

TUGAS AKHIR

**TEKNIK CLUSTERING PADA LOG FILE IDS
MENGUNAKAN ALGORITMA HIERARCHICAL
CLUSTERING**



**Disusun Oleh :
ERIKO JANUAR AKBAR
1210651284**

**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER**

2017

HALAMAN PENGESAHAN

TEKNIK CLUSTERING PADA LOG FILE IDS MENGUNAKAN ALGORITMA HIERARCHICAL CLUSTERING

Oleh :

ERIKO JANUAR AKBAR

12 1065 1284

Telah Mempertanggung Jawabkan Laporan Tugas Akhir Pada Sidang Tugas
Akhir Tanggal 8 Agustus 2016 Sebagai Salah Satu Syarat Kelulusan Dan
Mendapatkan Gelar Sarjana Komputer (S.Kom)

di

Universitas Muhammadiyah Jember

Disetujui oleh :

Dosen Penguji :

Penguji I

Dosen Pembimbing :

Pembimbing I

Agung Nilogiri., ST, M.Kom

NIP. 19770330 2005011002

Penguji II

Triawan Adi Cahyanto., M.Kom

NPK. 1203719

Daryanto., M.Kom

NPK. 1103589

Mengesahkan,

Dekan Fakultas Teknik

Mengetahui,

Ketua Program Studi Teknik Informatika

Ir. Suhartinah, MT.

NPK. 9505246

Yeni Dwi Rahayu, S. ST., M. Kom.

NIP.19770330 200501 1 002

PERNYATAAN

Yang bertanda tangan di bawah ini :

NIM : 12 1065 1284
Nama : ERIKO JANUAR AKBAR
Institusi : Teknik Informatika, Fakultas Teknik,
Universitas Muhammadiyah Jember.

Menyatakan bahwa Tugas Akhir yang berjudul “**TEKNIK CLUSTERINGPADA LOG FILE IDS MENGGUNAKAN ALGORITMA HIERARCHICAL CLUSTERING**” Bukan merupakan karya orang lain kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini dibuat dengan sebenar-benarnya dan apabila pernyataan ini tidak benar penulis bersedia mendapatkan sanksi dari akademik.

Jember, 23 Maret 2017

Eriko Januar Akbar
NIM. 12 1065 1284

KATA PENGANTAR

Bismillahirrahmanirrahim

Puji syukur kehadiran Allah SWT yang Maha Pengasih lagi Maha Penyayang, Yang hanya kepadaNya-lah segala sesuatu bergantung. Alhamdulillah tak lupa senantiasa saya panjatkan karena hanya dengan ridho, kemurahan dan kekuasaanNya-lah proyek akhir yang berjudul:

“TEKNIK CLUSTERING PADA LOG FILE IDS MENGUNAKAN ALGORITMA HIERARCHICAL CLUSTERING”

dapat diselesaikan dengan segala kelebihan dan tak lepas dari kekurangan yang terdapat di dalamnya.

Shalawat serta salam semoga senantiasa tercurah kepada baginda Rasulullah Muhammad SAW, keluarga beliau dan para sahabat hingga pengikutnya hingga akhir zaman, orang-orang yang senantiasa istiqomah menegakkan kebenaran dan menebar kebaikan di bumi Allah SWT.

Proyek akhir ini menjelaskan tentang bagaimana mengeksplorasi program malware poison ivy menggunakan metode malware analisis dinamis dan malware analisis statis.

Dengan segala kerendahan hati, penulis memohon maaf jika ternyata di kemudian hari diketahui bahwa hasil dari proyek akhir ini masih jauh dari kesempurnaan. Semoga bermanfaat bagi setiap insan yang mempergunakannya untuk kebaikan di jalan Allah SWT.

Jember, 23 Maret 2017

Penulis

DAFTAR ISI

HALAMAN JUDUL.....	i
MOTTO	Error! Bookmark not defined.
HALAMAN PENGESAHAN.....	2
PERNYATAAN.....	3
ABSTRAK	Error! Bookmark not defined.
ABSTRACT.....	Error! Bookmark not defined.
PERSEMBAHAN	Error! Bookmark not defined.
KATA PENGANTAR	4
UNGKAPAN TERIMA KASIH.....	Error! Bookmark not defined.
DAFTAR ISI.....	5
DAFTAR GAMBAR	7
DAFTAR TABEL.....	8
BAB I	
PENDAHULUAN	Error! Bookmark not defined.
1.1 Latar Belakang	Error! Bookmark not defined.
1.2 Perumusan Masalah.....	Error! Bookmark not defined.
1.3 Batasan Masalah.....	Error! Bookmark not defined.
1.4 Tujuan Penelitian.....	Error! Bookmark not defined.
1.5 Manfaat Penelitian.....	Error! Bookmark not defined.
BAB II	
TINJAUAN PUSTAKA	Error! Bookmark not defined.
1.1 Jaringan Komputer	Error! Bookmark not defined.
1.2 Konsep Dasar Intrusion Detection System (IDS)..	Error! Bookmark not defined.
1.3 Intrusion Prevention System (IPS)	Error! Bookmark not defined.
1.4 KDD 1999 Cup dataset.....	Error! Bookmark not defined.
1.4.1 Fitur yang Terdapat pada KDD Cup ‘99.....	Error! Bookmark not defined.
1.5 Serangan	Error! Bookmark not defined.
1.6 Clustering	Error! Bookmark not defined.
1.7 Hierarchical Clustering.....	Error! Bookmark not defined.

1.8	Centroid Complete Linkage Hierarchical Method	Error! Bookmark not defined.
1.9	Gene Cluster 3.0	Error! Bookmark not defined.
1.10	Java TreeView	Error! Bookmark not defined.
BAB III		
METODE PENELITIAN.....		Error! Bookmark not defined.
3.1	Metodologi	Error! Bookmark not defined.
3.2	Sumber Data	Error! Bookmark not defined.
3.3	Penerapan AlgoritmaHierarchical Clustering.....	Error! Bookmark not defined.
3.1.1	Hitung Hierarchical Clustering	Error! Bookmark not defined.
3.1.2	Hitung Complete Linkage	Error! Bookmark not defined.
3.4	Implementasi Pada Gene Cluster 3.0 dan Java Treeview	Error! Bookmark not defined.
3.5	Analisis	Error! Bookmark not defined.
3.6	Dokumentasi.....	Error! Bookmark not defined.
BAB IV		
PEMBAHASAN DAN HASIL ANALISIS		Error! Bookmark not defined.
4.1	Pembahasan	Error! Bookmark not defined.
4.2	Metode Pengujian.....	Error! Bookmark not defined.
4.3	Pengujian Hierarchical Clustering.....	Error! Bookmark not defined.
4.4	Hasil Analisa	Error! Bookmark not defined.
BAB V		
KESIMPULAN DAN SARAN.....		Error! Bookmark not defined.
5.1	Kesimpulan.....	Error! Bookmark not defined.
5.2	Saran	Error! Bookmark not defined.
DAFTAR PUSTAKA		9

DAFTAR GAMBAR

Gambar 2. 1 Algoritma Hierarchical Clustering	Error! Bookmark not defined.
Gambar 2. 2 Dendogram Centroid Complete Linkage...	Error! Bookmark not defined.
Gambar 3. 1 Desain Sistem	Error! Bookmark not defined.
Gambar 4. 1 Metode Pengujian	Error! Bookmark not defined.
Gambar 4. 2 Dendogram Hasil	Error! Bookmark not defined.

DAFTAR TABEL

- Tabel 2. 1 Sifat bagi setiap sambungan TCP..... **Error! Bookmark not defined.**
- Tabel 2. 2 Sifat Kandungan Bagi Setiap Sambungan yang Dicadangkan oleh
Domain Pengetahuan **Error! Bookmark not defined.**
- Tabel 2. 3 Sifat Trafik Bagi 2 Saat “Time Windows” **Error! Bookmark not defined.**
- Tabel 2. 4 Jenis-jenis Serangan Probe **Error! Bookmark not defined.**
- Tabel 2. 5 Jenis-jenis Serangan R2L..... **Error! Bookmark not defined.**
- Tabel 2. 6 Jenis-jenis Serangan U2R..... **Error! Bookmark not defined.**
-
- Tabel 3.1 Hitung Hierarchical Clustering **Error! Bookmark not defined.**
- Tabel 3.2 Hasil Jarak **Error! Bookmark not defined.**
- Tabel 3.3 Hitung Complete Linkage..... **Error! Bookmark not defined.**
- Tabel 3.4 Menghapus Baris-baris dan Kolom-kolom Matrik Jarak yang
Bersesuaian dengan Kelompok 1 dan 3 **Error! Bookmark not defined.**
- Tabel 3.5 Hasil Setelah Dihapus **Error! Bookmark not defined.**
- Tabel 3.6 Menghapus Baris dan Kolom Matrik yang Bersesuaian...**Error! Bookmark not defined.**
- Tabel 3.7 Hasil Menambahkan Kelompok untuk (45) ... **Error! Bookmark not defined.**
- Tabel 3.8 Menghapus Baris dan Kolom Matrik yang Bersesuaian dengan
Kelompok (45) dan 2 **Error! Bookmark not defined.**
- Tabel 3.9 Hasil Menambahkan Baris dan Kolom untuk (452).... **Error! Bookmark not defined.**
-
- Tabel 4. 4 Data Jenis Serangan..... **Error! Bookmark not defined.**

DAFTAR PUSTAKA

- Han, J. 2006. *Data Mining Concepts and Techniques Second Edition*, Bloomington, USA.
- Edelstein, H. A. 1999. *Introduction to Data Mining and Knowledge Discovery*, Third Edition. Two Crows Corporation, USA.
- Pinkard, B. dan Orebaugh, A. 2008. *Nmap in the Enterprise : Your Guide to Network Scanning*, syngress, United state of America.
- Endorf, C., Schultz, E., dan Mellander, J. 2004. *Intrusion Detection & Prevention*. Emeryville, California.
- Han, J., dan Micheline. 2001. *Data Mining Concepts and Technique*, Morgan Kaufman, USA.
- Margo, R, dan Eka R.K. 2014. *Penerapan Algoritma Clustering untuk Mengelompokkan Ketertarikan Siswa Berdasarkan Aktivitas di Mode Pembelajaran Elektronik*. STMIK AMIKOM, Yogyakarta.
- Stiawan, D. 2005. *Sistem Keamanan Komputer*, PT Elex Media Komputindo, Jakarta.
- Syafrizal, M. 2005. *Pengantar Jaringan Komputer*, Penerbit ANDI, Yogyakarta.
- Everitt, B.S. 1993. *Cluster Analysis* (3ed). Edward Arnold, London.
- Scott, C., Wolfe P., dan Hayes B., 2004. *SNORT for Dummies*, Willey Publising Inc, USA.
- Ariyus, D. 2007. *Intrusion Detection System*, Penerbit ANDI, Yogyakarta.
- Raifudin, R. 2010. *Mengayang Hacker dengan SNORT*. Penerbit ANDI, Yogyakarta.
- Anh, L. 2008, *On Optimizing Load Balancing of Intrusion Prevention and Prevention System*, IEEE, INFOCOM workshops.
- Sathya, S., Ramani, G., dan Sivaselvi, K., 2011. *Discriminant Analysis Based Feature Selection in KDD Intrusion Dataset*, International journal of Computer Applications.

Riad, M., dkk. 2013. *Visualize Network Anomaly Detection by Using K-means Clustering Algorithm*, International Journal of Computer Network & Communications.

Irvine. 1999. *The UCI KDD Archive* [Online]. Tersedia : (<http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>, diakses 1 Juli 2016)

JTV User Manual[Online]. Tersedia : (<http://jtreeview.sourceforge.net/docs/JTVUserManual/JTVUserManual.pdf> , diakses 1 Juli 2016)

Cluster 3.0 Manual [Online] Tersedia : (<http://bonsai.hgc.jp/~mdehoon/software/cluster/cluster3.pdf>, diakses 1 Juli 2016)