PERANCANGAN APLIKASI PENGOLAHAN LOG DATA PACKET SNIFFER UNTUK MENDETEKSI SERANGAN INTERNET WORMS PADA JARINGAN KOMPUTER

Sugiharto[1], Lukas[2], Aloysius Adya Pramudita[3]
[1,2,3]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Katolik Indonesia Atma Jaya
Jl. Jenderal Sudirman no. 51, Jakarta 12930 - Indonesia
[1]gieharto@gmail.com, [2]lukas@atmajaya.ac.id, [3]pramudita@atmajaya.ac.id

ABSTRAK

Di tengah perkembangan teknologi, angka pengguna internet semakin meningkat setiap hari, namun keamanan dalam berselancar pada jaringan komputer/internet merupakan faktor yang sering kali dilupakan oleh penggunanya. Salah satu gangguan yang banyak terjadi pada jaringan komputer adalah penyebaran worms. Banyak upaya yang dapat dilakukan untuk menjaga keamanan dijaringan komputer tersebut contohnya adalah dengan melakukan pemeriksaan terhadap paket yang melintas pada jaringan tersebut, namun proses pengamatan tersebut akan menghasilkan suatu log data dalam jumlah yang sangat besar, yang akan memakan waktu untuk melakukan proses analisa. Penelitian ini bermaksud untuk mengembangkan suatu aplikasi untuk membantu mengolah log data hasil packet analyzer untuk menghasilan suatu laporan dengan cepat dan lebih akurat

Kata Kunci— Packet Analyzer, Network Analysis, Python, Worms, Raspberry Pi

1. PENDAHULUAN

Keamanan sudah menjadi salah satu perhatian utama sejak pertumbuhan komputer, jaringan komputer Secara berkelanjutan telah mendapat banyak ancaman keamanan, seperti virus, worms dan ancaman lainnya. Dari berbagai jenis ancaman tersebut *worms* merupakan ancaman yang paling menarik bagi peneliti keamanan komputer, karena kemampuannya untuk menginfeksi jutaan komputer dalam waktu yang singkat melalui media jaringan, yang dapat menyebabkan kerugian yang sangat besar akibat kerusakan yang diciptakan[1]

Banyak cara untuk bisa mengamanankan jaringan komputer Salah satu caranya adalah dengan melakukan analisis terhadap paket yang lewat pada jaringan adalah dengan menggunakan aplikasi *packet sniffer*. Aplikasi ini mampu menangkap informasi yang dikirimkan melalui jaringan. Banyak informasi berharga yang bisa didapat dengan menggunakan aplikasi *packet sniffer* seperti *username* dan *password*, yang akan sangat merugikan jika informasi berharga tersebut didapatkan oleh orang yang salah. Namun dalam mendapatkan informasi lalu lintas jaringan pada *packet sniffer* akan menghasilkan suatu log data dalam jumlah yang sangat besar, sehingga memakan waktu untuk melakukan analisis terhadap informasi yang didapat.

2. PRINSIP KERJA *WORM*

Worms sudah menjadi fenomena umum di Internet saat ini dan menyebabkan puluhan hingga ratusan milyar dolar dalam kerusakan pada bisnis di seluruh dunia setiap tahunnya. *Worm* bisa didefinisikan sebagai sebuah kode berbahaya/*script* (berdiri sendiri atau menginfeksi *file*) yang menyebar melalui jaringan, dengana atau tanpa bantuan manusia [2]. Secara prinsip *worm* terlihat mirip seperti sebuah virus, hanya saja *worm* secara mandiri dan tidak perlu menjadi bagian dari program lain untuk menyebarkan dirinya.

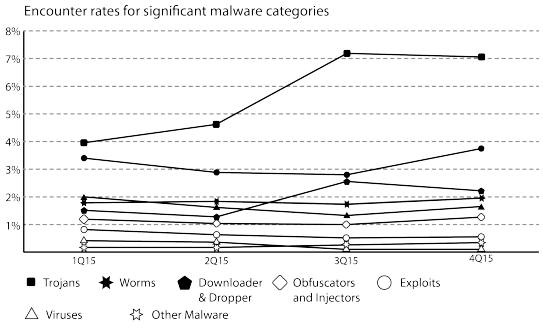
Berdasarkan penelitian yang dilakukan oleh Microsoft di tahun 2016 seperti yang ditunjukan pada gambar 1 dan tabel 2 yang mendeskripsikan gangguan berbagai macam ancaman di beberapa negara. *worms* menduduki peringkat kedua jenis serangan yang paling banyak terjadi di bawah *Trojan horse*. Namun dampak atau kerugian yang disebabkan oleh worms sangat jauh lebih besar dibandingkan *Trojan horse*. Worms mempunyai beberapa kategori berdasarkan pola serangan yang diakibatkannya antara lain[2]:

Internet worms: *worms* yang menemukan target di alamat IP pada jaringan komputer dan menyebarkan diri di Internet dengan memanfaatkan kelemahan keamanan di komputer

P2P *(peer-to-peer) worms*: *worms* ini menemukan sasarannya pada jaringan P2P

Email *worms*: worms ini mencari sasaran lewat alamat email. Kemudian menyebarkan diri dengan mengirimkan pesan email yang terinfeksi.

Instant messaging worms: worms ini menemukan sasarannya pada user ID pengguna aplikasi pesan singkat



Gambar 1. Statistik Gangguan Komputer Tahun 2016 Yang Dilakukan Oleh Mircosoft[3]

Tabel.1. Statistik Gangguan Komputer Di Beberapa Negara Pada Tahun 2016 Yang Dilakukan Oleh Microsoft[3]

Category	Worldwide	USA	Brazil	China
Browser Modifiers	7.6%	9.1%	11.8%	0.6%
Trojans	7.1%	4.2%	12.7%	10.2%
Worms	3.3%	0.6%	8.9%	5.6%
Software Bundlers	3.1%	1.7%	1.5%	0.2%
Downloader & Droppers	2.2%	2.3%	6.5%	3.2%
Obfuscators & Injectors	1.7%	1.0%	5.3%	5.2%
Adware	1.6%	4.5%	7.1%	0.2%
Exploits	1.4%	3.4%	2.4%	1.7%
Viruses	1.1%	0.4%	2.2%	7.4%
Other	0.6%	0.9%	0.3%	1.2%
Backdoors	0.5%	0.7%	1.4%	1.8%
Randsomware	0.3%	0.6%	0.5%	0.0%
Password Stealers & Monitoring Tools	0.2%	0.4%	1.0%	0.5%

Tabel.2. Sejumlah Insiden Serangan Worms[4]

Tahun	Nama Worms	Estimasi Kerugian
1999	Melissa	$ 1.1 Milyar
2000	I Love You	$ 8.75 Milyar
2001	Code Red	$ 2.6 Milyar
	Sircam	$ 1.03 Milyar
	NIMDA	$ 645 Juta
	Klez	$18.9 Milyar
2003	SQL Slammer	$ 1.2 Milyar
	Sobig	$ 36.1 Milyar
	Blaster	$ 1.3 Milyar
2004	Mydoom	$ 3.85 Milyar
	Witty	$ 11 Milyar
	Sasser	$ 14.8 Milyar

Dari keempat jenis *worms* tersebut, *internet worms* lebih sulit untuk dideteksi keberadaannya karena dapat melakukan pemindahan otomatis dan infeksi otomatis melalui eksploitasi jarak jauh dimana kode *worms* dapat ditransfer dan dieksekusi tanpa tindakan manusia.

Sebelum internet *worms* menginfeksi mesin, pertama-tama harus mencari target di ruang alamat IP. Ada sejumlah strategi pencarian target yang bisa diklasifikasikan tiga kelas utama[2]:

a. **Blind**
Blind scanning secara menyeluruh memindai seluruh ruang alamat IPv4 / IPv6 Internet tanpa sepengetahuan sebelumnya tentang targetnya

b. **Pasif**
Tidak agresif mencari target dengan cara scanning. Sebagai gantinya, ia secara pasif menunggu korban potensial untuk menghubungi mesin tempat worms berada, dan kemudian mencoba menginfeksi pengunjung selama berinteraksi dengan mereka.

c. ***hit-list***
Adalah daftar alamat yang dikenal sebagai host target, yang harus diidentifikasi sebelum serangan sebenarnya. Strategi ini menggunakan daftar target untuk mempercepat kecepatan propagasi

Salah satu upaya mengetahui suatu komputer terinfeksi internet worms adalah dengan melakukan analisa terhadap paket yang melintas di jaringan dengan *packet sniffer*

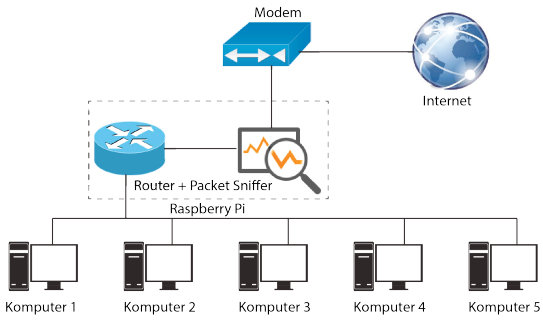
3. PRINSIP KERJA *PACKET SNIFFER*

Ketika sebuah paket dikirimkan dari sumber ke tujuan, didalam perjalanannya paket tersebut akan melewati banyak perangkat telekomunikasi seperti *router/hub*. Setiap perangkat tersebut memiliki alamat fisik yang berbeda-beda. Packet sniffer bertugas untuk mencatat semua informasi yang ditambahkan pada paket tersebut. Seperti alamat pengirim, alamat penerima, besarnya paket dan perangkat yang dilewatinya dari bentuk *binary* menjadi bentuk yang mudah dibaca oleh manusia

Dengan *packet sniffer*, banyak informasi berharga yang bisa didapatkan seperti

a. Nama pengguna dan kata kunci *(password)*
b. Menemukan pola kebiasaan pengguna di jaringan
c. Menggangu informasi pemilik
d. Memetakan tata letak jaringan

Aplikasi *packet sniffer* biasanya dipasang pada sebuah perangkat dalam penelitian ini digunakan Rapsberry Pi yang difungsikan sebagai sebuah wireless nirkabel yang kemudian diletakan pada lalu lintas yang dilalui oleh pengguna lain untuk berkomunikasi di dalam jaringan.



Gambar 2. Konsep Packet sniffer

4. PENGATURAN PERANGKAT

Perangkat Keras (*Hardware*)

Rapsberry pi merupakan sebuah perangkat komputer kecil seukuran kartu kredit, dijalankan pada operating system raspbian. Populer digunakan dengan bahasa pemrograman python[5]

Untuk dapat mengetahui informasi mengenai paket yang melintas pada jaringan komputer, perangkat yang berisi aplikasi *packet sniffer* harus diletakan pada jalur yang dilewati oleh seluruh penguna komputer, pada penelitian ini sebuah komputer mini berupa Raspberry Pi yang sudah terpasang aplikasi tcpdump diatur menjadi sebuah *router* nirkabel, diletakan antara modem dengan penggunanya agar bisa menangkap seluruh informasi pengguna didalam berinteraksi dengan internet, untuk itu perlu dilakukan pengaturan pada port *Ethernet* perangkat raspberry pi agar selalu mendapatkan ip static. Dengan perintah */etc/network/interfaces*

Port eth0

```
Iface etho inet static
address 192.168.0.100
netmask 255.255.255.0
network 192.168.0.1
broadcast 192.168.0.255
gateway 192.168.0.1
```

Selanjutnya adalah menjadikan Raspberry Pi tersebut menjadi *router* nirkabel dhcp dengan memasang beberapa aplikasi pendukung yaitu hostapd dan isc-dhcp-server dengan perintah

```
sudo apt-get update
sudo apt-get install hostapd isc-
dhcp-server
```

setelah terpasang dilakukan pengaturan terhadap aplikasi tersebut agar port wlan0 menjadi *access point* bagi pengguna komputer didalam jaringan tersebut

Perangkat Lunak (*Software*)

Tcpdump

Tpdump merupakan sebuah aplikasi packet sniffer tertua yang berbasis *command line* pada linux, aplikasi ini mengijinkan pengguna untuk mencegat dan melihat TCP/IP dan paket lainya yang melintas pada jaringan komputer yang terhubung dengan menggunakan libpcap libary[6], tcpdump lebih sesuai untuk digunakan pada Raspberry pi karena lebih mudah dijalankan melalui telnet.

Untuk memasang aplikasi tcpdump pada Raspberry Pi dilakukan dengan perintah

```
Sudo apt-get tcpdump
```

Python

Python merupakan bahasa pemrograman yang sangat mempunyai fungsi yang baik dan disukai oleh pengguna karena[7]

a. **Sederhana:** Python dibangun berdasarkan prinsip pengkodean yang dikembangkan oleh bahasa sebelumnya, namun prinsip-prinsip ini telah dieksploitasi untuk implementasi yang lebih sederhana dalam pemrograman Python.
b. ***High Level*:** Python adalah bahasa pemrograman yang sederhana. Ini bisa digunakan untuk pemrograman fungsi yang paling canggih.
c. **Sangat sesuai untuk analisis:** Python banyak digunakan dalam matematika dan sains
d. ***Open Source*:** Python adalah Bahasa pemrograman yang bersifat open source dapan diunduh pada www.python.org secara gratis. juga banyak tutorial yang dapat ditemukan di internet.

Untuk melakukan installasi aplikasi tcpdump pada Raspberry Pi dilakukan dengan perintah

```
Sudo apt-get install python3-
picamera
```

5. PENGUMPULAN DATA

Data dikumpulkan dengan menjalankan aplikasi tcpdump pada raspberry pi dengan menuliskan perintah

```
Sudo tcpdump –i wlan0 –w
namafile.pcap
```

Selanjutnya, akan dihasilkan sebuah log data yang berisi informasi lalu lintas data pada jaringan komputer. Pada penelitian ini pengumpulan data dilakukan selama 6 jam setiap hari dari jam 10.00 sd jam 16.00 setiap harinya. Besar file yang dihasilkan setiap hari berkisar 15 – 25 MB, yang terbentuk dari sekitar 200.000 – 300.000 baris teks yang dengan bahasa yang sulit dimengerti oleh manusia, dan akan sangat memakan waktu bagi penggunanya untuk menganalisis log data tersebut untuk mengetahui adanya ancaman gangguan pada jaringan komputer seperti ditampilkan pada gambar 4

MEMETAKAN SERANGAN WORMS PADA HASIL PACKET SNIFFER

Setelah didapatkan data hasil lalu lintas packet sniffer, selanjutnya dilakukan analisa terhadap data tersebut.

Pengelompokan IP

Sebuah jaringan WAN dirancang dengan IP 192.168.0.1/26 yang mempunyai jumlah host maksimal 62 perangkat untuk pengguna internal dari suatu jaringan perusahaan yang dilengkapi dengan password dan perangkat Raspberry yang terpasang

tcpdump sebagai Access point dan terdapat sebuah server perusahaan dengan alamat IP 192.168.0.60, dan sebuah jaringan WAN lain dengan alamat ip 192.168.0.63/26 yang memiliki jumlah host maksimal 62 perangkat dibiarkan terbuka tanpa *password*, dikhususkan untuk pengguna tamu dalam sebuah kantor. Kedua jaringan wan tersebut dipisahkan dalam sebuah virtual LAN yang berbeda sehingga jika ada lalu lintas data dari kelas IP jaringan WAN publik ke IP jaringan local ada kemungkinan adanya sebuah ancaman pada jaringan komputer lokal.

Alamat IP Pengirim dan penerima yang berulang dalam waktu yang berdekatan

Jika dari hasil perekaman lalu lintas data ditemukan alamat pengirim dan alamat penerima yang sama, secara berulang dan dilakukan dalam waktu yang berdekatan ada kemungkinan adanya ancaman didalam jaringan komputer

PERANCANGAN APLIKASI PENGOLAH DATA

Aplikasi untuk pengolahan log data packet analyser dikembangkan pada operating system berbasis windows, dengan mengunakan compiler PyCharm community, compiler ini banyak disukai para programmer python karena dalam penulisan kode pemrograman tersedia fitur *auto correction* yang sangat memudahkan penggunanya, navigasi proyek yang intuitif, dengan cepat memeriksa kesalahan dan memperbaiki. Untuk mendukung perancangan aplikasi pengolahan log data ini diperlukan library / modul pendukung yang dapat diunduh langsung dari aplikasi ini dengan cara menambahan plug-in. adapun aplikasi pendukung yang berperan didalam perancakan aplikasi ini antara lain:

Parser

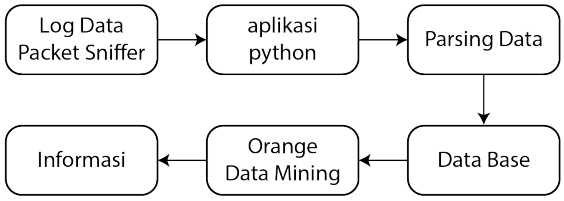
Modul Parser merupakan library pada python yang berfungsi untuk melakukan parsing data yang cocok untuk format file .txt. modul ini menyediakan sebuah interface yang mengijinkan bahasa pemrograman python untuk memanipulasi parse tree dari sebuah ekspresis dari sebuah bahasa pemrograman python dan membuat kode eksekusinya[8] dari aplikasi ini akan terbentuk suatu data yang lebih terkelompok yang kemudian akan diolah aplikasi data mining.

Orange

Orange adalah sebuah data mining suite yang berguna untuk analisis data untuk mendukung Bahasa pemrograman python, Modul ini menjadi semakin popular dan disukai oleh kebanyakan programmer python yang bergelut dengan analisis data karena mampu menampilkan analisis data yang interaktif.[9]

Kelebihan utama dari orange:

a. Pengelolaan data dan preprocessing
b. Klasifikasi
c. Regresi
d. Pengelompokan
e. Evaluasi



Gambar 3. Proses Kerja Aplikasi Pengolah Data

6. KESIMPULAN

Dengan dikembangkannya aplikasi pengolahan log data paket analyzer ini diharapkan dapat membantu dalam mengidentifikasi serangan worms didalam jaringan komputer sehingga dapat dilakukan penanunggalan secara lebih cepat, selain itu dapat pula membantu administrator jaringan untuk melakukan intepretasi dari data secara lebih cepat dan akurat.

DAFTAR PUSTAKA

[1] O. T. Adebayo, B. K. Alese, and A. J. Gabriel, "A Model for Komputer Worm Detection in a Komputer Network," *Int. J. Comput. Appl.*, vol. 66, no. 2, 2013.
[2] Yang. T, Luo. J, Xiao. B, Wei. G "Concept, Characteristics and Defending Mechanism of Worms", IEICE TRANSE INE & SYST. Vol E92-D No. 5 May 2009
[3] Microsoft Coorporation "2016 Trends in Cybersecurity" .
[4] C. Fosnock, "Komputer worms: past, present, and future," *East Carol. Univ.*, vol. 8, 2005.
[5] S. N. Basha, S. A. K. Jilani, and M. S. Arun, "An Intelligent Door System using Raspberry Pi and Amazon Web Services IoT."
[6] Asrodia. P, Patel. H "Network Traffic Analysis Using Packet Sniffer" IJERA Vol.2, Issue 3, May-Jun 2012
[7] H. Panggabean and C. A. Tobing, "Computational Linguistics Application Using Python Programming."
[8] G. Van Rossum and others, "Python Programming Language.," in *USENIX Annual Technical Conference*, 2007, vol. 41, p. 36.
[9] J. Demšar *et al.*, "Orange: data mining toolbox in Python," *J. Mach. Learn. Res.*, vol. 14, no. 1, pp. 2349–2353, 2013.

Gambar 4. Tampilan Log Data Yang Ditangkap Packet Sniffer