**Tugas Keamana Jaringan Komputer**

**Analisis Trojjan Pada Operating System Windows**

**Disusun Oleh:**

**Aditiya Gunanta**

**09011181520001**

**Universitas Sriwijaya**

**Fakultas Ilmu Komputer**

**Jurusan Sistem Komputer**

**2019**

 **Keylogger**

1. **Introduction**

 Keylogger adalah alat yang paling berkembang karena aplikasi ini sangat jarang dikenali sebagai program jahat oleh antivirus, fungsi keylogger akan merekam semua kegiatan yang berkaitan dengan penekanan pada tombol keyboard atau aktivitas pada sistem operasi. Alamat email dan kata sandi bahkan hingga akun Facebook dengan kata sandi dapat dicocokkan dengan keyloggerapps tanpa disadari pengguna komputer

 String Matching adalah metode pencocokan karakter dari proses input seperti keyboard, dan proses pencocokan dilakukan dengan memeriksa setiap karakter yang masuk. Penggunaan algoritma pencocokan string pada aplikasi keylogger yang digunakan untuk merekam aktivitas pengguna akan lebih nyaman dan lebih cepat.

 Aplikasi keylogger yang dirancang dengan menerapkan algoritma Pencocokan String Tepat dapat merekam aktivitas semua pengguna yang terkait dengan keyboard, dan hasilnya disimpan secara otomatis dalam database khusus yang hanya dapat diakses oleh pemilik keylogger, pengembangan aplikasi keylogger selanjutnya dapat merekam aktivitas tersebut. pada keyboard virtual atau aktivitas jarak jauh di komputer pengguna.

 Sebuah penelitian menemukan bahwa 20 juta pengguna di AS, atau sekitar 1/3 dari tenaga kerja online (yaitu, para pengguna dengan akses internet reguler di tempat kerja), melakukan penelusuran web atau surel. Secara global, angkanya sekitar 28 juta, atau sekitar 1/4 dari tenaga kerja online global

 Ini dipantau termasuk layanan yang tidak dibutuhkan, port terbuka yang tidak perlu, beberapa peristiwa sistem / keamanan, driver, folder bersama, program yang dimuat saat startup dan konfigurasi jaringan. Pemantauan adalah faktor penting untuk menjaga stabilitas jaringan. Keamanan informasi berfokus pada memastikan, kerahasiaan, integritas, dan ketersediaan.

1. **OverVIew**

 Keyboard adalah tujuan utama penebang kunci untuk mengambil input pengguna dari karena itu adalah antarmuka pengguna yang paling umum dengan komputer. Meskipun baik hardware dan software key logger ada, software key logger adalah bentuk dominan dan dengan demikian merupakan poin utama dalam makalah ini. Software keylogger adalah program yang paling murah dan mudah digunakan. Keyloggers ini perlu disesuaikan dengan setiap sistem operasi target untuk memastikan I / O ditangani dengan tepat. Perbedaan sistem dengan demikian tak terhindarkan mengarah pada mekanisme spesifik sistem operasi yang diterapkan pada keylogger perangkat lunak: penggunaan tabel keadaan keyboard, kait rutin sistem, dan driver berlapis mode-kernel [3]. Detail tambahan tentang teknik yang digunakan dalam pengembangan, distribusi, pelaksanaan, dan deteksi keylogger mode pengguna dan kernel, khususnya pada sistem operasi Microsoft Windows. Konsep dasar di balik keyloggers dan malware serupa adalah pola serangan mereka. Sebagian besar infeksi malware mengikuti pola serangan yang cukup standar yang melibatkan urutan pengembangan, distribusi dan infeksi, serta tahapan eksekusi. Distribusi dan eksekusi keduanya dapat diimplementasikan sebagai komponen malware dan karena itu merupakan faktor yang berkontribusi dalam desain dan pengembangannya. Malware keylogging untuk mulai mengeksekusi dan dapat terjadi dalam beberapa cara berbeda tergantung pada implementasi dan konteks keylogger. Namun, keyloggers paling realistis berbagi dua operasi: (a) menghubungkan ke aliran input pengguna untuk menerima penekanan tombol dan (b) mengangkut data ke lokasi yang jauh

1. **Method**

 Keylogger adalah perangkat baik perangkat keras atau perangkat lunak yang digunakan untuk memantau penekanan tombol keyboard. Keylogger biasanya akan menyimpan hasil pemantauan penekanan tombol keyboard ke dalam file log / record / record. Beberapa keylogger tertentu bahkan dapat mengirim rekaman ke email tertentu secara berkala. Keyloggercan bisa digunakan untuk kepentingan yang bermanfaat atau bahkan bisa digunakan untuk kepentingan kejahatan. Minat yang tepat mencakup pemantauan produktivitas karyawan untuk penegakan hukum dan pencarian bukti kejahatan. Minat yang salah termasuk pencurian data dan kata sandi.

 Algoritma pencocokan string yang tepat digunakan untuk mencocokkan variabel input keyboard dengan input yang diterima dari keyboard, dan pencocokan string yang tepat adalah metode yang dapat dilakukan untuk mencocokkan variabel string input dengan variabel perbandingan string, untuk pengujian algoritma pencocokan string yang tepat pada aplikasi keylogger.

 Kata tersebut akan diidentifikasi sebagai kata yang dimasukkan oleh pengguna, kata tersebut adalah "Kata Sandi" seperti yang ditunjukkan pada Gambar 2, kata tersebut kemudian diubah menjadi bentuk ASCII, setelah diubah hasilnya adalah "80 97 115 115 119 119 111 114 100", karakter hasil ASCII akan dibandingkan dengan kode ASCII yang terkandung dalam sistem keyloggers, jika ditemukan maka sistem akan merekam karakter ASCII dan mengubahnya menjadi huruf.

1. **Logging and Monitoring**

 Dari pemantauan Anda dapat mendeteksi upaya peretasan, pelacakan, infeksi dan penyebaran virus atau worm, masalah konfigurasi, masalah perangkat keras dan banyak lainnya. Pemantauan adalah faktor terpenting untuk menjaga stabilitas jaringan. Keamanan informasi berfokus pada memastikan kerahasiaan, integritas dan ketersediaan, akuntabilitas. Dari pemantauan jaringan, Anda dapat mendeteksi upaya akses untuk mengecualikan informasi atau sumber daya seperti akses tidak sah, yang pada gilirannya memastikan kerahasiaan. Anda dapat mendeteksi upaya untuk mengubah atau mengubah informasi seperti modifikasi file, yang memastikan integritas. Dan Anda dapat mendeteksi segala jenis masalah yang dapat mempengaruhi ketersediaan informasi seperti serangan DOS atau DDOS. Tujuan utama dari makalah ini adalah untuk memberikan gambaran tentang beberapa manfaat yang dapat diperoleh siapa saja dari pemantauan lengkap jaringan. Logging dapat memberikan informasi terperinci tentang akses atau perubahan apa pun untuk sumber daya jaringan apa pun

 Log adalah catatan peristiwa yang terjadi dalam sistem dan jaringan organisasi. Log terdiri dari entri log; setiap entri berisi informasi yang terkait dengan peristiwa spesifik yang telah terjadi dalam suatu sistem atau jaringan. Log digunakan terutama untuk masalah pemecahan masalah, tetapi log sekarang melayani banyak fungsi di sebagian besar organisasi, seperti mengoptimalkan sistem dan kinerja jaringan, merekam tindakan pengguna, dan menyediakan data yang berguna untuk menyelidiki aktivitas berbahaya. Meluasnya penyebaran server jaringan, workstation, dan perangkat komputasi lainnya, dan semakin banyaknya ancaman terhadap jaringan dan sistem, jumlah, volume, dan berbagai log keamanan komputer telah meningkat pesat. Ini telah menciptakan kebutuhan untuk manajemen log keamanan komputer, yang merupakan proses untuk menghasilkan, mentransmisikan, menyimpan, menganalisis, dan membuang data log keamanan komputer. Logging bisa menjadi teman terbaik administrator keamanan. Ini seperti mitra administratif yang selalu bekerja, tidak pernah mengeluh, tidak pernah lelah, dan selalu di atas segalanya. Jika diinstruksikan dengan benar, mitra ini dapat menyediakan waktu dan tempat setiap peristiwa yang terjadi di jaringan atau sistem Anda.

 Proses operasional manajemen log utama biasanya mencakup mengkonfigurasi sumber log, melakukan, analisis log, memulai respons terhadap peristiwa yang diidentifikasi, dan mengelola penyimpanan jangka panjang. Administrator memiliki tanggung jawab lain juga, seperti berikut ini :

* Memantau status pencatatan semua sumber log.
* Memantau proses rotasi arsip dan arsip
* Memeriksa pembaruan dan tambalan untuk perangkat lunak logging, dan memperoleh, menguji, dan menggunakan mereka
* Memastikan bahwa setiap jam host pencatatan disinkronkan ke sumber waktu umum. • Mengkonfigurasi ulang logging sesuai kebutuhan berdasarkan perubahan kebijakan, perubahan teknologi, dan faktor lainnya
* Mendokumentasikan dan melaporkan anomali dalam pengaturan, konfigurasi, dan proses log
1. **Cara Kerja**

 Keylogger yang menempel pada API keyboard komputer ini bekerja sama dengan sistem operasi. Jika ada aktivitas penekanan tombol, secara otomatis Keylogger akan mencatatnya. Dalam hal ini sistem API pada Windows, digunakan guna menyelidiki keadaan serta memantau kegiatan keyboard. Beberapa sistem API yang kita kenal ada dari GetAsyncKeyState(), GetForegroundWindow(), dan lain-lain. Keylogger berbasis API dianggap sebagai Keylogger yang sangat mudah digunakan, namun diperlukan adanya penyelidikan secara konstan pada setiap kunci. Hal ini justru berdampak pada meingkatnya penggunaan CPU.

 Sebuah alat Keylogger pada akhirnya akan menyimpan hasil pemantauan dari aktivitas penekanan tombol keyboard ke dalam sebuah berkas cecatat (*log file*). Sementara itu, beberapa Keylogger tertentu bahkan bisa mengirimkan hasil rekamannya ke surel tertentu secara berkala. Memang jika diperhatikan lebih unggul Keylogger berbentuk perangkat lunak karena dapat ditambah dengan fitur yang mampu menangkap informasi pengguna tanpa harus bergantung pada penekanan tombol keyboard sebagai input tunggal.

**Referense**

[1] Preeti Tuli and Priyanka Sahu, “System Monitoring and Security Using Keylogger System Monitoring and Security Using Keylogger” Vol. 2, Issue. 3, 2013

[2] Robbi Rahim, “Keylogger Application to Monitoring Users Activitywith Exact String Matching Algorithm” J. Phys.: Conf. Ser.954 012008, 2018