39 UNS BERKARYA UNTUK INDONESIA

ISBN : 978-602-18580-3-5

PROSIDING

Seminar Nasional Matematika, Sains dan Informatika

SAINTEKINFO 2015

Surakarta, 25 April 2015

PERANAN DATA MINING UNTUK PROSES PENGOLAHAN DATA PENELITIAN SAINS

Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Sebelas Maret

Supported by:

DUTA NETWORK

PROSIDING Seminar Nasional Matematika, Sains dan Informatika
Saintekinfo 2015
FMIPA UNS
25 April 2015

Makalah ini dipresentasikan pada
Seminar Nasional Matematika, Sains dan Informatika
Saintekinfo 2015
"Peran Data Mining untuk Proses Pengolahan Data Penelitian Sains"
Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Sebelas Maret
Surakarta, 25 April 2015

Penerbit: Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Sebelas Maret
Surakarta

ISBN : 978-602-18580-3-5

KATA PENGANTAR

Seminar Nasional ini merupakan rangkaian acara Dies Natalis Universitas Sebelas Maret yang ke 39 yang diselenggarakan oleh Fakultas Matematika dan Ilmu Pengetahuan alam Universitas Sebelas Maret Surakarta yang meliputi Jurusan Matematika, Kimia, Biologi, Fisika, Farmasi, dan Informatika. Pada acara ini dihadirkan dua *keynote speaker* yang pertama dari Kementrian Pariwisata Republik Indonesia dengan tema **"e-tourism Data Mining : Solusi Promosi bagi Pariwisata"** dan yang kedua adalah dari Pemerintahan Kota Madya Surakarta dengan tema **"Pengembangan Pariwisata Terintegrasi di Wilayah Solo Raya"**.

Presentasi makalah seminar ini terdiri atas presentasi makalah undangan (3 pemakalah), presentasi makalah oral (77) pemakalah) dan presentasi poster (3 poster) dari para peneliti yang berasal dari Universitas Gadjah Mada (UGM), Universitas Sebelas Maret (UNS), Universitas Jambi, Universitas Islam Indonesia (UII), Universitas Atma Jaya, Universitas Jenderal Soedirman (UNSOED), Institute Teknologi Sepuluh Nopember (ITS), Universitas Diponegoro (UNDIP), IAIN Kalijaga, Universitas Nusa Nipa Maumere, Universitas Jenderal Achmad Yani (UNJANI), Universitas Widya Dharma (UNWIDHA), Universitas Indonesia (UI), Universitas Sanata Dharma Yogyakarta, MAN Babat., SMP NEGERI 1 MAJENANG KABUPATEN CILACAP STMIK Sinar Nusantara Surakarta, LPPKS Indonesia, Stain Kediri dan serta mahasiswa baik tingkat sarjana maupun pascasarjana.

Surakarta, April 2015
Editors

DAFTAR REVIEWER

1. Prof. Dr. Ir. Khairil Anwar Notodiputro, M.S. (Institut Pertanian Bogor)
2. Prof. Drs. Tri Atmojo, M.Sc., Ph.D (Universitas Sebelas Maret)
3. Dr. Sunarto, MS (Universitas Sebelas Maret)
4. Anto Satriyo Nugroho (Badan Pengkajian dan Penerapan Teknologi)
5. Drs. Bambang Harjito, M.App.Sc., Ph.D. (Universitas Sebelas Maret)
6. Venty Suryanti, M.Phil., Ph.D. (Universitas Sebelas Maret)
7. Nuryani, S.Si., M.Si., Ph.D. (Universitas Sebelas Maret Surakarta)
8. Dr. Dewi Retno Sari Saputro, S.Si, M.Kom (Universitas Sebelas Maret)
9. Dra. Isnandar Slamet, M.Sc., Ph.D (Universitas Sebelas Maret)
10. Winita Sulandari, M.Si. (Universitas Sebelas Maret)
11. Drs. Sarngadi Palgunadi, M.Sc(Universitas Sebelas Maret)
12. Ristu Saptono, S.Si., M.T.(Universitas Sebelas Maret)

TIM PROSIDING

Editor:

Dra. Purnami Widyaningsih, M.App.Sc
Nughthoh Arfawi Kurdhi, S.Si., M.Sc.
Hasan Dwi Cahyono, S.Kom., M.Kom.
Rini Anggrainingsih, ST., M.T.
Afrizal Doewes, S.Kom., M.Sc.

Pelaksana Teknis :

Indiawati Ayik Imaya
Zulia Nurdina Arba'ati
Beta Vitayanti
Armada Dwika Panji Kusuma

Desain Cover :

Yudho Yudhanto, S.Kom

SAMBUTAN KETUA PANITIA

Syukur Alhamdulilah, kita panjatkan puji syukur kehadirat Allah SWT yang telah memberikan kenikmatan dan keselamatan pada kita semua, sehingga pada hari ini kita dapat melaksanakan kegiatan Seminar Nasional Matematika, Sains dan Informatika dengan tema "Peranan Data Mining dalam Pengolahan Data Penelitian Sains" yang diselenggarakan oleh oleh Fakultas Matematika dan Ilmu pengetahuan alam yang meliputi Jurusan Matematika, Kimia, Biologi, Fisika, Farmasi, dan Informatika dalam rangka Dies Natalis Universitas Sebelas Maret ke 39. Kegiatan seminar ini diharapkan dapat meningkatkan kerjasama diantara perguruan tinggi, lembaga penelitian dan industri sebagai sarana bertukar informasi dan menyebarkan hasil penelitian/pemikiran dan dapat memberikan kontribusi terhadap pemecahan masalah IPTEK khusunya dalam pengambilan sebuah keputusan dari sekian juta data yang bertebaran. Dengan dipublikasikannya semua artikel dalam prosiding seminar maka masyarakat luas berkesempatan untuk melakukan penelitian lebih lanjut atau mengaplikasikan dalam kehidupan praktis.

Kami mengucapkan selamat datang dan terima kasih yang sebesar-besarnya kepada nara sumber yang menjadi pembicara dalam seminar ini. Terima kasih kami sampaikan juga kepada pemakalah dan peserta seminar yang telah hadir. Demikian juga kepada para sponsor yang telah membantu dalam pelaksanaan kegiatan seminar ini.

Akhir kata, selaku panitia memohon maaf jika masih banyak kekurangan dan dalam pelaksanaan seminar dan semoga memperoleh banyak manfaat memberikan kesegaran keilmuan sekarang dan masa yang akan datang.

Wassalamu alikum wr wb

Surakarta, April 2015
Ketua Panitia

Drs. Bambang Harjito, M.App.Sc, Ph.D

SAMBUTAN REKTOR

Assalamualaikum wr. wb.

Hari ini merupakan hari yang berbahagia bagi UNS dalam rangkaian Dies Natalis UNS ke-39, FMIPA dapat mengadakan ***Seminar Nasional Matematika dan Informatika.*** Momentum ini menjadi penting bagi UNS sebagai perguruan tinggi yang menjadi salah satu pusat rujukan akademis yang juga memilki tanggung jawab besar untuk menjawab tantangan bangsa. UNS sejak tahun 2011 telah mencanangkan dan menerapkan secara konsisten 10% dari dana Penerimaan Negara Bukan Pajak (PNBP) untuk dana penelitian. Menurut arahan dari Dirjen Pendidikan Tinggi, penelitian perguruan tinggi harus mempunyai *ouput* dan *outcome* yang jelas. Output-nya diarahkan agar hasil riset dapat diterbitkan di jurnal nasional dan internasional terakreditasi. Saat ini para peneliti UNS tengah bersemangat untuk mempublikasikan risetnya di berbagai publikasi ilmiah bertaraf internasional.

Apakah benar bahwa riset-riset yang dilakukan oleh perguruan tinggi benar-benar dapat menjawab masalah-masalah yang dihadapi masyarakat? Pertanyaan ini menjadi penting, manakala masih banyak penelitian yang hanya berhenti sebagai laporan saja atau semata-mata hanya memenuhi "kepuasan intelektual" (*intelektual exercises*). Berkaitan dengan itu, seminar ini diharapkan dapat memberikan sumbangan pemikiran terhadap **peranan data mining untuk proses pengolahan data penelitian sains.** Data *mining* (penambangan data) merupakan serangkaian proses yang dirancang untuk mengeksplorasi kumpulan data dalam jumlah besar untuk membantu menemukan pola yang konsisten dan atau mencari hubungan sistematis antara variabel satu dengan yang lain, selanjutnya memvalidasi temuan dengan menerapkan pola terdeteksi. Dengan penambangan data, maka data yang tersedia menjadi sumber informasi dan pengetahuan yang berguna dan dapat sebagai acuan pengambilan keputusan. Sehingga peranan data mining diperlukan untuk aplikasi khususnya dibidang matematika, sains, dan informatika, atau terapan dibidang yang lebih luas seperti telah diaplikasikan dibidang pariwisata (*e-tourism*) dengan pemanfaatan pola data yang konsisten. Dengan seminar ini mudah-mudahan bisa mengawali kerjasama UNS dengan berbagai pihak untuk menyumbangkan keilmuan kita untuk kepentingan masyarakat. Akhirnya mudah-mudahan seminar ini dapat berlangsung lancar dan sukses serta hasil-hasilnya dapat diimplementasikan dan bermanfaat bagi masyarakat luas. Semoga Tuhan yang Maha Esa mengabulkannya, amien.

Wassalamu'alaikum wr wb.

Rektor,
Prof. Dr. Ravik Karsidi, M.S.

SUSUNAN PANITIA

Pelindung	:	Prof. Ravik Karsidi (Rektor UNS)
Steering Committee	:	Prof.Ir.Ari Handono R,M.Sc (Hons),Ph.D Dr. Sutanto, S.Si., DEA, Drs. Harjana, M.Si.,M.Sc.,Ph.D Drs. Sutrimo, M.Si
Ketua Panitia	:	Drs. Bambang Harjito, M.App.Sc., Ph.D
Sekretaris	:	Winita Sulandari, M.Si
Bendahara	:	Dr. Sayekti Wahyuningsih, S.Si., M.Si Titin Sri Martini, S.Si., M.Kom Setyaningsih, A.Md
Anggota	:	Hartatik, S.Si., M.Si. Edi Pramono, S.Si., M.Si. Eny Winarni, S.Sos. Dian Prajarini, S.T., M.Eng. Rosita Yanuarti, S.Kom., M.Eng. Sakroni, A.Md., S.Kom. Endar Suprih Wihidayat, S.T., M.Eng. Liliek Triyono, S.T., M.Kom. Zulfa Nurul Hakim, A.Md. Mohtar Yunianto, M.Si. Dra. Purnami Widyaningsih, M.App.Sc Nughthoh Arfawi Kurdhi, S.Si., M.Sc. Hasan Dwi Cahyono, S.Kom., M.Kom. Rini Anggrainingsih, ST., M.T. Afrizal Doewes, S.Kom., M.Sc. Aji Kurniawan Mulya, A.Md. Dra. Etik Zukhronah, M.Si. Dra. Yuliana Susanti, M.Si. Dra. Respatiwulan, M.Si Esti Suryani, S.Si., M.Kom. Sari Widya Sihwi, S.Kom., M.T.I Meiyanto Eko Sulistyo, S.T., M.Eng. Vinci Mizranita, S.Farm., M.Pharm., Apt. Winarno, S.IP Fendi Aji Purnomo, S.Si. Gimin Heri Sukarno Putro

DAFTAR ISI

Bildang Informatika dan Teknik

ANALISIS KINERJA PERANGKAT LUNAK KEAMANAN KOMPUTER

Bambang Sugiantoro, S.Si., M.T.[1] Yazid Ubaidilah, S.Kom.[2]
[1,2]Program Studi Teknik Informatika UIN Sunan Kalijaga Yogyakarta
Jl marsda adisucipto Yogyakarta

ABSTRACT. Utilization of computers in almost every aspect of life we often see. But over time the security aspects in the exchange of information and data to be ignored even become mandatory aspect to make the exchange of information and data to be safe from people who are not interested. To answer these challenges, Suricata comes as one solution to reducing crime in the field of computer security is to make it as an alarm when the computer server where data and information are attacked.One computer crime is a DOS attack is to make a server serving multiple clients at one time that led to the use of bandwidth and computer memory quickly drained away. So when there is a client or other user who attempts to access the server can not receive the service server because the server was down. Having conducted more in-depth analysis of a series of views of the descriptive analysis of pre-test and post-test can be concluded that the Suricata IDS is able to reduce DOS attack.

***Keywords**: Suricata, IDS, memory usage, DOS Attack*

1. PENDAHULUAN

Penggunaan media telekomunikasi memang memudahkan pekerjaan kita semua.Namun dari segudang kegunaannya tersimpan ancaman, gangguan dan dampak buruk yang terkadang tidak terpikirkan ketika kita menggunakan telekomunikasi.Teknologi telekomunikasi yang bisa diakses kapan saja dan di mana saja membuat pertukaran data dan informasi begitu mudahnya dilakukan oleh siapa saja.Bahkan tidak sedikit orang melakukan pencurian data dan informasi demi keuntungannya sendiri.Untuk mencegah terjadinya pengaksesan oleh orang yang tidak mempunyai wewenang sistem dapat diperkuat dari sisi keamanannya.

Keamanan jaringan tergantung pada kecepatan pengatur jaringan dalam menindaklanjuti sistem saat terjadi gangguan. Untuk memperkuat keamanan jaringan komputer dapat diterapkan sistem pendeteksi serangan dalam jaringan tersebut.

IDS (Intrusion Detection System) membantu administrator jaringan dalam memantau keadaan sistem dengan mendeteksi dan menganalisa lalu lintas paket-paket data yang terjadi pada jaringan. Suricata adalah salah satu IDS engine open source yang dirilis oleh OISF (Open Information System Foundation) organisasi non-profit yang didanai oleh pemerintahan Amerika Serikat.

Dalam pengamatan penulis IDS snort paling banyak digunakan karena snort merupakan *standard de facto* IDS di dunia. Akan tetapi kemunculan Suricata sebagai IDS belum banyak

dilakukan riset dalam dunia.Oleh karena itu, penulis mencoba melakukan riset kecil tentang Suricata IDS.Di mana penulis menitikberatkan pada penelitian bagaimana performa server sebelum dan sesudah adanya Suricata.Dalam hal ini pemakaian memori komputer yang menjadi tolok ukur.

Berdasarkan latar belakang yang telah diuraikan sebelumnya, penulis mengambil rumusan masalah bagaimana kinerja server sebelum dan sesudah adanya Suricata IDS dalam menangani IP Flooding/DOS attack yang menguras memori komputer.

2. LANDASAN TEORI

2.1 IDS (Intrusion Detection System)

Salah satu metode keamanan jaringan tersebut yaitu dengan IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*). Menurut Dr. Natarajan Meghanathan professor di Jackson State University menyatakan bahwa IDS (Intrusion Detection System) adalah layaknya alarm di dunia nyata. Tugas utama dari sebuah IDS yaitu mengidentifikasi aktivitas mencurigakan ataupun aktivitas yang merugikan sistem, bukan aktivitas normal. Selain itu juga mampu mengklasifikasikan aktivitas tersebut dan jika memungkinkan IDS dapat merespon aktivitas itu.

Ada beberapa alasan untuk memasang IDS di sistem :

1. Untuk mencegah masalah yang disebabkan adanya peningkatan resiko ditemukannya lubang keamanan.
2. Untuk mendeteksi serangan dan masalah keamanan lainnya yang tidak bisa dicegah oleh alat keamanan lainnya.
3. Untuk mendokumentasikan ancaman yang telah terdeteksi.
4. Bertindak sebagai *quality control* untuk administrasi dan desain keamanan, khususnya untuk organisasi skala besar dan kompleks.
5. Untuk menyediakan informasi yang berguna tentang serangan dimana hal itu terjadi, mengizinkan diagnose yang lebih mendalam, upaya pemulihan sistem dan pembenaran faktor kausatif.

IDS merupakan sebuah sistem komputer yang dapat dipadukan antara hardware dan software yang bekerja secara bersama-sama yang dapat mengenali adanya penyusupan pada sebuah jaringan. Beberapa komponen dari sebuah IDS yaitu :

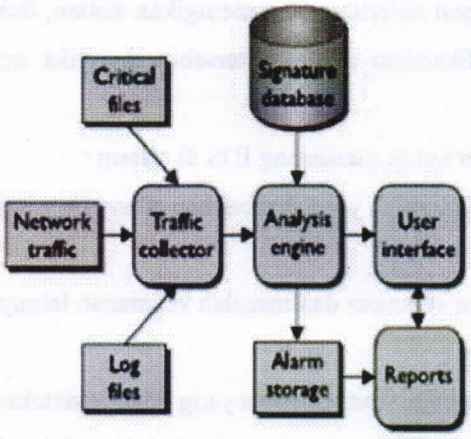
a. *Analysis engine* :melakukan pengujian terhadap trafik jaringan dan membandingkannya dengan pola aktivitas mencurigakan atau merugikan di dalam database engine. Komponen ini sering disebut "otak" dari sebuah IDS.

b. *Traffic collector (sensor)* : mengumpulkan aktivitas atau even dari IDS untuk dilakukan pengujian. Untuk sebuah HIDS (Host-based Intrusion Detection System) bisa berupa file-file log, log audit, atau trafik yang datang ataupun yang keluar dari sistem. Sedangkan untuk NIDS (Network-based Intrusion Detection System) bisa berupa trafik jaringan yang tertangkap oleh sebuah *sniffer*.

c. *Signature database* :sebuah kumpulan pola dan definisi dari aktivitas mencurigakan atau merugikan.

d. *User interface and reporting* : tampilan yang menyajikan *alert* dan memberikan interaksi kepada pengguna untuk mengoperasikan IDS tersebut.

Berikut gambar komponen IDS dari Conklin and White dalam karyanya yang berjudul *Principles of Computer Security, 2nd Edition* :



Gambar 2.1 Komponen IDS

Dilihat dari kemampuan IDS dalam hal mendeteksi serangan atau upaya penyusupan di dalam jaringan, maka IDS terbagi menjadi dua yaitu :

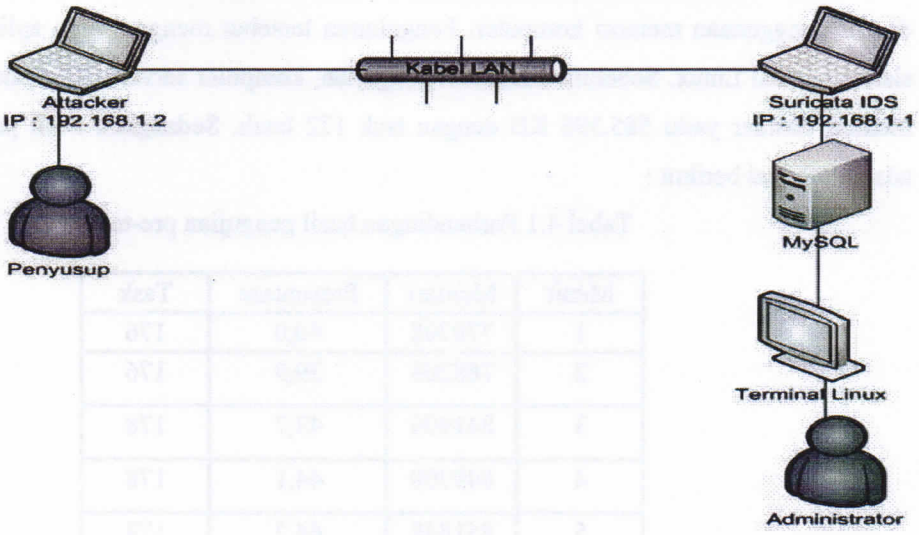
1. NIDS (*Network-based Intrusion Detection System*) yaitu IDS yang menguji aktivitas trafik yang melewati jaringan dengan mengumpulkan paket-paket data lalu dianalisa apakah paket tersebut merupakan paket normal atau paket serangan. NIDS biasanya diletakkan di bagian penting jaringan seperti di server atau pintu masuk jaringan.

2. HIDS (*Host-based Intrusion Detection System*) yaitu IDS yang hanya memantau aktivitas jaringan di sistem individu dan tidak mempedulikan sistem lain atau jaringan itu. HIDS sering diletakkan di firewall, web server atau server yang terhubung langsung dengan internet.

3. METODE PENELITIAN

Penelitian ini termasuk jenis penelitian laboratorium (*Laboratory-based research*), yaitu penelitian kuantitatif dalam pengumpulan data dengan cara eksperimen.Eksperimen bertujuan untuk menumbuhkan variabel-variabel dan selanjutnya dikontrol untuk dilihat efektivitas dari Suricata IDS dalam menangani adanya upaya serangan dari attacker berupa DOS attack. Pengukuran keefektivitasan dari Suricata dilihat dari besarnya penggunaan memori komputer dalam hal menangani serangan tersebut. Yaitu dengan cara membandingkan hasil dari pengukuran memori sebelum dan sesudah diinstall Suricata ke dalam server.

Sebelum melakukan pengujian, terlebih dahulu merancang ruang lingkup penelitian yaitu desain jaringan yang akan digunakan. Berikut rancangan jaringan penelitian :



Gambar 3.1 Arsitektur Penelitian

Komputer yang digunakan sebagai server diuji terlebih dahulu dengan software aplikasi DOS bawaan Kali Linux OS yaitu Siege.Pengujian ini dilakukan selama 5 kali berturut-turut dimulai dari batas waktu 1 menit sampai 5 menit dengan jarak pengujian selama 1 menit. Untuk mengetahui konsumsi memori komputer yang digunakan, peneliti menggunakan aplikasi top yaitu aplikasi task manager Linux.

Dalam menghubungkan komputer server dan attacker diperlukan ip address. IP address diatur statik secara manual dengan merubah file konfigurasi dari file *interfaces* di dalam folder /etc/network. Dalam hal ini komputer server mendapat IP address 192.168.1.1 sedangkan komputer attacker mempunyai IP address 192.168.1.2. Dalam menguji Suricata yang berada di server dengan IP address 192.168.1.1, attacker melakukan IP Flooding langsung dari komputer dengan IP address 192.168.1.2.

Setelah dilakukan pengujian pre-test (sebelum adanya Suricata) langkah selanjutnya ialah dengan melakukan pengujian post-test (setelah adanya Suricata). Akan tetapi sebelum melakukan post-test, terlebih dahulu diberikan treatment yaitu instalasi Suricata.

4. HASIL PENELITIAN DAN PEMBAHASAN

Hasil dari penelitian ini dibagi menjadi dua hasil yaitu pre-test dan post-test.Hasil pre-test adalah dimana komputer diserang sebelum menggunakan Suricata IDS.Sedangkan hasil post-test adalah komputer diserang setelah diinstall Suricata IDS.Setiap kali dilakukan penyerangan, diukur penggunaan memori komputer. Pengukuran tersebut menggunakan aplikasi top bawaan sistem operasi Linux. Sebelum dilakukan pengujian, komputer server menunjukkan penggunaan memori standar yaitu 585.396 KB dengan task 172 buah. Sedangkan hasil pengujian pre-test adalah sebagai berikut :

Tabel 4.1 Perbandingan hasil pengujian pre-test

Menit	Memori	Prosentase	Task
1	770708	40,0	176
2	768208	39,9	176
3	841900	43,7	178
4	849700	44,1	178
5	851848	44,2	178

Pengujian post-test pertama diambil setelah pengujian tahap pertama selesai dilakukan. Akan tetapi komputer server di *reboot*terlebih dahulu agar seperti kondisi baru dinyalakan. Hasil dari pengujian post-test tersaji di tabel 4.2.

Tabel 4.2 Tabel hasil pengujian post-test

Menit	Mem Used	Percentage	Task
1	1182480	61,4	181
2	1193232	61,9	181
3	1197644	62,2	181
4	1202396	62,4	184
5	1207644	62,7	184

Secara keseluruhan hasil pengujian Suricata menggunakan serangan IP Flooding yang difokuskan terhadap penggunaan memori komputer dapat dilihat di tabel 4.3.

Uji normalitas pre-test dengan metode *Kolmogorov-Smirnov* dengan tool PSPP dapat dilihat di bawah ini.

One-Sample Kolmogorov-Smirnov Test

		Memori	Task	Menit
N		5	5	5
Normal Parameters	Mean	816472.80	177.20	3.00
	Std. Deviation	43086.84	1.10	1.58
Most Extreme Differences	Absolute	.32	.37	.14
	Positive	.26	.26	.14
	Negative	-.32	-.37	-.14
Kolmogorov-Smirnov Z		.72	.82	.31
Asymp. Sig. (2-tailed)		.68	.51	1.00

Gambar 4.1 Uji normalitas pre-test

Dari gambar tersebut tingkat signifikansi data pre-test mulai dari variabel menit, memori dan task masing-masing bernilai 1,00; 0,68; dan 0,51 yang berarti melebihi nilai signifikansi sebesar 0,05. Hal ini membuktikan bahwa distribusi data pre-test termasuk distribusi data yang normal. Berikut hasil uji normalitas data post-test yang telah dilakukan :

One-Sample Kolmogorov-Smirnov Test

		Memori	Task	Menit
N		5	5	5
Normal Parameters	Mean	1196679.20	182.20	3.00
	Std. Deviation	9583.06	1.64	1.58
Most Extreme Differences	Absolute	.16	.37	.14
	Positive	.13	.37	.14
	Negative	-.16	-.26	-.14
Kolmogorov-Smirnov Z		.36	.82	.31
Asymp. Sig. (2-tailed)		1.00	.51	1.00

Gambar 4.2 Uji normalitas Post-test

Dapat dilihat dari gambar di atas taraf signifikansi dari variabel menit senilai 1,00, variabel memori senilai 1,00 dan variabel task senilai 0,51 yang berarti telah melebihi taraf signifikansi yang telah ditetapkan yaitu sebesar 0,05. Hal ini membuktikan bahwa H_0 diterima dan data post-test memang termasuk distribusi data yang normal pula.

Setelah diketahui bahwa data dari pre-test maupun post-test adalah data yang berdistribusi normal, langkah berikutnya ialah uji homogenitas yang dimaksudkan untuk memperlihatkan bahwa dua atau lebih kelompok data sampel berasal dari populasi yang memiliki variansi yang sama. Berikut hasil uji homogenitas data pre-test yaitu data hasil pengujian sebelum adanya instalasi Suricata IDS :

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Memori	3.21	1	3	.17

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Memori	Between Groups	7367971396.80	1	7367971396.80	381.56	.00
	Within Groups	57930536.00	3	19310178.67		
	Total	7425901932.80	4			

Gambar 4.3 Uji homogenitas pre-test

Terlihat dari hasil pengolahan data melalui software aplikasi PSPP menunjukkan bahwa data tersebut berasal dari variansi yang homogen. Hasil uji homogenitas mencapai nilai signifikansi 0,17 melebihi 0,05 yang berarti H_0 diterima. Sedangkan hasil uji homogenitas data setelah diinstall Suricata dapat dilihat di gambar 4.4 di bawah ini :

Test of Homogeneity of Variances

	Levene Statistic	df1	df2	Sig.
Memori	1.60	1	3	.30

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Memori	Between Groups	231896482.13	1	231896482.13	5.14	.11
	Within Groups	135443466.67	3	45147822.22		
	Total	367339948.80	4			

Gambar 4.4 Uji homogenitas post-test

Uji homogenitas pada data hasil pengujian setelah diinstall Suricata memperlihatkan angka nilai signifikansi sebesar 0,30 yang berarti bahwa data-data tersebut merupakan data yang mempunyai variansi yang sama.

Pengujian ada tidaknya korelasi antar variabel dapat digunakan dengan metode *bivariate correlation* atau sering disebut juga Product Moment Pearson. Dalam melakukan uji korelasi perlu memperhatikan *Test of Significant* yaitu meliputi Two-Tailed (uji dua sisi) digunakan dalam kondisi belum diketahui bentuk hubungan antar variabel dan One-Tailed (satu sisi) digunakan untuk menguji test of significant dari dua variabel akan tetapi telah diketahui adanya arah kecenderungan hubungan negative atau positif di antara dua variabel yang berhubungan. Pengujian korelasi pertama dilakukan dengan data pre-test menghasilkan output sebagai berikut :

Correlations

		Memori	Task
Memori	Pearson Correlation	1.00	1.00
	Sig. (2-tailed)		.00
	N	5	5
Task	Pearson Correlation	1.00	1.00
	Sig. (2-tailed)	.00	
	N	5	5

Gambar 4.5 Uji korelasi Pre-test

Dari hasil di atas dapat diketahui bahwa besarnya penggunaan memori oleh server berdasarkan korelasi dengan banyaknya task yang berjalan dengan tingkat signifikansi sebesar 0,00. Hal ini berarti penggunaan memori tidak ada hubungannya dengan banyaknya task yang berjalan. Untuk pengujian kedua yaitu uji korelasi post-test dapat dilihat di gambar 4.6 :

Correlations

		Memori	Task
Memori	Pearson Correlation	1.00	.79
	Sig. (2-tailed)		.11
	N	5	5
Task	Pearson Correlation	.79	1.00
	Sig. (2-tailed)	.11	
	N	5	5

Gambar 4.6 Uji korelasi post-test

Dapat kita lihat dari hasil uji korelasi antara task dan memori setelah diinstall Suricata berbeda dengan uji korelasi sebelumnya. Dengan tingkat korelasi sebesar 0,11 berarti penggunaan memori memiliki hubungan yang erat dengan banyaknya task.

Langkah analisis selanjutnya yaitu menganalisis keefektifan penelitian ini. Apakah dengan menginstall Suricata IDS dapat mengurangi serangan DOS atau malah sebaliknya dapat membuat komputer server lebih cepat kehabisan memori. Sampel dependen atau sampel berpasangan biasanya diambil dari satu kelompok sampel yang diberikan dua perlakuan yang berbeda. Penelitian ini juga termasuk sampel dependen dikarenakan ada perlakuan berbeda yaitu penyerangan kepada komputer server sebelum Suricata IDS diinstall dan penyerangan sesudah IDS diinstall.

Tabel 4.4 Data Penggunaan Memori Pre-test dan Post-test

Pengujian	Memori	
	Sebelum	Sesudah
1	770708	1182480
2	768208	1193232
3	841900	1197644
4	849700	1202396
5	851848	1207644

Dengan menggunakan tingkat kepercayaan 95 %. Apakah instalasi Suricata tersebut efektif untuk menghalau serangan DOS atau tidak ?

Paired Sample Statistics

		Mean	N	Std. Deviation	S.E. Mean
Pair 1	Sebelum	816472.80	5	43086.84	19269.02
	Sesudah	1196679.20	5	9583.06	4285.67

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Sebelum & Sesudah	5	.86	.06

Paired Samples Test

	Paired Differences					t	df	Sig. (2-tailed)
				95% Confidence Interval of the Difference				
	Mean	Std. Deviation	Std. Error Mean	Lower	Upper			
Pair 1 Sebelum - Sesudah	-380206.40	35199.80	15741.83	-423912.72	-336500.08	-24.15	4	.00

Gambar 4.7 Uji T Sampel Dependen data penelitian.

Dari hasil analisis di atas dapat disimpulkan bahwa rata-rata memori komputer sebelum diinstall Suricata setelah diberi serangan DOS adalah 750.546,40 dengan standar deviasi 5.591,79

sedangkan penggunaan memori setelah diinstall Suricata ialah sebesar 1.056.064,00 dengan nilai standar deviasi 4622,60.

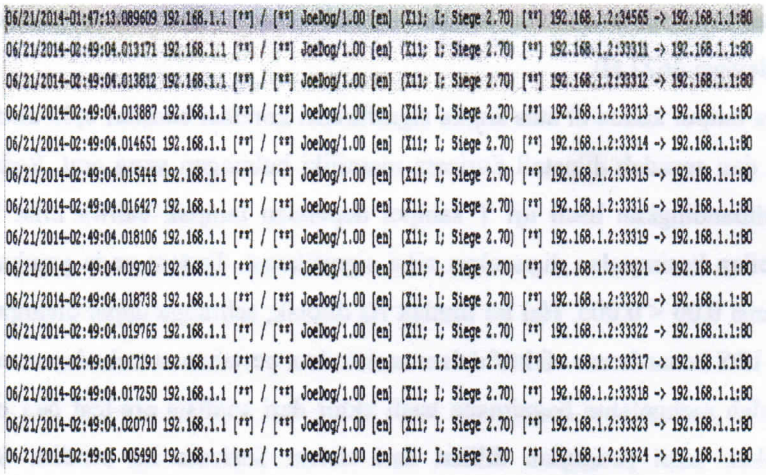
Pada output kedua di atas angka signifikansi korelasi bernilai 0,06 antara dua variabel yaitu sebelum dan sesudah diinstall Suricata memiliki hubungan yang erat. Sedangkan output ketiga setelah dibandingkan hasil uji T sampel dependen tampak bahwa nilai T* = -24,15. Dalam pengambilan kesimpulan digunakan nilai signifikansi. Tertera pada gambar di atas bahwa nilai signifikansi 0,00 < 0,005. Hal ini mutlak H_0 ditolak, sehingga dapat disimpulkan bahwa instalasi Suricata IDS benar-benar efektif dalam melakukan pertahanan terhadap serangan DOS.

Setelah mengetahui bagaimana hasil akhir dari analisis pre-test dan post-test, ada baiknya kita sajikan hasil pengujian dilihat dari sistem Suricata itu sendiri. Setelah Suricata IDS diaktifkan, secara otomatis Suricata akan mencatat apapun yang berjalan di trafik jaringan baik itu lalu lintas jaringan normal maupun serangan. Di bawah ini adalah hasil dari pengujian post-test :

Tabel 4.6 Deteksi serangan

pengujian	deteksi
1	1419
2	2837
3	6038
4	9724
5	16705

Dari rangkaian pengujian dan analisis terhadap penggunaan memori baik sebelum dan sesudah diinstall Suricata dapat disimpulkan bahwa meskipun penggunaan memori setelah diinstall Suricata lebih tinggi dibanding memori yang digunakan sebelum adanya instalasi Suricata, akan tetapi Suricata mampu menghasilkan *alert* berupa output http.log, fast.log dan stats.log yang masing-masing dapat menerangkan dari mana penyerang berasal baik berupa informasi IP address yang digunakan, http header yang dikirim maupun jenis serangan yang digunakan. Di bawah ini adalah contoh output http.log dan fast.log :



Gambar 4.8 Output http.log

Dapat dilihat dari gambar di atas bahwa Suricata mampu mengenali IP address yang telah melakukan IP Flooding adalah 192.168.1.1.

Gambar 4.9 Output fast log

Serangan yang berhasil dideteksi berupa TCPv4 invalid checksum dengan klasifikasi keamanan tingkat 3 dari IP address 192.168.1.2 yaitu IP Flooding. Deteksi ini berjalan sesuai dengan *rule* yang telah dibuat didalam folder /etc/suricata/rules.

5. KESIMPULAN

Berdasarkan hasil analisa dan pembahasan dapat diperoleh kesimpulan bahwa penelitian "Analisis Sistem Deteksi Serangan Keamanan Jaringan Menggunakan Suricata" dengan menggunakan sistem operasi Ubuntu LTS 12.04.2 desktop dengan memanfaatkan tools attacker

Siege bawaan sistem operasi Kali Linux memperlihatkan bahwa Suricata dapat menangani serangan dengan baik. Hal ini dapat dilihat dari penggunaan memori yang baik. Didukung pula Suricata dapat mendeteksi adanya serangan DOS.

Hasil analisis uji T sampel dependen membuktikan bahwa server dengan bantuan Suricata IDS dapat meredam lebih banyak daripada server yang berjalan tanpa diinstall Suricata IDS.

DAFTAR PUSTAKA

Al Fatta, H. (2007). *Analisis dan Perancangan Sistem Informasi untuk Keunggulan Bersaing Perusahaan & Organisasi Modern.* Yogyakarta: CV. Andi Offset.

Albin, E. (2011). *A Comparative Analysis of The Snort and Suricata Intrusion-Detection Systems.* Monterey: Naval Postgraduate School.

Alexander, L. A. (2010, November 19). *Ancaman keamanan data dan jenis gangguan.* Retrieved Desember 5, 2013, from Double klikk: http://dobelklikk.wordpress.com/2010/11/19/ancaman-keamanan-data-dan-jenis-jenis-gangguanancaman/

Complete list of Suricata Features. (n.d.). Retrieved March 20, 2014, from Suricata IDS: http://suricata-ids.org/features/all-features/

cyruslab. (2012, 10 18). *Building an IDS : installing snorby, suricata and barnyard2.* Retrieved March 24, 2014, from The Network Journal: http://cyruslab.net/2012/10/18/building-an-ids-part-1-installing-pre-requisites-and-snorby/

Day, D. J., & Burns, B. M. (2011). ICDS 2011. *A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines* , 187-192.

firnsy. (n.d.). *Barnyard2.* Retrieved March 24, 2014, from Github.com: https://github.com/firnsy/barnyard2

Fuzi, F. (2011). *An Analysis of Intrusion Detection System.* Melaka: Universiti Teknikal Malaysia Melaka.

Kacha, C., & Shevade, K. A. (2012). IJETAE_1212_44. *Comparison of Different Intrusion Detection and Prevention Systems* , 243-245.

Keamanan Jaringan. (2013, April 11). Retrieved Desember 05, 2013, from Wikipedia: http://id.wikipedia.org/wiki/Keamanan_jaringan

Kusumawati, M. (2010). *Implementasi IDS (Intrusion Detection System) Serta Monitoring Jaringan dengan Interface Web Berbasis Base pada Keamanan Jaringan.* Depok: UI Press.

L. Person, L., & S. Davie, B. (2012). *Computer Networks: A Systems Approach.* Elsevier.

McRee, R. (2010). ISSA Journal. *Suricata: An introduction* , 40-42.

Meghanathan, D. N. (2012). *Intrusion Detection Systems.* Jackson State University.

Messer, W. H. (2011). *Performance Testing Suricata : The Effect of Configuration Variables On Offline Suricata Performance.* Georgia Institute of Technology.

Messer, W. H. (2011). *Performance Testing Suricata: The Effect of Configuration Variables On Offline Suricata Performance.* Georgia Institute of Technology.

Mulyono. (2013). *Perancangan dan Implementasi Sistem Monitoring Jaringan LAN (Local Area Network) dengan Notifikasi SMS.* Yogyakarta: UIN Sunan Kalijaga.

Naimzada, A. K., Stefani, S., & Torriero, A. (2009). *Networks, Topology and Dynamics: Theory and Applications to Economics and Social Systems.* Milano: Springer.

Panwar, S. S., Mao, S., Ryoo, J. d., & Li, Y. (2004). *TCP/IP Essentials : A Lab-Based Approach.* Cambridge University Press.

Putri, L. (2011). *Implementasi Intrusion Detection System (IDS) Menggunakan Snort pada Jaringan Wireless.* Jakarta: UIN Syarif Hidayatullah.

Qudratullah, M. F., & Suphandi, E. D. *Handout Praktikum Metode Statistika.* Yogyakarta.

Rahardjo, B. (2005). *Keamanan Sistem Informasi Berbasis Internet.* Jakarta: PT Insan Infonesia & PT INDOCISC.

Rob. (2013, July 2). *What is Linux.* Retrieved March 20, 2014, from Linux.org: http://www.linux.org/threads/what-is-linux.4076/

Saputra, A. (2005). *Pengembangan perangkat wireless IDS (Intrusion Detection System) berbasis embedded sytem .* Jakarta: UIN Syarif Hidayatulloh.

Stammler, J. H. (2011). *Suricata Performance White Paper.*

Syafrizal, M. (2005). *Pengantar Jaringan Komputer.* Yogyakarta: Andi.

Yuhefizar. (2008). *10 Jam menguasai internet, teknologi dan aplikasinya.* Jakarta: Elex Media Komputindo.