SKRIPSI

PEMANFAATAN API VIRUSTOTAL UNTUK PENDETEKSIAN MALWARE

Louis Genio

NPM: 2016730003

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN SAINS
UNIVERSITAS KATOLIK PARAHYANGAN
2023

UNDERGRADUATE THESIS

USING VIRUSTOTAL API FOR MALWARE DETECTION

Louis Genio

NPM: 2016730003

DEPARTMENT OF INFORMATICS
FACULTY OF INFORMATION TECHNOLOGY AND SCIENCES
PARAHYANGAN CATHOLIC UNIVERSITY
2023

LEMBAR PENGESAHAN

PEMANFAATAN API VIRUSTOTAL UNTUK PENDETEKSIAN MALWARE

Louis Genio

NPM: 2016730003

Bandung, 13 Januari 2023

Menyetujui,

Pembimbing

Digitally signed by Chandra Wijaya

Chandra Wijaya, M.T.

Ketua Tim Penguji

Digitally signed by Elisati Hulu

Elisati Hulu, M.T.

Anggota Tim Penguji

Digitally signed by Pascal Alfadian Nugroho

Pascal Alfadian, Nugroho, M.Comp.

Mengetahui,

Ketua Program Studi

Digitally signed by Mariskha Tri Adithia

Mariskha Tri Adithia, P.D.Eng

PERNYATAAN

Dengan ini saya yang bertandatangan di bawah ini menyatakan bahwa skripsi dengan judul:

PEMANFAATAN API VIRUSTOTAL UNTUK PENDETEKSIAN MALWARE

adalah benar-benar karya saya sendiri, dan saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika keilmuan yang berlaku dalam masyarakat keilmuan.

Atas pernyataan ini, saya siap menanggung segala risiko dan sanksi yang dijatuhkan kepada saya, apabila di kemudian hari ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya, atau jika ada tuntutan formal atau non-formal dari pihak lain berkaitan dengan keaslian karya saya ini.

Dinyatakan di Bandung,
Tanggal 13 Januari 2023

Louis Genio
NPM: 2016730003

ABSTRAK

Malware (malicious software) adalah program yang dibuat khusus untuk mengganggu kinerja computer. Malware ini dapat menyebar melalui jaringan, email, flashdisk. Biasanya *malware* ini selalu membawa hal buruk atau gangguan terhadap kinerja sistem, contohnya seperti adanya aplikasi yang tidak pernah diinstall oleh pengguna, terjadi degradasi performa *lag* pada pomputer pengguna, adanya *popup*/iklan yang mengganggu, kinerja prosesor tinggi, walau tidak ada program yang dijalankan pengguna.

Untuk dapat mengetahui/mendeteksi adanya malware pada jaringan maka diperlukan *Packet sniffer / packet capture*. *Packet sniffer* ini digunakan untuk identifikasi, klasifikasi dan *troubleshooting* terhadap trafik jaringan berdasarkan aplikasi yang mengirimkan data, alamat sumber dan alamat tujuan paket data. Dengan hasil dari *paket sniffer* tersebut akan kita upload ke website *virus total* untuk dianalisis lebih lanjut. Website *VirusTotal* ini adalah salah satu produk layanan online gratis yang berguna untuk menganalisis berkas/file dan pranala (link) dari virus, worm, trojan, dan segala jenis malware dengan menggunakan lebih dari 70 mesin antivirus.

Pada penelitian ini akan dibangun sebuah perangkat lunak yang dapat menerima *input/request* untuk dikirim ke *Virustotal* dan dilakukan pengecekan serta pemindain terhadap *request* tersebut, Perangkat lunak juga akan menampilkan hasil pemindain tersebut beserta jenis *malware* yang ditemukan jika ada. Hasil pengujian yang dilakukan menunjukan bahwa perangkat lunak dapat melakukan proses pengiriman *request* dan menerima hasil laporan sesuai dengan *request* yang dikirim dan ditampilkan ke pengguna.

Kata-kata kunci: *sniff*, *virusTotal pyshark*, *malware*

ABSTRACT

Malware (malicious software) is a program created specifically to interfere with performance computers. This malware can spread through the network, email, flash. Usually malware this always brings bad things or disturbances to system performance, for example as there is applications that were never installed by the user, there was a lag performance degradation on the computer users, annoying popups/ads, high processor performance, even if there is no program user run.

To be able to find out / detect malware on the network, Packet is needed sniffers / packet capture. This packet sniffer is used for identification, classification and troubleshooting against network traffic based on the application that sends data, source address and address data packet destination. With the results of the sniffer package, we will upload it to the total virus website for further analysis. This VirusTotal website is one of the free online service products which is useful for analyzing files/files and links from viruses, worms, trojans, and everything types of malware using more than 70 antivirus engines.

In this research a software will be built that can receive input request to be sent to VirusTotal and scan the request. The software will also display the scan results along with the type of malware found if any. The results of the tests performed show that the software can process sending *request* and receiving report results in accordance with the request sent and displayed to the user

Keywords: sniff, VirusTotal, pyshark, malware

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, karena dengan rahmat dan karuniaNya, penulis dapat menyelesaikan skripsi yang berjudul "Pemanfaatan API Virustotal Untuk Pendeteksian Malware", sebagai salah satu syarat untuk menyelesaikan Program Sarjana (S1) Jurusan Teknik Informatika Universitas Katolik Parahyangan. Penulis berharap skripsi dan perangkat lunak yang dibangun dapat berguna bagi siapa pun yang membutuhkan dan dapat membantu bagi orang yang akan melanjutkan penelitian ini untuk selanjutnya. Skripsi ini tidak akan selesai tanpa orang-orang tercinta di sekeliling penulis yang mendukung dan membantu. Terima kasih saya sampaikan kepada:

1. Kedua orang tua, kakak, adik dan saudara-saudara tercinta yang selalu memberikan semangat, doa, dan dukungan dalam menyelesaikan skripsi ini.
2. Bapak Chandra Wijaya, M.T. selaku dosen pembimbing yang telah membantu, membimbing, dan memberikan saran kepada penulis sehingga skripsi dan perangkat lunak yang dibangun dapat diselesaikan dengan baik.
3. Bapak Bapak Elisati Hulu, M.T. dan Pascal Alfadian Nugroho, M.Comp. sebagai penguji atas kritik dan sarannya untuk hasil penyusunan skripsi ini.
4. Teman - teman seangkatan yang telah memberikan semangat, dan dukungan dalam menyelesaikan skripsi ini.

Bandung, Januari 2023

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR KODE PROGRAM

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Malware (malicious software) adalah program yang dibuat khusus untuk mengganggu kinerja computer. Malware ini dapat menyebar melalui jaringan, *email, flashdisk*. *Malware* ini selalu membawa hal buruk atau gangguan terhadap kinerja sistem, contohnya seperti adanya aplikasi yang tidak pernah diinstall oleh pengguna, terjadi degradasi performa *lag* pada komputer pengguna, adanya popup/*iklan* yang mengganggu, kinerja prosesor tinggi, walau tidak ada program yang dijalankan pengguna.

Untuk dapat mengetahui/mendeteksi adanya malware pada jaringan maka diperlukan *Packet sniffer / packet capture*. *Packet sniffer* ini digunakan untuk identifikasi, klasifikasi dan *troubleshooting* terhadap trafik jaringan berdasarkan aplikasi yang mengirimkan data, alamat sumber dan alamat tujuan paket data. Dengan hasil dari *packet sniffer* tersebut akan kita upload ke website *virus total* untuk dianalisis lebih lanjut. Salah satu alat yang dapat memenuhi permintaan ini adalah *pyshark*. *Pyshark*. *pyshark* adalah pembungkus untuk tshark, artinya ini memungkinkan *python* untuk mengurai paket dengan menggunakan disektor wireshark namun ini unik karena *pyshark* ini tidak mengurai paket melainkan menggunakan kemampuan (utilitas baris perintah wireshark) *tshark* untuk mengekspor XML untuk menggunakan penguraiannya.

Website VirusTotal ini adalah salah satu produk layanan online gratis yang berguna untuk menganalisis berkas/file dan pranala (link) dari *virus, worm, trojan*, dan segala jenis *malware* dengan menggunakan lebih dari 54 mesin *antivirus*. Situs *VirusTotal* tersebut dapat menampilkan jumlah deteksi untuk tiap *request* berdasarkan tipe-tipenya, contohnya *malicious*, *undetected*, dan lain-lain. Situs *VirusTotal* ini juga memiliki *API* atau *Application Programming Interface* yang bisa digunakan oleh *programmer* untuk membangun sebuah perangkat lunak seputar pendeteksi *malware*.

Pada skripsi ini, akan dibuat sebuah perangkat lunak yang dapat menampilkan hasil analisa *website virus total* dari berkas file yang diupload. Dengan menggunakan perangkat lunak tersebut, pengguna dapat mengetahui berkas/file apa saja yang merupakan *malware/virus/worm/trojan* dan dapat ditindaklanjuti dengan menghapusnya. Perangkat lunak akan dibuat menggunakan bahasa python dengan bantuan *API* Virustotal.

1.2 Rumusan Masalah

Berdasarkan deskripsi, rumusan masalah pada skripsi ini adalah sebagai berikut:

- Apa dan bagaimana *malware* bekerja?
- Bagaimana melakukan *packet capture* di lingkungan system operasi *windows*?
- Bagaimana cara membangun perangkat lunak dengan Pemanfaatan API *Virustotal* Untuk Pendeteksian *Malware*?

1.3 Tujuan

Berdasarkan rumusan masalah, maka tujuan dari skripsi ini adalah sebagai berikut:

- Mengetahui tentang berbagai jenis *malware* dan akibatnya.
- Mempelajari *packet capture*.
- Mengetahui cara untuk membangun perangkat lunak Pemanfaatan API *Virustotal* Untuk Pendeteksian Malware.

1.4 Batasan Masalah

1. Adanya batas pengiriman *request* yaitu 4 *request* permenit dari *VirusTotal* sehingga perangkat lunak yang dibuat tidak bisa melakukan pengiriman langsung ke *Virus/total* secara bersamaan dengan *packet capture*.

1.5 Metodologi

Metodologi yang digunakan dalam penelitian ini adalah sebagai berikut

1. Mempelajari lebih dalam mengenai jenis-jenis malware.
2. Mempelajari packet capture di lingkungan system operasi linux/unix.
3. Melakukan analisis pada aplikasi pemanfaatan API Virustotal untuk pendeteksian Malware.
4. Melakukan perancangan pada aplikasi pemanfaatan API Virustotal untuk pendeteksian Malware.
5. Melakukan pembangunan aplikasi pemanfaatan API Virustotal untuk pendeteksian Malware.
6. Mengimplementasikan aplikasi.
7. Melakukan pengujian & eksperimen pada aplikasi pemanfaatan API Virustotal untuk pendeteksian Malware.
8. Menulis dokumen skripsi.
9. Dapat mencapture data dijaringan.
10. Dapat mengextract file exe/pdf/sesuatu yang mencurigakan dan dikirimkan ke *virustotal*.
11. Dapat memberikan informasi mengenai nama file yang diekstraksi dari jaringan.
12. Dapat memberikan informasi mengenai waktu ekstraksi file yang ditangkap.
13. Dapat memberikan informasi mengenai hasil pemeriksaan virustotal mengenai file yang diekstraksi.
14. Dapat memberikan informasi mengenai alamat komputer sumber pengirim file dan alamat komputer yang telah dikirim file.
15. Membuat dokumen skripsi

1.6 Sistematika Pembahasan

Laporan penelitian tersusun ke dalam enam bab secara sistematis sebagai berikut.

1. Bab 1 Pendahuluan, berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika pembahasan.
2. Bab 2 Dasar Teori, berisi dasar teori umum tentang *malware*, jenis dan tipe *malware* beserta *tools* yang dipakai untuk melaksanakan penelitian.
3. Bab 3 Analisis, berisi analisis perangkat lunak, analisis *sniff* pada *pyshark*, langkah untuk mendapatkan laporan *VirusTotal*, analisis *Use Case* Diagram, analisis *Data Context* Diagram dan *Data Flow* Diagram.
4. Bab 4 Perancangan, berisi perancangan perangkat lunak yang dibangun meliputi perancangan modul, *flowchart* antarmuka dan perancangan antarmuka.
5. Bab 5 Implementasi dan Pengujian, berisi implementasi antarmuka perangkat lunak, pengujian fungsional, pengujian eksperimental, dan kesimpulan dari pengujian.

6. Bab 6 Kesimpulan dan Saran, berisi kesimpulan dari awal hingga akhir penelitian dan saran untuk pengembangan selanjutnya.