ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU

NASKAH PUBLIKASI

Disusun Oleh :

Alim Nuryanto

Muhammad Kusban, S.T, M.T

PROGRAM STUDI INFORMATIKA

FAKULTAS KOMUNIKASI DAN INFORMATIKA

UNIVERSITAS MUHAMMADIYAH SURAKARTA

2015

HALAMAN PENGESAHAN

Publikasi ilmiah dengan judul :

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, BARNYARD2 PADA VPS UBUNTU

Telah disetujui pada :

Hari : Jum'at

Tanggal : 24 Juli 2015

Pembimbing,

(Muhammad Kusban, S.T, M.T)

NIK : 663

Publikasi ilmiah ini telah diterima sebagai persyaratan untuk memperoleh gelar sarjana

Tanggal 30 Juli 2015

Mengetahui

Ketua Program Studi

Informatika

Dr. Heru Supriyono, M.Sc.

NIK : 970

UNIVERSITAS MUHAMMADIYAH SURAKARTA
FAKULTAS KOMUNIKASI DAN INFORMATIKA
PROGRAM STUDI INFORMATIKA
Jl. A Yani Tromol Pos I Pabelan Kartasura Telp. (0271)717417, 719483 Fax (0271) 714448
Surakarta 57102 Indonesia. Web: http://informatika.ums.ac.id. Email: informatika@fki.ums.ac.id

SURAT KETERANGAN LULUS PLAGIASI

/A.3-II.3/INF-FKI/VIII/2015

Assalamu'alaikum Wr. Wb

Biro Skripsi Program Studi Informatika menerangkan bahwa :

Nama	:	ALIM NURYANTO
NIM	:	L200110022
Judul	:	ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU
Program Studi	:	Informatika
Status	:	**Lulus**

Adalah benar-benar sudah lulus pengecekan plagiasi dari Naskah Publikasi Skripsi, dengan menggunakan aplikasi Turnitin.

Demikian surat keterangan ini dibuat agar dipergunakan sebagaimana mestinya.

Wassalamu'alaikum Wr. Wb

Surakarta, 6 Agustus 2015

Biro Skripsi
Informatika

Adjie Sapoetra, S.Kom

Turnitin Originality Report

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU by Alim Nuryanto

From publikasi september 2015 (publikasi)

Processed on 03-Aug-2015 15:37 WIB
ID: 559232207
Word Count: 2010

Similarity Index	Similarity by Source	
10%	Internet Sources:	6%
	Publications:	0%
	Student Papers:	6%

sources:

1 2% match (student papers from 10-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554918914

2 2% match (student papers from 06-Jul-2015)
Class: publikasi
Assignment:
Paper ID: 554221324

3 1% match (student papers from 06-Feb-2014)
Class: publikasi maret 2014
Assignment:
Paper ID: 394090721

4 1% match (Internet from 23-Jun-2015)
http://digilib.unpas.ac.id/files/disk1/7/jbptunpaspp-gdl-yuanharryp-331-1-bab1--i.pdf

5 1% match (student papers from 23-Mar-2015)
Class: publikasi
Assignment:
Paper ID: 519457794

6 1% match (Internet from 09-Jun-2015)
http://repository.amikom.ac.id/files/Publikasi_09.11.2743.pdf

7 1% match (Internet from 31-Dec-2014)
http://news.palcomtech.com/wp-content/uploads/2013/03/ZAID_TE02032012.pdf

8 1% match (Internet from 09-Oct-2010)
http://www.darknet.org.uk/tag/intrusion-detection/

9 1% match (Internet from 10-Jun-2012)
http://repository.politekniktelkom.ac.id/Proyek%20Akhir/MI/PENGEMBANGAN%20MODUL%20REPORTING%20TREASURY%20PADA%

10 < 1% match (Internet from 10-Jan-2014)
http://repository.amikom.ac.id/files/Publikasi%2009.12.3598.pdf

11 < 1% match (Internet from 03-Nov-2012)
http://iko4x.com/tutorial.html

12 < 1% match (Internet from 19-May-2014)
http://www.bcasyariah.co.id/media/2011/05/Annual-Report-BCAS-2010.pdf

paper text:

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU NASKAH PUBLIKASI Disusun Oleh : Alim Nuryanto

3**Muhammad Kusban, S.T, M.T PROGRAM STUDI INFORMATIKA FAKULTAS KOMUNIKASI DAN INFORMATIKA UNIVERSITAS MUHAMMADIYAH SURAKARTA** 2015 **HALAMAN PENGESAHAN Publikasi ilmiah dengan judul** : ANALISIS **DAN**

IMPLEMENTASI SURICATA, SNORBY, BARNYARD2 PADA VPS UBUNTU

2**Telah disetujui pada : Hari : ..... Tanggal : ..... Pembimbing, (Muhammad Kusban, S.T, M.T)**

ANALISIS DAN IMPLEMENTASI SURICATA, SNORBY, DAN BARNYARD2 PADA VPS UBUNTU

Alim Nuryanto, Muhammad Kusban, S.T, M.T

Informatika, Fakultas Komunikasi dan Informatika

Universitas Muhammadiyah Surakarta

E-mail : alimnurss@gmail.com

ABSTRAK

Server merupakan perangkat yang telah ter-integrasi dengan spesifikasi *hardware* tertentu, dan *software* yang memiliki fungsi tertentu seperti ftp, ssh, web server. Layanan tersebut rentan akan serangan yang dapat menimbulkan kerugian. Oleh karena itu diperlukan sistem pendukung yang mampu mendeteksi sebuah aktifitas jaringan. Suricata adalah IDS yang mambu mendeteksi sebuah aktifitas jaringan dan mengidentifikasi ancaman serangan dibantu dengan *rules* yang ter-intergasi. Suricata memindai setiap datagram yang dikirim pada sesi TCP dan mengubah menjadi informasi dan dikirim pada pada aplikasi Snorby untuk diolah. *Rules* pada suricata berperan dalam mengidentifikasi serangan yang terjadi pada sebuah host.

Kata kunci : Server, *Suricata, Snorby, Rules, IDS*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini khususnya pada sistem jaringan komputer sangatlah cepat. Bahkan sekarang semua komunikasi terutama komunikasi data bisa dilakukan dengan sistem jaringan yang telah ter-integrasi. Berkembangnya sistem jaringan komputer bukan berarti tanpa kelemahan. *Server* merupakan perangkat yang telah ter-integrasi dengan spesifikasi *hardware* tertentu, dan *software* yang memiliki fungsi tertentu seperti *web server, dns server, proxy server, dll.* Oleh karena itu, perlu para administrator untuk lebih berhati – hati dalam mengelola *server*. Jika dalam pengawasan sistem jaringan terutama pada *server* terjadi gangguan lalu lintas data seperti, lalu lintas data penuh yang dapat menimbulkan masalah pada sistem jaringan itu sendiri.

Suricata merupakan *software* yang bisa digunakan untuk melakukan kegiatan *Network IDS, IPS* dan *Network Security Monitoring engine.* Suricata merupakan *software Open Source* yang dikembangkan oleh organisasi *non-profit* dari *Open Information Security Foundation (OISF).* Snorby dan Barnyard2 adalah *software* yang dapat digunakan untuk melakukan *remote* pada sebuah *server* yang telah terpasang *IDS, IPS* dan *NSM.* Penggunaan *VPS* dapat menggantikan dedicated server untuk penelitian dengan spesifikasi lebih rendah serta hemat biaya.

2. TINJAUAN PUSTAKA

Network Information Detection System (NIDS) biasa disebut dengan sensor keamanan. NIDS adalah teknologi *hardware* ataupun *software* yang telah terintegrasi dan berfungsi sebagai *Detection System.* Dalam sebuah analogy, NIDS ditunjukkan untuk mendengarkan sebuah frase kunci dari sebuah paggilan daripada melaporkan statistik panggilan

itu sendiri. (*Network Security Monitoring 1st edition,* 2009, Hal 101-102).

Suricata engine merupakan *open source next generation intrusion detection and prevention engine.* Suricata merupakan *engine* yang memiliki kemampuan *Multi threaded.* Hal ini dapat diartikan kita dapat menjalankannya secara instan dan mengaturnya secara seimbang dalam setiap pemrosesan sensor Suricata yang telah terkonfigurasi (*Suricata-ids*, 2015:1).

Snorby adalah web aplikasi network *security monitoring* antarmuka yang populer dengan *instrusi detection system* (Snort, Suricata, dan Sagan). Konsep dasar pada snorby adalah sederhana, organisasi, dan kekuatan. Tujuan besar dari pembuatan snorby adalah membuat aplikasi open source dan sangant komprehentif untuk monitoring jaringan yang dapat digunakan untuk pribadi maupun pBarnyard2 adalah software open source interpreter untuk snort unified2 binary output files. Memiliki fungsi utama untuk menulis pada disk dengan efektif dan meninggalkan parsing dalam berbagai format data biner dengan proses yang terpisah tanpa meyebabkan Snort kehilangan network traffic.erusahaan. supporting vendors.

3. METODE PENELITIAN

Metode penelitian yang digunakan oleh peneliti adalah metode penelitian eksperimental yaitu teknik penelitian yang digunakan untuk mengetahui suatu kondisi sebuah sistem yang diimplementasi setelah mendapakan pengujian yang berbeda - beda.

3.1 Waktu dan Tempat

Waktu yang digunakan dalam penelitian ini adalah sekitar 6 bulan yakni bulan Februari 2015 sampai dengan Juli 2015 yang dilakukan pada indekost Najma yang terletak di area Universitas Muhammadiyah Surakarta.

3.2 Peralatan Utama dan Pendukung

Peralatan Utama

Notebook dengan spesifikasi sebagai berikut :

1) *Hardware* :

a) Processor Intel® Core™ i3 , 2.2 Ghz,

b) Harddisk 465 GB.

2) *Software* :

a) Sistem Operasi Windows 7 Ultimate 64-bit,

b) Putty.

Virtual Private Server (VPS) berjumlah 2 dengan masing - masing spesifikasi sebagai berikut:

1) *Hardware* :

a) Dedicated RAM :256MB,

b) vSwap : 512MB,

c) HDD : 25GB,

d) Premium Bandwidth : 500GB,

e) CPU Cores : 2 Cores,

f) Public Uplink : 1000Mbps.

1) *Software* :

a) Sistem Operasi Ubuntu Server 12.00 32-bit,

b) SSH Server,

c) Apache Web Server,

d) MySQL Databases,

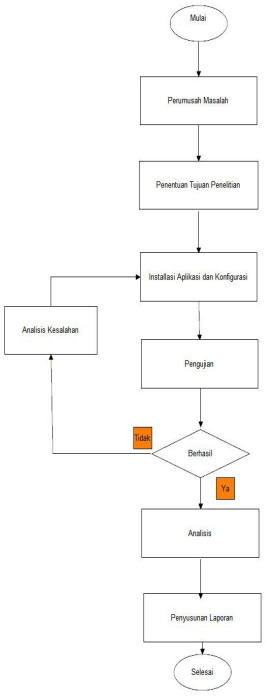
e) Suricata,

f) Barnyard2,

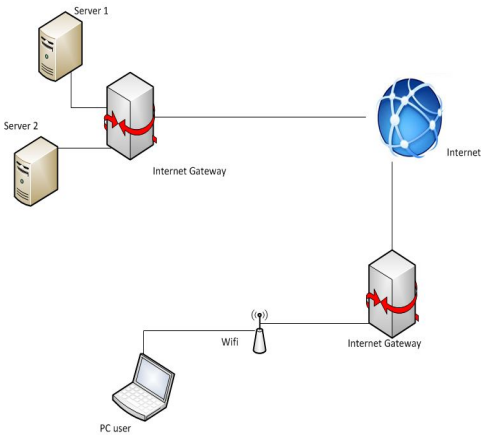
g) Snorby.

3.4. Alur Penelitian

Alur penelitian digunakan untuk mengetahui tahapan - tahapan dari penelitian. Berikut ini merupakan alur penelitian berdasarkan diagram alir dan topologi jaringan server 1 dan server 2 :



Gambar 3.1 Diagram Alir



Gambar 3.2 Topologi Jaringan

Berdasarkan gambar 3.1 alur peneltian adalah mengidentifikasi sebuah masalah dan dilanjutkan dengan penentuan tujuan dari penelitian. Selanjutanya adalah installasi dan konfigurasi sistem delanjutkan dengan pengujian apablila mengalami kegagalan maka akan dianalisa kesalah kemudian mengulangi dari installasi dan konfigurasi sistem. Ketika berhasil maka akan dilanjutkan dengan analisis kemudian penyusunan laporan.

Pada gambar 3.2 topologi ini menjelaskan bahwa Server 1 dan Server 2 berada dalam 1 Internet Gateway dikarenakan menggunakan VPS yang disewa dari tempat yang sama. Sedangkan PC user terhubung dengan wifi yang sudah terkoneksi dengan jaringan internet.

3.4.1 Pengujian *Request Packet Data*

Pengujian ini akan dilakukan *request packet* oleh PC *client* kepada Server 1 dengan meminta *packet* data dan dilakukan sebanyak 5 kali percobaan dengan besar bytes yang berbeda - beda. Berikut adalah tabel percobaan *request packet* pada server 1.

Tabel 3.1 *Request Packet Data*

No	Tanggal	Waktu	Besar Paket
1	12 Juli 2015	5.10 - 5.20	1 bytes
2	12 Juli 2015	6.01 - 6.11	10 bytes
3	12 Juli 2015	18.59 - 19.09	100 bytes
4	13 Juli 2015	3.46 - 3.56	1000 bytes
5	13 Juli 2015	15.35 - 15.45	10000 bytes

3.4.2 Pengujian Menggunakan Nmap

Pada tahapan pengujian ini peneliti menggunakan Nmap untuk melakukan *scanning* pada Server 1. *Scanning* dilakukan sebanyak 8 kali di dengan perintah yang berbeda.

3.4.3 Pengujian Menggunakan Tool

Hydra

Peneliti saat ini menggunakan tool hydra yang telah ada pada sistem operasi kali linux. Tools tersebut berfungsi untuk melakukan serangan *brute force* untuk mencari *user name* dan *password* yang digunakan untuk *login* pada *service* Server 1.

3.4.4 Pengujian Menggunakn Sqlmap

Sqlmap adalah tool yang bekerja menyerang sebuah layanan web server dengan cara menginjeksi melalui kelemahan URL pada sebuah Server. Peneliti hanya melakaukan pengujian sebanyak 1 kali dengan menggunakan tool ini.

3.4.5 Pengujian Menggunakan Metasploit Konsol

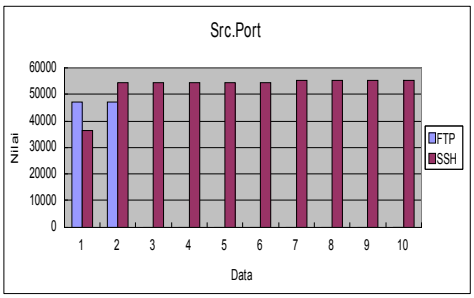
Peneliti menggunakan salah satu tool yang cukup terkenal yaitu Metasploit. Terdapat banyak *source exploit* yang dapat dijalankan pada tool ini. Penguji menggunakan 4 exploit yang berbeda untuk melakukan uji coba serangan pada Server 1 yang telah ter install aplikasi Suricata. Exploit yang digunakan oleh peneliti menyarang *service ftp, ssh, dan web server.*

4. HASIL DAN PEMBAHASAN

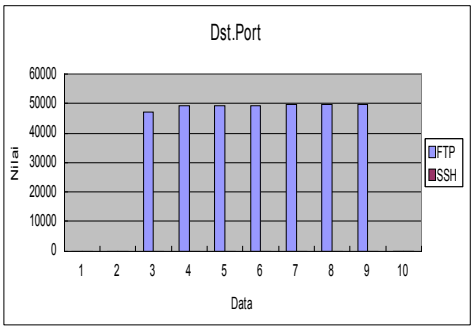
Dari tahapan - tahapan yang telah dilakukan oleh peneliti dalam rangka uji coba yang meliputi installasi, konfigurasi, dan pengujian aplikasi telah mendapatkan beberapa hasil yang sesuai dengan yang diharapkan oleh peneliti.

4.1 Hasil Pengujian

Dari ke 5 pengujian yang dilakukan oleh peneliti dengan menggunakan hydra, cmd, sqlmap, nmap dan metasploit konsol menghasilkan data yang didalamnya adalah informsai mengenai IP Header dan TCP Header dari sebuah sesi TCP. Berikut ini adalah contoh data yang telah dibuat menjadi diagram :



Gambar 4.1 Pengujian Hydra Src,Port TCP Header



Gambar 4.2 Pengujian Hydra Dst.Port TCP Header

Diagram tersebut menunjukan field - field yang ada pada TCP Header yang berhasil ditanggap keberadaannya oleh aplikasi Suricata dan dilaporakan ke aplikasi Snorby.

4.2 Pembahasan

4.2.1 Analisis Kebutuhan Sistem

Pada bagian analisis kebutuhan sistem ini akan dibagi menjadi 2 bagian utama, yaitu analisis kebutuhan fungsional dan analisis kebutuhan non-fungsional.

a. Analisis Kebutuhan Fungsional

Analisis kebutuhan fungsional menjelaskan tentang pemaparan proses - proses terjadinya pengolahan pada sistem dan fitur - fitur apa saja yang disediakan oleh sebuah sistem, serta menganalisis data apa saja yang dibutuhkan untuk pengujian pada sistem aplikasi yang diimplementasi. Sistem aplikasi yang tengah diuji ini memiliki kebutuhan fungsional sebagai berikut :

1) Aplikasi Suricata yang terdapat pada Server 1 mampu mendeteksi sebuah aktifitas pada server dengan cara melakukan pemindaian pada setiap fragment - fragment data,
2) Aplikasi Suricata dapat menganalisis bagian - bagian yang ada pada fragment data seperti *IP Header, TCP Header,*

dan *ICMP Header*.

3) Aplikasi Barnyard2 ini mampu menghubungkan antar server dan melakukan pengiriman *event, ip header information, tcp header information,* dan *icmp header information* kepada aplikasi Snorby yang terkonfigurasi pada Server 2,

4) Aplikasi Snorby yang ada pada Server 2 memiliki memiliki tampilan GUI sehingga memudahkan user.

b. Analisis Kebutuhan Non - Fungsional

Analisis Kebutuhan non - fungsional merupakan bagian yang akan membantu selesainya sebuah penelitian. Pada analisis ini akan dibedakan menjadi 2 bagian penting yaitu :

1) Analisis Kebutuhan Perangkat Keras

Merupakan analisis untuk mengetahui kebutuhan perangkat keras yang akan digunakan untuk menjalankan aplikasi. Perangkat keras harus memiliki spesifikasi minimum agar aplikasi dapat berjalan dengan baik.

Perangkat keras yang digunakan memiliki processor minimal pentium 3 dengan kebutuhan kebutuhan media penyimpanan 20 *Giga bytes* serta dedicated RAM sebesar 256 *Mega bytes*.

2) Analisis Kebutuhan Perangkat Lunak

Perangkat lunak adalah program yang

digunakan untuk menjalankan dan memberikan perintah pada perangkat keras komputer. Dengan adanya perangkat lunak perangkat keras yang ada pada sebuah komputer dapat berjalan sesuai dengan yang diinginkan. Agar aplikasi dapat berjalan maka diperlukan perangkat lunak minimal perangkat lunak yang ada adalah mysql dan apache2.

4.2.2 Analisis Pengujian Request Packet Data Pada Server 1

Suricata dapat melakukan pemindaian pada segmen - segmen ICMP yang terjadi pada server 1. Aktifitas tersebut kemudian disaring dan ditentukan oleh rule yang terkonfigurasi pada Server 1. Pada field *Total Length IP Header* ditemukan perbedaan nilai yaitu, 29, 128, 1028, ini dikarenakan perbedaan permintaan paket yang dikirim oleh host ke client.

4.2.3 Analisis Pengujian Scanning Menggunakan Nmap Pada Server 1

Suricata menangkap setiap transmisi yang terjadi pada sesi TCP. Semua aktifitas yang terjadi pada sesi TCP dipindai dan dikelompokkan oleh suricata sebagai gangguan. Hal ini terjadi karena suricata berhasil membuktikan bahwa dia dapat mengindikasi serangan dengan melihat besarnya field - field dalam sesi TCP.

4.2.4 Analisis Pengujian Tool Hydra

Tanda yang diidentifikasi sebagai serangan pada uji coba menggunakan Tool Hydra adalah besar *payload* pada setiap data yang dimasukkan pada sesi TCP.

4.2.5 Analisis Pengujian Menggunakan Tool Sqlmap

Tanda yang diidentifikasi sebagai serangan pada uji coba menggunakan Tool Sqlmap adalah pada *payload* yang dikirim pada sesi TCP. *Payload* yang dikirim pada sesi TCP ini mengandung permintaan konten sebuah URL yang dianggap oleh rule sebagai serangan pada Server 1.

4.2.6 Analisis Pengujian Menggunakan Metasploit Konsol

Percobaan pengujian menggunakan Metasploit Konsol suricata berhasil menangkap sesi pengiriman data. Suricata mengindikasi serangan dari *source exploit* dan *payload* yang dikirim oleh metasploit konsol seperti pada pengujian menggunakan Tool Sqlmap dan Tool Hydra.

5. PENUTUP

5. 1 Kesimpulan

Dari hasil data pengujian dan pembahasan dapat ditarik kesimpulan bahwa :

1. Aplikasi Suricata yang bekerja pada Server 1 mengidentifikasi serangan dengan membaca setiap datagram yang dikirim pada sesi TCP,
2. Datagram tersebut tidak dapat ditentukan sebagai tindakan serangan tanpa adanya *rules* yang mendukung untuk mengidentifikasi,
3. Serangan diidentifikasi dengan melihat besarnya field - field pada *TCP Header* seperti field flags dan window,
4. Serangan juga diidentifikasi pada *payload* yang dikirim melalui sesi TCP seperti percobaan login pada *service* FTP yang gagal secara terus menerus.
5. Aplikasi Snorby yang terinstall pada Server 2 dapat memberikan laporan yang sesuai dengan keadaan Server 1,

5.2 Saran

Dari hasil penulisan skripsi ini pastinya memiliki beberapa kekurangan yang kemungkinan dapat disempurnakan pada penelitian lain. Berikut saran yang dapat digunakan sebagai evaluasi :

1. Melakukan pengujian yang melibatkan serangan seperti DDOS ataupun memasukkan

virus,

Mencoba menggunakan fungsi *IPS* yang terdapat pada aplikasi suricata dan melakukan beberapa pengaturan pada *rules* untuk mencegah serangan.

DAFTAR PUSTAKA

Kusmayadi, Ismail. 2008. "*Think Smart Bahasa Indonesia"*. Bandung : Grafindo Media Pratama.

Javvin, 2005. *Network Protocols Handbook 2nd Edition.* USA : Saratoga.

Snyder, Garth dkk. 2007. *Linux Administration Handbook 2nd Edition. USA : Pearson Education, Inc.*

Wikipedia. (2014). *Putty.* diakses dari : http://en.wikipedia.org/wiki/PuTTY (Tanggal 18 September 2014)

Fry, Chris dkk. 2009. *Network Security Monitoring*. *USA : O'Reilly Media, Inc.*

OISF, 2015. "*Suricata Documentation"*. Diakses dari : https://redmine.openinfosecfoundation.org/projects/suricata/wiki (Tanggal 4 Juni 2015)

Wikipedia. (2014). *Payload (Computing)*. diakses dari : https://en.wikipedia.org/wiki/Payload_(computing) (Tanggal 21 Juli 2015)

Wikipedia. (2014). "*Protokol Internet"*. diiakses dari : https://id.wikipedia.org/wiki/Protokol_Internet (Tanggal 21 Juli 2015)

Wikipedia. (2014). *Transmission Control Protocol.* diakses dari : https://id.wikipedia.org/wiki/Transmission_Control_Protocol (Tanggal 21 Juli 2015)