MEMBANGUN SISTEM MONITORING MALICIOUS TRAFFIC DI JARINGAN DENGAN MALTRAIL

[1]Hudzaifah, [2]Anang Sularsa, [3]Devie Ryana Suchendra

[1 2 3] Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Telkom University
[1]avzhudzaifah92@gmail.com, [2]ananks@gmail.com, [3]deviersuchendra@tass.telkomuniversity.ac.id

Abstrak

Jaringan komputer merupakan media informasi yang berkembang begitu pesat, hampir seluruh kegiatan komunikasi menggunakan jaringan komputer sebagai media transformasi informasi. Namun ada hal-hal yang harus diperhatikan dalam penggunaan jaringan komputer yaitu banyaknya arus data yang keluar masuk, malicious traffic merupakan suatu kejadian abnormal pada lalu lintas jaringan yang dapat membahayakan komputer. Untuk mengetahui kondisi normal dan abnormal pada jaringan dibutuhkan sistem monitoring untuk pengawasan, mengolah, dan mengontrol. Untuk mengatasi masalah tersebut pada Proyek Akhir ini dilakukanlah sistem monitoring dengan menggunakan aplikasi maltrail yang memanfaatkan daftar yang tersedia secara publik yang berisi jalur berbahaya atau secara umum mencurigakan, bersama dengan jejak statis yang dikumpulkan dari berbagai laporan AV dan daftar yang ditetapkan pengguna khusus, jejak tersebut dapat berupa apa pun dari nama domain, alamat URL atau IP. Aplikasi maltrail ter-integrasi dengan berbagai tools yaitu sensor, server, dan klien. Sensor merupakan komponen untuk pemantauan lalu lintas untuk mencari "jejak" yang telah ditandai dalam blacklist, dan server akan menyimpan semua peristiwa (yaitu entri log) dalam periode (24h) yang akan di transfer ke klien dalam bentuk CSV. Kemudian client berupa web browser sebagai web interface untuk monitoring via web yang menampilkan data berupa presentasi seperti ancaman, kejadian, sumber, dan jejak dengan cara mengakses http://127.0.0.1:8338.

Kata kunci : jaringan, malicious traffic, sistem monitoring, maltrail, sensor, server, klien.

1. Pendahuluan

1.1 Latar Belakang

Malicious traffic adalah ancaman yang paling serius dalam keamanan di dunia cyber, karena malicious traffic dapat mendistribusikan beberapa kegiatan ilegal seperti penyebaran serangan Denial of Service (DoS), penyebaran malware, dan phising.

Secara teknis malicious traffic suatu kejadian abnormal pada lalu lintas jaringan dan merupakan perbuatan user yang tidak bertanggung jawab tanpa sepengetahuan pengguna komputer yang sah. Penjahat bisa melakukan berbagai macam tidak pidana bermotif finansial maupun pencurian informasi dalam jaringan.

Oleh karena itu penelitian ini dibangun untuk memonitoring jaringan yang keluar masuk dengan menggunakan aplikasi maltrail untuk sistem deteksi lalu lintas yang berbahaya, analisis jaringan, atau pemantauan keamanan.

1.2 Rumusan Masalah

Adapun perumusan masalah dari latar belakang tersebut adalah sebagai berikut.

1. Bagaimanakah cara mendeteksi malicious traffic di jaringan ?
2. Bagaimana penerapan penggunaan maltrail untuk monitoring malicious traffic di jaringan ?

1.3 Tujuan

Adapun tujuan dibuatnya alat ini adalah sebagai berikut.

1. Merancang dan membangun sistem monitoring malicious traffic di jaringan dengan menggunakan maltrail.
2. Penerapan penggunaan maltrail untuk monitoring malicious traffic di jaringan.

1.4 Batasan Masalah

Untuk membatasi meluasnya bahasan masalah yang akan diteliti, maka dibatasilah masalah yang berkaitan dengan perancangan dan implementasi sistem monitoring ini, yaitu sebagai berikut.

1. Sistem monitoring di akses melalui aplikasi web browser.
2. Menggunakan sistem operasi kali linux.
3. Hanya membahas mengenai pembangunan sistem monitoring malicious traffic pada jaringan menggunakan maltrail.

2. Tinjauan Pustaka

Pada Bab ini penulis akan menjelaskan tentang tinjauan pustaka yang mendukung pada Proyek Akhir ini.

2.1 Sistem Monitoring

Sistem monitoring merupakan suatu kegiatan analisis terhadap data-data pada lalu lintas jaringan, untuk melakukan pengawasan[1], mengolah, dan mengontrol arus data maupun aktifitas-aktifitas yang terjadi pada jaringan tersebut yang bertujuan mencegah hal yang tidak di inginkan terjadi [2].

2.2 *Malicious*

Malicous merupakan suatu kejadian abnormal yang biasanya mencurigakan dan berbahaya yang mencakup aktivitas atau serangan yang tidak sah atau anomali yang timbul dari kegagalan hardware atau software untuk paket internet pada sebuah jaringan [3].

2.3 *Traffic*

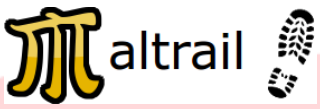
Traffic merupakan suatu arus lalu lintas yang terjadi pada suatu jaringan yang membawa data keluar masuk karena adanya permintaan dari satu tempat untuk melakukan komunikasi agar terhubung ke satu tempat lain melalui jaringan [4].

2.4 Jaringan

Jaringan komputer merupakan media informasi yang berkembang begitu pesat, hampir seluruh kegiatan komunikasi menggunakan jaringan komputer sebagai media transformasi informasi yang menghubungkan perangkat dari satu tempat ke tempat lain [5].

2.5 Maltrail

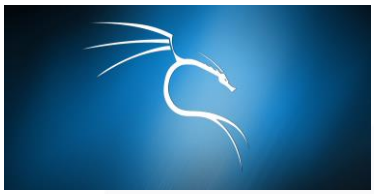
Maltrail adalah sistem pendeteksi lalu lintas berbahaya, memanfaatkan daftar publik (hitam) yang berisi jalur berbahaya atau secara umum mencurigakan, bersama dengan jejak statis yang dikumpulkan dari berbagai laporan Anti-Virus dan daftar yang ditetapkan pengguna khusus, jejak tersebut dapat berupa nama domain, URL, dan alamat IP [6].



Gambar 2.1 Maltrail

2.6 Kali Linux

Kali linux merupakan sebuah sistem operasi berbasis debian yang dikembangkan oleh Offensive Security sebagai penerus BackTrack [7], yang merupakan distribusi dari induknya, yaitu linux. Digunakan untuk alat penetrasi keamanan computer [8]. Kali Linux dan bersifat opensource yang disebarluaskan ke masyarakat secara gratis [9].



Gambar 2.2 Kali Linux

2.7 Python

Python adalah bahasa pemrograman yang memungkinkan Anda bekerja lebih cepat dan mengintegrasikan sistem Anda lebih efektif.. Tidak seperti bahasa lain yang susah untuk dibaca dan dipahami, python lebih menekankan pada keterbacaan kode agar lebih mudah untuk memahami sintaks [10].

Gambar 2.3 Python

2.8 Pcapy

Pcapy adalah modul ekstensi Python yang berinteraksi dengan libpcap paket capture library. Pcapy memungkinkan skrip python untuk menangkap paket pada jaringan [11].

2.9 Cara Kerja

Arsitektur maltrail didasarkan pada Sensor > Server > Klien.

2.9.1 Sensor

Sensor adalah komponen mandiri yang berjalan pada node pemantau yang bertugas memantau traffic yang lewat untuk jalur yang masuk daftar hitam (URL atau IP) pada jaringan. Sensor akan mengirimkan detail acara ke Server.

2.9.2 Server

Server merupakan komponen yang menyimpan semua peristiwa yang terjadi dalam periode (24h) dan memberikan data ke Klien untuk aplikasi web pelaporan. Data dikirim ke klien dalam potongan terkompresi, dan diproses secara berurutan.

2.9.3 Klien

Klien berupa web browser (IE, Chrome, Firefox, dll.) dengan mengakses http://127.0.0.1:8338. Semua peristiwa (yaitu entri log) dalam periode (24h) akan ditransfer ke Klien , dan aplikasi web pelaporan yang bertanggung jawab penuh atas bagian presentasi seperti ancaman, kejadian, sumber, dan jejak.

2.10 Fitur

Maltrail mempunyai fitur antara lain :

1. Menggunakan banyak blacklist publik (alientvault, autoshun, badips, sblam, dll).
2. Memiliki jalur statis yang luas untuk identifikasi (nama domain, URL, atau alamat IP).
3. *Interface* pelaporan dalam bentuk aplikasi *web browser*.

3. ANALISIS DAN PERANCANGAN

3.1 Analisis

3.1.1 Gambaran Sistem Saat ini

Pada Gambar 3.1 diilustrasikan proses masuknya malicious traffic pada jaringan, lalu lintas jaringan bebas keluar masuk jaringan tanpa tahu data yang diterima dan dikirim. Sehingga membuat jaringan rentan terhadap serangan dan aktivitas yang tidak sah. Hanya dengan mengandalkan firewall sebagai pertahanan, namun tidak ada monitoring jaringan yang dilakukan.

Gambar 3.1 Sistem saat ini

3.1.2 Analisis Kebutuhan

Sistem pendeteksi malicious traffic ini memanfaatkan daftar publik(blacklist) serta jejak statis yang dikumpulkan dari berbagai laporan AV(Anti Virus) untuk dijadikan parameter beroperasinya komponen pada sistem yang di buat. Sensor yang ditempatkan pada komponen mandiri yang berjalan pada node pemantau beserta server yang berfungsi pengolah data dari sensor untuk semua peristiwa yang terjadi kemudian di kirimkan ke klien yang nantinya data tersebut di olah dan ditampilkan memakai aplikasi web untuk bagian presentasi pelaporan.

3.1.2.1 Analisis Kebutuhan Masukan

Pada sistem pendeteksi malicious traffic ini dibutuhkan masukan sebagai berikut :

a. Masukan data dari sensor yang menjadi parameter beroperasinya monitoring malicious traffic di jaringan yang nantinya akan memberikan data detail peristiwa(event) kepada server.

b. Masukan data dari server yang menjadi parameter beroperasinya klien yang berperan sebagai presentasi pelaporan semua peristiwa yang terjadi dengan memakai aplikasi web browser.

3.1.2.2 Analisis Kebutuhan Keluaran

Pada sistem ini dibutuhkan keluaran sebagai berikut :

a. Keluaran data berupa interface presentasi pelaporan dengan memakai aplikasi web browser.

b. Dapat mengetahui jejak, alamat IP, waktu kejadian, tingkat level berbahaya, dan protokol yang digunakan.

3.1.3 Kebutuhan Pengguna

Adapun kebutuhan pengguna sebagai berikut:

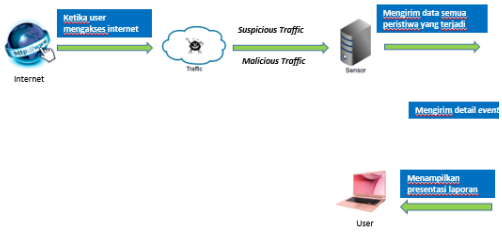
1. Laptop sebagai perangkat akses maltrail.
2. Web browser sebagai penghubung untuk melihat hasil detail event presentasi pelaporan pada maltrail.

3. Mengunduh paket aplikasi maltrail https://github.com/stamparm/maltrail.
4. Mengekstrak paket aplikasi maltrail.

3.2 Perancangan

3.2.1 Gambaran Sistem Usulan

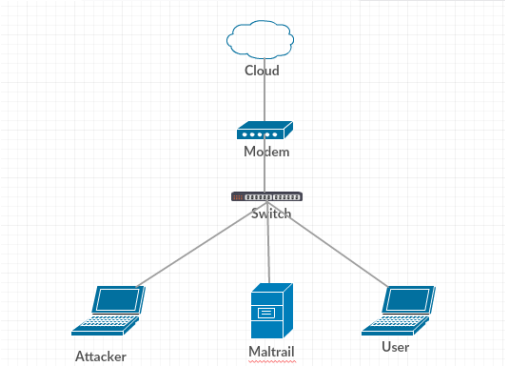
Pada Gambar 3.2 menjelaskan sistem usulan dengan melakukan instalasi sensor dan server pada laptop, kemudian sensor akan mendeteksi traffic termasuk malicious traffic atau suspicious traffic ketika berselancar di internet. Ketika malicious traffic terdeteksi maka sensor akan mengirimkan semua peristiwa yang terjadi kepada server dan akan disimpan ke log database. Kemudian server mengirimkan detail peristiwa(event) kepada klien yang diakses lewat 127.0.0.1:8338 yang berbentu web browser agar lebih mudah dipahami oleh user.



Gambar 3.2 Gambaran Sistem

3.2.2 Topologi Sistem

Pada gambar 3.3 tentang Topologi sistem di atas, yang menjelaskan cara kerja sistem ini. Ketika traffic melewati maltrail, maka maltrail akan mendeteksi malicious traffic atau suspicious traffic melalui Sensor. Sensor akan mengirimkan data ke Server yang selanjutnya Server akan menyimpan data semua peristiwa yang terjadi, lalu data tersebut akan dikirimkan lagi dan akan diterima oleh Client berupa informasi alamat IP penyerang, IP target, reference, dan info termasuk kategori malware, scanner, atau penyerang anonim.



Gambar 3.3 Topologi Sistem

3.2.3 Spesifikasi Sistem

Berikut ini adalah kebutuhan perangkat keras dan perangkat lunak yang dibutuhkan dalam Proyek Akhir ini.

3.2.3.1 Perangkat Keras

Adapun beberapa perangkat keras yang di gunakan di sistem ini, yaitu :

Tabel 3.1 Perangkat Keras Yang di Gunakan

No.	*Hardware*	Unit	Keterangan
1.	Laptop	2	Penempatan Sensor, server, dan Klien
2.	Modem	1	Untuk koneksi internet

3.2.3.1 Perangkat Lunak

Adapun beberapa perangkat lunak yang di gunakan di sistem ini, yaitu :

Tabel 3.2 Perangkat Lunak Yang di Gunakan

No.	*Software*	Spesifikasi	Keterangan
1.	Kali	Distro Debian Linux	Sensor dan Server
2.	Windows	Windows 10	Klien
3.	Python	Python 2.6 atau 2.7	Bahasa pemrograman yang dipakai
4.	Pcapy	Modul ekstensi python	Untuk menangkap paket pada jaringan
5.	Maltrail	*Default* spesifikasi	Monitoring sistem pendeteksi *malicious traffic*

4. PENGUJIAN

4.1 Hasil Pengujian *Malware Conficker*

Berikut merupakan hasil pengujian data yang didapat pada pengujian *malware conficker* pada jaringan yang terpasang Maltrail.

Gambar 4.1 Pengujian *Malware Conficker*

4.2 Hasil Pengujian Metode Nmap

Berikut merupakan hasil pengujian data yang didapat pada pengujian metode nmap pada jaringan yang terpasang Maltrail.

Gambar 4.2 Pengujian Nmap pada Maltrail

4.3 Hasil Pengujian *Malware Banjori*

Berikut merupakan hasil pengujian data yang didapat pada pengujian *malware banjori* pada jaringan yang terpasang Maltrail.

Gambar 4.3 Pengujian *Malware Banjori*

4.4 Hasil Pengujian Penambahan Daftar Hitam

Berikut merupakan hasil pengujian data yang didapat pada pengujian penambahan nama *domain* facebook.com di daftar hitam di jaringan yang terpasang Maltrail.

Gambar 4.4 Pengujian Penambahan Daftar Hitam

5. Kesimpulan

Dari hasil implementasi dan pengujian , maka dapat disimpulkan bahwa :

1. Sistem monitoring malicious traffic telah berhasil dirancang dan dibangun.
2. Penerapan sistem maltrail telah berhasil mendeteksi malicious traffic di jaringan.

6. Daftar Pustaka

[1] B. ROSIDHARTA, IMPLEMENTASI SISTEM MONITORING PERFORMA MYSQL MENGGUNAKAN PRTG, T. ZANI, Ed., Bandung: Universitas Telkom, 2017.

[2] A. W. S. Permana, "SISTEM MONITORING DAN NOTIFIKASI POWER MANAGEMENT SYSTEM," Desember 2017.

[3] C. C. M. M. Ernst Biersack, Data Traffic Monitoring and Analysis, Springer Berlin Heidelberg, 2013.

[4] S. C. Tao Li, Traffic Measurement on the Internet, Springer New York, 2013.

[5] A. R. SYAHPUTRA, MONITORING TRAFIK DAN PERFORMANSI PADA JARINGAN KOMPUTER DAN SERVER CLOUD DI FAKULTAS ILMU TERAPAN, N. H. Devie Ryana Suchendra, Ed., Bandung: Universitas Telkom, 2018.

[6] M. Stampar, "GitHub," 26 Januari 2016. [Online]. Available: https://github.com/stamparm/maltrail. [Accessed 28 November 2017].

[7] M. A. Rahmadani, "IMPLEMENTASI HACKING WIRELESS DENGAN KALI LINUX MENGGUNAKAN KALI NETHUNTER," 2017.

[8] M. Dzulkarnaen, "IMPLEMENTASI USB HID KEYBOARD ATTACKS DENGAN REMOTE PENETRATION TEST PADA KALI NET HUNTER," Desember 2017.

[9] O. Fachrizal, KALI LINUX 300% ATTACK, Jasakom, 2015.

[10] H. W. R.H Sianipar, Pemrograman Python Teori dan Implementasi, Bandung: Informatika Bandung, 2015.

[11] C. Security, "Pcapy," [Online]. Available: https://www.coresecurity.com/corelabs-research/open-source-tools/pcapy. [Accessed 28 November 2017].