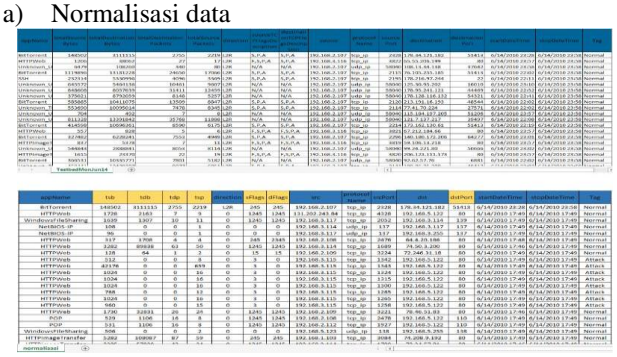
Gambar 6. Ekstraksi dan Korelasi Data Hasil Pengujian Snort Dataset ISCX

F. Pengujian Dataset menggunakan Algoritma *K-MeansClustering*

Pada tahapan pengujian menggunakan algoritma k-means clustering, dilakukan dua macam percobaan. Percobaan pertama dilakukan clustering dataset menggunakan program dengan bahasa pemrograman "python".Sedangkan, pada tahapan pengujian kedua dataset dilakukan percobaan menggunakan tool yang sudah sering digunakan oleh para penelitian [11], [12] yaitu "WEKA".

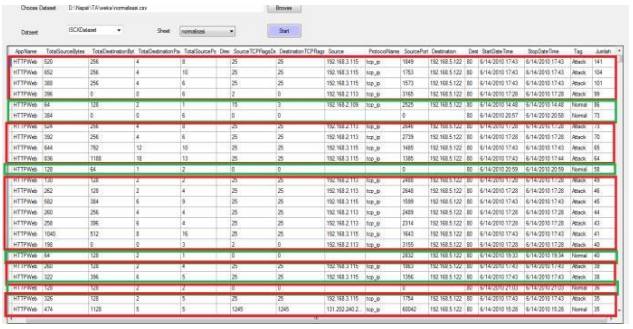
d) 1. Pengujian *Dataset ISCX* dengan Program *Clustering* menggunakan Algoritma *K-means*

a) Normalisasi data



Gambar 7. Paket Dataset ISCX 14 Juni.csv *before- After* Normalisasi

b) Menentukan nilai dari *k cluster, k cluster* dalam
c) program *clustering* menggunakan *k-mean* ini terdiri dari dua *k cluster* yaitu *cluster attack* dan *cluster* normal.
d) Menentukan centroid awal, centroid awal pada program ini ditentukan secara acak dari hasil program sebelumnya yaitu program perhitungan paket data dominan.



Gambar 9. Pola Paket Dataset ISCX 14

e) Menghitung jarak paket data ke *centroid* menggunakan rumus *Euclidean distance* [9], [10].

$$d(x,y) = |x-y| = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (1)$$

Dari perhitungan menggunakan rumus diatas maka didapatkan hasil jarak setiap paket ke centroid :

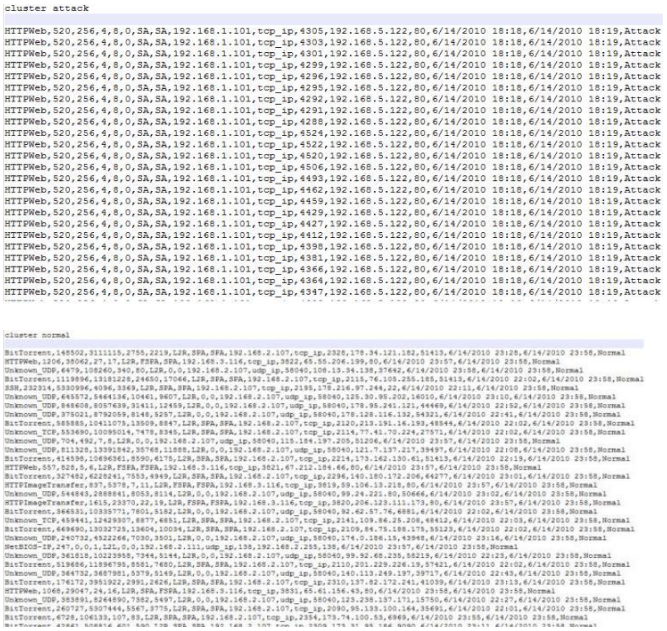
```
[97, 419, 1, 1, 53]
[454.18608521177748, 334.64757581670898, 477.04402312574882]
[84, 149, 1, 1, 53]
[449.81329460121156, 179.32094133145745, 391.53799304792886]
[88, 167, 1, 1, 53]
[441.96379942253191, 178.44887222955487, 388.94472615013046]
[95, 158, 1, 1, 53]
[437.05377243538351, 169.89408465276242, 381.18499445807151]
[1369, 1982, 6, 6, 80]
[1923.5085131082733, 2160.3742731295429, 2058.7236337109457]
[99, 309, 1, 1, 53]
[425.24933862382431, 243.76423035384005, 417.30923785605324]
[78, 596, 2, 1, 53]
[558.34218898449717, 502.87374160916374, 613.67255112152441]
[91, 291, 1, 1, 53]
[431.33861408410911, 236.36624124438751, 417.15584617742087]
[1305, 1716, 5, 5, 80]
[1657.6594945886807, 1900.9942135629976, 1792.2904340535883]
[92, 193, 1, 1, 53]
[433.52047241162671, 182.17573932881405, 388.47136316593532]
[128, 64, 1, 2, 80]
[436.54667562587167, 146.72763884149435, 351.90481667632798]
[128, 128, 2, 2, 80]
[412.41726443009151, 132.015150645674, 346.02601058301963]
[128, 64, 1, 2, 80]
[436.54667562587167, 146.72763884149435, 351.90481667632798]
[1884, 43795, 35, 28, 80]
[43560.376238044591, 43697.207027451994, 43689.774753367637]
[943, 6035, 7, 13, 80]
[5794.4632193154875, 5946.3659490482087, 5925.5951599818227]
[892, 7461, 8, 13, 80]
[7214.5997809996361, 7360.1936115838689, 7344.9088489919332]
[8207, 157132, 120, 101, 80]
[157064.29080174859, 157205.07015360543, 157194.39476648014]
[288, 0, 0, 3, 137]
[350.21422015674921, 142.94754282603111, 232.93346689559232]
[1323, 43957, 32, 19, 80]
[43708.387238606731, 43841.90099664931, 43837.232656726861]
[2640, 102544, 80, 30, 80]
[102310.0022089727, 102443.68679425785, 102438.93692341795]
```

Gambar 10. Hasil Perhitungan Jarak Antar Paket di Dataset ISCX 14 Juni

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

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

6. *Clustering* paket data kedalam *cluster* berdasarkanjarak minimum sampai tidak ada perubahan / perpindahan *cluster.*



Gambar 12. Hasil Clustering Paket *Attack* dan Normal Dataset ISCX 14 Juni

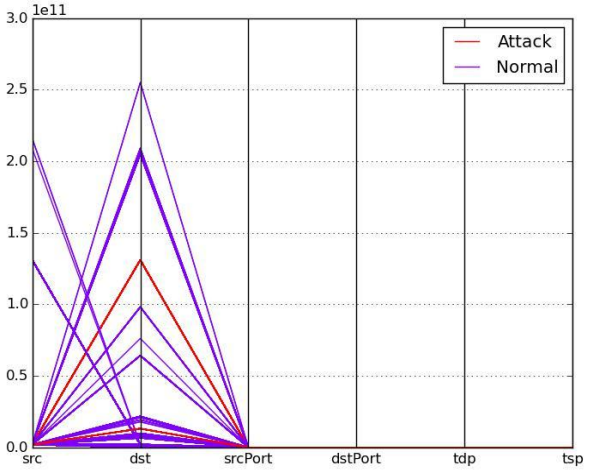
TABLE III. HASIL PERHITUNGAN *CLUSTERING* MENGGUNAKAN ALGORITMA *K-MEANS*

Total paket *cluster attack*	Total paket *cluster normal*	*Iterasi*	*Centroid* akhir normal (1)	*Centroid* akhir *attack*
1830	171338	*0*	*[6139.0, 36110.0, 33.0, 22.0, 1591.0]*	*[260.0, 128.0, 2.0, 3.0, 80.0]*
1830	171338	*1*		

TABLE IV. PERHITUNGAN *CONFUSION MATRIX* PEMROGRAMAN *K-MEANS*

Jenis Paket	Jumlah Paket	*Accuracy %*	*Detection %*	*False Alarm %*
TN	167611	*97,83*	*98,36*	*0,02*
FP	30			
FN	3727			
TP	1800			

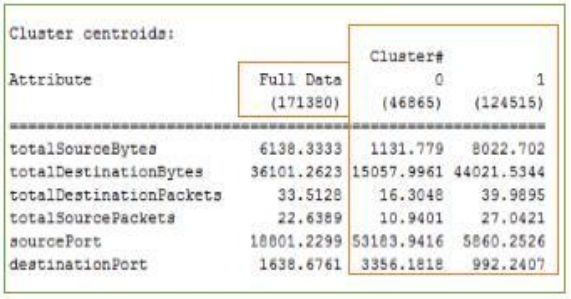
Tingkat akurasi dari program clustering menggunakan algoritma k-means dilihat dari tabel 6 sebesar 97,83%, untuk detection rate nya sebesar 98,63%, sedangkan hasil perhitungan confusion matrix untuk false alarm dari program sebesar 0,02%. Setelah di lakukan validasi terhadap program clustering menggunakan perhitungan confusion matrix, selanjutnya hasil dari clustering akan di visualisasikan berdasarkan cluster attack dan cluster normal. Berikut bentuk dari visualisasi nya :



Gambar 13. Visualisasi Paket Data *Attack* dan Normal Dataset ISCX 14 Juni

d) 2. Pengujian Dataset menggunakan Algoritma *K-Means Clustering* dengan "*WEKA*"

Hasil pengujian dataset ISCX pada gambar 17 menunjukan bahwa total paket data di *cluster* 0 sebanyak 46865 baris, sedangkan paket data yang terdapat di nilai *centroid* 1 sebanyak 124515 baris dari total paket data 171380 baris.

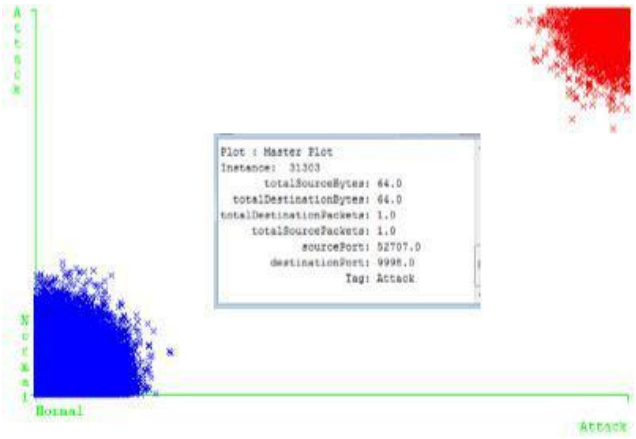


Cluster centroids:

Attribute	Full Data (171380)	Cluster# 0 (46865)	1 (124515)
totalSourceBytes	6138.3333	1131.779	8022.702
totalDestinationBytes	36101.2623	15057.9961	44021.5344
totalDestinationPackets	33.5128	16.3048	39.9895
totalSourcePackets	22.6389	10.9401	27.0421
sourcePort	18801.2299	53183.9416	5860.2526
destinationPort	1638.6761	3356.1818	992.2407

Gambar 14. Pengolahan Dataset ISCX dengan WEKA

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



Gambar 15. Visualisasi Serangan DoS dengan *Clustering* menggunakan algoritma *K-means* DatasetISCX dengan WEKA

Hasil akhir *clustering* pada gambar diatas menggambarkan setiap paket pada dataset, dimana bentuk visual normal dan *attack* ditampilkan berdasarkan sumbu x dan sumbu y yangdigunakan. Berikut hasil perhitungan *confusion matrix* dari *clustering* menggunakan algoritma *k-means* yang terdeteksiuntuk setiap *cluster.*

TABLE V. PERHITUNGAN *CONFUSION MATRIX TOOL WEKA*

Jenis Paket	Jumlah Paket	*Accuracy %*	*Detection %*	*False Alarm %*
TN	53907	*99,69*	*99,01*	***3,70***
FP	20			
FN	151			
TP	2010			

IV. KESIMPULAN DAN SARAN

2.1. *Kesimpulan*

Serangan *Denial of Service* di dataset *ISCX* memiliki pola sebagai berikut : banyaknya *IP host* yang hanya meng-*exploit* ke satu *IP server, HTTP request* dibanjiri melalui port 80, ukuran *window* dan *packet length* yang tetap selama serangan, flags dalam protokol TCP dimanipulasi hanya melakukan *SYN* dan *ACK, port numbers* secara acak dari jumlah paket palsu. Sedangkan, paket normal membentuk pola yaitu : banyaknya satu *source* ke banyak *destination*, banyak *source* ke satu *destination* dan satu *source* ke satu *destination*. Persentasiakurasi dari program *clustering* menggunakan algoritma *k-means* sebesar 97,83%, untuk *detection rate* nya sebesar98,63%, dan hasil perhitungan *confusion matrix* untuk false *alarm* dari program sebesar 0,02%. Nilai persentase akurasidari *clustering* menggunakan algoritma *k-means* dengan *toolWEKA* yang dihitung menggunakan *confusion matrix* menghasilkan nilai *accuracy* 99,69%, *detection rate* 99,01% dan *false alarm* sebesar 3,70%.

B. Saran

Pada penelitian lanjutan, ada baiknya mencoba untuk melakukan visualisasi menggunakan dataset dengan topologi sendiri dan secara *real-time*.

REFERENSI

1. J. J. Siregar, "Web Denial Of Service Attack," no. 9, pp. 1199–1205.
2. Y.-J. Yang and Y.-H. Liu, "A DoS Attack Situation Visualization Method Based on Parallel Coordinates," 2012 IEEE 12th Int. Conf. Comput. Inf. Technol., pp. 340–344, 2012.
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. H. Kim, I. Kang, and S. Bahk, "Real-time visualization of network attacks on high-speed links," IEEE Netw., vol. 18, no. 5, pp. 30–39, 2004.
5. H. Kim, I. Lee, J. Cho, and J. Moon, "Visualization of Network Components for Attack Analysis," 2009.
6. P. A. R. Kumar and S. Selvakumar, "Distributed denial of service attack detection using an ensemble of neural classifier," Comput. Commun., vol. 34, no. 11, pp. 1328–1341, 2011.
7. M. Kale, "DDOS Attack Detection Based on an Ensemble of Neural Classifier," vol. 14, no. 7, pp. 122–129, 2014.
8. R. F. Malik and V. Puspita, "Classification Denial Of Service (DoS) Attack Using Artificial Neural Network Learning Vector," no. August, pp. 20–21, 2014.
9. B. Santoso, "Data Mining: Teknik Pemanfaatan Data untuk Keperluan Bisnis." Yogyakarta: Graha Ilmu, 2007.
10. .K. Sholeh, B. D. Setiawan, and I. Cholissodin, "Implementasi Metode K-Means Clustering untuk Pembangkitan Aturan Fuzzy pada Klasifikasi Ketahanan Hidup Penderita Kanker Payudara," pp. 1–9.
11. N. Sharma, A. Bajpai, and R. Litoriya, "Comparison the various clustering algorithms of weka tools," vol. 2, no. 5, pp. 73–80, 2012.
12. S. Jain, "K-means Clustering Using WEKA Interface," 2010.