Implementasi Metrik Keluaran Unjuk Kerja Network Intrusion Detection System

(Output Metrics Implementation Performance Network Intrusion Detection System)

YUDHI ARDIYANTO

ABSTRACT

Perfomance of Network Intrusion Detection System (NIDS) very important to be monitored, because this system must perform packet inspection on computer network. Failure to detect data packets can produce malicious packet sneak into networks. Snort is one of the NIDS plug ins in the form of perfomance statistics that will provide performance information in real time, in the form of comma delimited value format. It takes long time to generated performance information. Thepigdoktah is a tools that can be used to process the output performance of the NIDS to be more informative .This research has been successfully implemented on a computer network, one of the performance information that can be generated is the average packet loss amounted to 0,012%.

Keywords: Network Intrusion Detection System, Network Security, Snort

PENDAHULUAN

Ancaman terhadap keamanan jaringan komputer semakin lama semakin meningkat seiiring dengan berkembangnya teknologi jaringan komputer yang mengalami peningkatan yang cukup signifikan dalam beberapa tahun terakhir. Salah satu cara untuk mendeteksi adanya ancaman tersebut adalah dengan melakukan implementasi NIDS pada jaringan yang akan dilindungi. Sistem tersebut akan mengirimkan peringatan (*alert*) apabila berhasil mendeteksi adanya serangan. Terdapat dua isu jenis peringatan sampai saat ini yaitu *false positive* dan *false negative*. *False positive* merupakan suatu peristiwa dimana NIDS akan menghasilkan alarm di mana sebetulnya tidak terjadi serangan. *False negative* didefinisikan sebagai suatu peristiwa yang tidak menghasilkan alarm padahal sebenarnya terjadi serangan (Vijarani dan Maria, 2015).

False negative dapat terjadi dikarenakan beberapa faktor. Salah satunya adalah kegagalan NIDS dalam melakukan inspeksi paket dari lalu lintas data. Kegagalan untuk melakukan pemeriksaan terhadap paket data tersebut akan menyebabkan kemungkinan tidak semua paket dapat diperiksa, hal ini tentu saja dapat membahayakan keamanan jaringan (Salah dan Kahtani 2009).

Pengamatan unjuk kerja dari NIDS perlu dilakukan, hal ini sebagai sarana untuk mengetahui kinerja pada saat proses pendeteksian, yang nantinya dapat berfungsi sebagai bahan pertimbangan dalam melakukan konfigurasi agar mempunyai perfoma yang lebih baik. Snort merupakan salah satu produk NIDS. Terdapat komponen yang disebut sebagai *preprocessor*. Secara umum komponen ini berfungsi sebagai suatu modul yang berfungsi mengambil paket yang mempunyai potensi yang berbahaya yang kemudian dikirim ke *detection enggine* untuk dikenali polanya. Mode statistik *perfomance* dapat diaktifkan dengan melakukan konfigurasi terlebih dahulu. Keluaran dari unjuk kerja tersebut mempunyai format *Comma Separated Values* (CSV). Format tersebut mempunyai bentuk yang relatif lebih sulit untuk dilakukan analisa (Snort.org, 2016). *Thepigdoktah* merupakan perangkat lunak

yang digunakan sebagai sarana menganalisa unjuk kerja keluaran dari Snort. Hasilnya berupa metrik yang lebih informatif dan mudah untuk dianalisa (Cumming, 2010).

Penelitian mengenai unjuk kerja NIDS dalam mendeteksi adanya serangan sudah banyak sekali dilakukan. Diantara penelitian tersebut adalah analisa unjuk kerja penggunaan sumber *Central Processing Unit* (CPU) antara dua produk NIDS, yaitu Suricata dan Snort (Day dan Burns, 2011). Membandingkan unjuk kerja Snort NIDS dalam mendeteksi adanya serangan yang diinstal pada sistem operasi Windows 7 dan Windows Server 2008 (Salah et al., 2011). Penelitian ini akan melakukan implementasi metrik keluaran unjuk kerja NIDS yang lebih informatif dengan memanfaatkan perangkat lunak *Thepigdoktah* pada sistem operasi Centos. Implementasi sistem yang sejenis dengan ini sudah banyak dilakukan, perbedaan terletak pada topologi jaringan yang digunakan.

DASAR TEORI

Intrusion Detection System (IDS)

Intrusion detection adalah usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi atau seorang *user* yang sah tetapi menyalahgunakan hak akses sumber daya sistem. IDS atau Sistem Deteksi Penyusupan adalah sistem komputer (bisa merupakan kombinasi perangkat lunak dan keras) yang berusaha melakukan deteksi adanya penyusupan dalam jaringan komputer. IDS akan melakukan pemberitahuan saat mendeteksi sesuatu yang dianggap sebagai tindakan ilegal dan mencurigakan. Pengamatan untuk melakukan pemberitahuan itu bergantung pada seberapa baik konfigurasi IDS yang telah dilakukan. IDS tidak melakukan pencegahan akibat terjadinya penyusupan (Balasubramaniyan et al., 2007).

Dilihat dari cara kerja dalam menganalisa apakah paket data dianggap sebagai penyusupan atau tidak, IDS dibagi menjadi *Signature-based* dan *Anomaly-based* IDS. *Signature-based* bekerja dengan cara menyadap paket data kemudian membandingkannya dengan basis data *rules* IDS (berisi pola-pola serangan). Jika paket data mempunyai pola yang sama dengan (setidaknya) salah satu pola di *database rules* IDS, maka paket tersebut dianggap sebagai serangan, dan jika paket data tersebut sama sekali tidak mempunyai pola yang sama dengan pola di basis data *rules* IDS, maka paket data tersebut dianggap bukan serangan. *Anomaly based* dapat mendeteksi adanya penyusupan dengan mengamati adanya keanehan pada sistem. Keanehan tersebut akan dibandingkan dengan situasi normal yang ada pada sistem. Tipe serangan baru sangat efektif dideteksi dengan model ini.

Berdasarkan kemampuan mendeteksi adanya penyusupan pada jaringan dapat dikelompokan ke dalam dua kategori, yaitu *Host-Based Instrusion Detection System* (HIDS) dan *Network Instrusion Detection System* (NIDS). HIDS dipasang pada sistem yang akan dimonitor. IDS ini hanya memonitor data, baik data yang berasal dari sistem tersebut maupun data yang menuju sistem tersebut. NIDS merupakan sebuah sistem yang diterapkan secara strategis pada segmen jaringan untuk mendeteksi serangan yang ditujukan pada host yang ada di jaringan itu. NIDS dapat memonitor banyak segmen jaringan dan menghasilkan sejumlah laporan serangan yang muncul di seluruh jaringan. Senua data yang berjalan pada jaringan ditangkap dan dianalisis.

Snort

Snort merupakan *open source* IDS yang dikembangkan oleh Martin Roesch dan Brian Caswell. IDS ini ringan dan mampu berjalan pada sistem operasi berbasis Linux maupun Windows. Snort merupakan *packet sniffing* yang ringan, mudah dalam proses instalasi dan konfigurasinya. Snort termasuk ke dalam *signature based* IDS yang tersusun atas beberapa komponen seperti *packet sniffer* atau penyadap paket merupakan aplikasi yang dapat melihat lalu lintas data pada jaringan komputer. Paket yang telah berhasil di tangkap oleh *packet sniffer akan* dikodekan sesuai dengan struktur yang diinginkan agar dapat diproses ke tahap selanjutnya, proses tersebut disebut dengan nama *decoder*. Paket yang telah di klasifikasikan oleh *preprocessor* akan diolah oleh *detection engine*, dengan cara membandingkan dengan *rules* untuk mendapatkan *alert*, apabila paket ada yang

cocok dengan *database rules* maka akan paket tidak cocok dengan basis data *rules* maka paket akan diteruskan. *Rules* IDS merupakan deretan teks berisi daftar aturan yang strukturnya sudah diketahui. Strukturnya meliputi protokol, *Internet Protocol* (IP) *address*, *port* dan lain-lain. *Output plugins* merupakan suatu modul yang mengatur format keluaran untuk *alert* sesuai dengan kebutuhan yang diinginkan. Dapat disimpan dalam *database* maupun *log file* (Michael et.al, 2005).

Snort Perfomance Statistics

Modul *plug in performance statistics* digunakan sebagai modul yang berguna untuk mengetahui unjuk kerja dari NIDS secara *real time*. Modul ini dapat diaktifkan dengan melakukan konfigurasi pada *file snort.conf*, Hilangkan tanda "#" di depan baris "*preprocessor perfmonitor: time 300 file /var/log/snort.stats pktcnt 10000*". *Time* 300 merupakan jumlah interval dalam satuan detik. *File /var/log/snort.stats* merupakan hasil keluaran unjuk kerja yang akan disimpan pada direktori */var/log* dengan nama *snort.stats*. *Pktcnt 10000* berfungsi untuk menyesuaikan jumlah paket yang akan diproses. Secara *default* bernilai 10000 (Snort.org, 2016).

METODOLOGI PENELITIAN

Pada tahapan ini akan dijabarkan mengenai metodologi yang digunakan dalam penelitian ini, yaitu berupa alat yang digunakan dan jalannya penelitian. Penelitian ini menggunakan perangkat lunak (*software*) dan perangkat keras (*hardware*). Tabel 1 menunjukan perangkat keras yang digunakan pada penelitian ini.

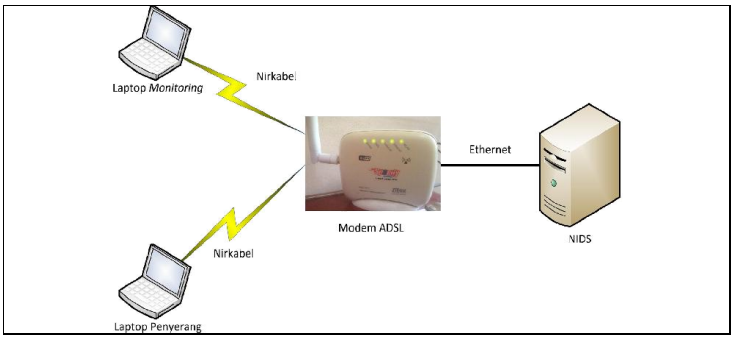
dinyatakan sebagai *alert*, sedangkan apabila

Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Snort
b. Data AcQuisition (DAQ) Library 2.0
c. Libpcap
d. Thepigdoktah
e. Perl
f. *Network Mapper* (NMAP)
g. Putty

Selain *software*, penelitian ini menggunakan beberapa perangkat keras (*hardware*). Perangkat terdiri dari server NIDS berupa mini *Personal Computer* (PC), laptop *monitoring* yang digunakan untuk memonitor aktivitas NIDS dan laptop penyerang yang digunakan untuk melakukan simulasi penyerangan baik ke server NIDS. Semua perangkat dapat terhubung ke internet melalui modem *Asymmetric Digital Subscriber Line* (ADSL) menggunakan akses internet *Speedy* dari PT. Telkom dengan kecepatan *up to* 512 *Kilo bit per second* (Kbps). *Server* NIDS langsung terhubung ke *ethernet* modem, sedangkan laptop penyerang dan *monitoring* terhubung ke jaringan melalui media nirkabel. Topologi tersebut dapat dilihat pada Gambar 1.

Konfigurasi IP *address server* NIDS dibuat statis yaitu 192.168.1.251/24, *gateway* 192.168.1.254 dan *Domain Name System* (DNS) 8.8.8.8. Laptop penyerang dan *monitoring* memperoleh IP *address* dari *Dynamic Host Configuration Protocol* (DHCP) *server* modem ADSL. Laptop penyerang digunakan untuk menguji apakah NIDS sudah berhasil mendeteksi adanya serangan. Setelah berhasil, akan dipergunakan untuk melakukan aktivitas seperti *browsing*, mengirim *email* dan lain sebagainya.



GAMBAR 1. Topologi implementasi NIDS pada jaringan

TABEL 1. Perangkat keras (*hardware*)

No.	Nama Perangkat	Spesifikasi	IP *Address*
1	Server NIDS	Processor Intel Atom N 270 CPU 1.6 GHz, RAM 1 GB, Hard Disk 230 GB, Sistem operasi Centos 6.6.	192.168.1.251/24
2	Modem Telkom *Speedy*	Modem ADSL terdapat 2 buah *Ethernet* dan *wireless*	192.168.1.254/24
3	PC Penyerang	Intel(R) Core i5 CPU 2.5 Ghz, Memori 4 GB, Hard Disk 256 GB, dengan Sistem Operasi Sierra	DHCP
4	PC *Monitoring*	Intel(R) Core(TM)2 CPU T5300 @1,73Ghz (2CPUs), Memori 2 GB, Hard Disk 80 GB, dengan Sistem Operasi Windows 7	DHCP

HASIL DAN PEMBAHASAN

Pengujian awal dilakukan dengan menggunakan *software* NMAP. *Tool* tersebut dapat digunakan untuk melakukan audit keamanan jaringan. Skenarionya dilakukan dengan menjalankan *software* tersebut pada laptop penyerang dengan tujuaannya adalah *server* NIDS. Dari hasil pengujian diperoleh alert "nmap scan". *Alert* tersebut akan disimpan dalam wujud deretan teks yang disimpan pada direktori */var/log/snort* dengan nama *file alert.ids*.

[**] [1:1000003:1] nmap scan [**] [Classification: Detection of a Network Scan] [Priority: 1] 12/28-19:30:49.887718 192.168.1.7:1149 -> 192.168.1.251:22 TCP TTL:128 TOS:0x0 ID:6120 IpLen:20 DgmLen:48 DF******S* Seq: 0x408C3CA9 Ack: 0x0 Win: 0x2000 TcpLen: 28 TCP Options (4) => MSS: 1460 NOP NOP SackOK

Dari *alert* diatas membuktikan bahwa NIDS sudah sanggup melakukan pendeteksian adanya usaha ekplorasi dari laptop penyerang dengan IP *address* 192.168.1.7 ke *server* NIDS dengan IP *address* 192.168.1.251 menggunakan *tool* NMAP.

Proses pendeteksian mulai dilakukan pada tanggal 28 Desember 2016 sampai dengan 2 Januari 2017 dan menghasilkan metrik keluaran unjuk kerja NIDS. *File* tersimpan pada direktori */var/log* dengan nama snort berekstensi stats. Gambar 2 menunjukkan sebagian hasil unjuk kerja NIDS selama proses pendeteksian berlangsung berformat CSV. Thepigdoktah lebih mempermudah menganalisa unjuk kerja dari NIDS. Perintah yang digunakan adalah sebagai berikut :

[root@IDS-SENSOR-2~]#perl thepigdoktah.pl -r /var/log/snort.stats -s /var/log

Hasil perintah tersebut akan menghasilkan keluaran dengan format dibawah ini.

-= Tha Pig Doktah 0.1 Dev =-
Copyright (C) 2010 JJ Cummings

Report Info:
Processed: /var/log/snort.stats
First Entry: Wed Dec 28 19:27:03 2016
Last Entry: Mon Jan 2 09:51:10 2017
Time Span: 4 days, 14 hours, 24 minutes and 7 seconds

Wirespeed:
High: 0.665 Mbits/Sec | Wed Dec 28 20:43:16 2016
Low: 0.000 Mbits/Sec | Fri Dec 30 12:11:18 2016
Avg: 0.003 Mbits/Sec

% Packet Loss:
High: 0.311% | Wed Dec 28 20:43:38 2016
Low: 0.006% | Thu Dec 29 13:59:36 2016
Avg: 0.012%

Additional Info:
Avg Pkt Size: 92.648 bytes
Avg Syns/Sec: 0.001
Avg SynAcks/Sec: 0.001
Avg Alerts/Sec: 0.059
Avg Current Cached Sessions: 0.009

```
################################## Perfmon stop: pid=2572 at=Wed Dec 28 17:47:10 2016 (
################################## Perfmon start: pid=3048 at=Wed Dec 28 17:49:06 2016
#time,pkt_drop_percent,wire_mbits_per_sec.realtime,alerts_per_second,kpackets_wire_per_s
1482928023,0.000,0.001,0.000,0.001,149,112.969,0.001,0.001,0.001,0.001,0,3,0.017,0,302,0
1482932296,0.000,0.002,0.001,0.001,222,401.784,0.014,0.010,0.011,0.010,10,19,0.013,0,289
1482932318,0.000,0.010,0.000,0.002,511,662.322,0.033,0.023,0.025,0.023,10,19,0.068,0,150
1482932596,0.000,0.665,0.010,0.112,744,707.312,0.067,0.047,0.050,0.077,2,19,4.571,0,101,
1482932618,0.000,0.585,0.000,0.100,735,704.504,0.067,0.047,0.050,0.080,1,19,4.035,0,101,
1482933004,0.000,0.147,0.002,0.024,753,719.228,0.020,0.005,0.007,0.007,2,19,1.010,0,17,0
1482933008,0.000,0.157,0.000,0.026,765,720.701,0.020,0.005,0.008,0.005,2,19,1.070,0,15,0
################################## Perfmon start: pid=8568 at=Thu Dec 29 05:54:34 2016
#time,pkt_drop_percent,wire_mbits_per_sec.realtime,alerts_per_second,kpackets_wire_per_s
1482994776,0.000,0.000,0.001,0.000,133,143.328,0.000,0.000,0.000,0.000,0,2,0.003,0,219,0
################################## Perfmon start: pid=18626 at=Thu Dec 29 21:04:30 2016
#time,pkt_drop_percent,wire_mbits_per_sec.realtime,alerts_per_second,kpackets_wire_per_s
```

GAMBAR 2. Sebagian data snort.stats berformat CSV

Dari perintah tersebut dapat diperoleh bahwa lama proses pendeteksian selama 4 hari, 14 jam 24 menit dan 7 detik. Kecepatan data tertinggi yang melewati *ethernet server* NIDS sebesar 0,665 Mbps, hal ini sesuai dengan batas maksimal kecepatan internet yang dilanggan yaitu sebesar *up to* 512 Kbps. dan terendah sebesar 0 Mbps. Kondisi tersebut dapat terjadi dikarenakan disisi jaringan lokal tidak ada aktivitas baik itu *browsing* maupun *monitoring* ke *server* NIDS. *Packet lost*

terbesar terjadi pada tanggal 28 Desember 2016 pukul 20.43.38 sebesar 0,311% dan terkecil 0,006% pada tanggal 29 Desember 2016 pukul 13.59.36 dengan rerata *packet loss* sebesar 0,012%. Informasi tambahan berupa rerata ukuran paket yang dianalisa sebesar 92,648 bytes. *Alert* yang berhasil terdeteksi tiap detiknya sebesar 0,059. Rerata Syns dan SynAck tiap detiknya sebesar 0,001. Rata-rata *Current Cached Sessions* bernilai 0,009

KESIMPULAN

Metrik keluaran unjuk kerja NIDS telah berhasil diimplementasikan ke dalam jaringan. Thepigdoktah mempermudah menganalisa data unjuk kerja NIDS yang berformat CSV menjadi lebih informatif. Diperoleh bahwa rerata kecepatan data yang melewati *server* sebesar 0.003 Mbps, rata-rata besarnya *packet loss* sebesar 0.012%.

Saran untuk penelitian berikutnya adalah informasi unjuk kerja yang telah berhasil diperoleh dapat dikirim secara otomatis kepada *administrator* jaringan secara periodik melalui *email*. Diperlukan *tool* tambahan seperti *Multi Router Traffic Grapher* (MRTG) untuk memastikan kecepatan data yang melewati *ethernet* dengan *output* yang dihasilkan oleh snort *performance monitor*, sehingga dapat diketahui keakuratan seberapa kecepatan data yang melewati *server* NIDS.

DAFTAR PUSTAKA

Balasubramaniyan D.Z.J, Frenandez J.O.G, Isacoff D, Spafford E. (1998). An architecture for intrusion detection using autonomous agents. Proceeding of Computer Security Application. (pp.13-24).

Cummings J.J(2010). Thepigdoktah. Available:https://code.google.com/p/thepigdoktah/. □

Kamaruzaman Maskat, Mohd Afizi Mohd Shukran, Mohammad Adib Khairuddin & Mohd Rizal Mohd Isa (2011). Mobile Agents in Intrusion Detection System: Review and Analysis. Modern Applied Science Vol. 5, No. 6; December 2011. National University Defense University of Malaysia.

Michael J.B, Orebaugh A, Clark G, Becky Pinkard B (2005). □Intrusion Prevention And Active Response Deploying Network And Host Ips. Syngress□

Snort.org (2016). Users Manual Snort 2.9.9.0 □

Salah K, & Kahtani K, (2009). Improving Snort performance under Linux. IET Commun., Vol. 3, Iss. 12, (pp.1883–1895)

Salah K, Al-Khiyati M, Ahmed R, Mahdi A (2011). Performance Evaluation of Snort under Windows 7 and Windows Server 2008. Journal of Universal Computer Science, vol. 17, no. 11, (pp.1605-1622)

Vijayarani S and Maria S.S (2015). Intrusion Detection System – A Study. International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1 (pp.31-44)

PENULIS:

Yudhi Ardiyanto

Program Studi Teknik Elektro, Fakultas Teknik, Universitas Muhammadiyah Yogyakarta, Jalan Lingkar Selatan, Tamantirto, Kasihan, Bantul 55183, Yogyakarta.

Email: yudhi.ardiyanto@umy.ac.id