IMPLEMENTASI SISTEM PENDETEKSI SERANGAN PADA JARINGAN DENGAN BRIARIDS BERBASIS RASPBERRY PI

Muhamad Aldo Faizi[1], Setia Juli Irzal Ismail[2], Anang Sularsa[3]

1, 2, 3 Prodi D3 Teknik Komputer, Fakultas Ilmu Terapan, Universitas Telkom
[1]aldofaizi@gmail.com, [2]jul@tass.telkomuniversity.ac.id, [3]ananks@tass.telkomuniversity.ac.id

Abstrak

Setiap jaringan biasanya terdapat celah keamanan. Maka itu dibutuhkan sistem untuk mengamankan jaringan tersebut, yaitu *Intrusion Detection System* atau sistem pendeteksi serangan. Biasanya intrusion detection system berjalan pada PC. Tetapi dengan *BriarIDS*, sistem dapat berjalan dengan komputer papan tunggal *Raspberry Pi*. *Intrusion Detection System* berfungsi sebagai pendeteksi serangan secara *real time.* Informasi yang diperoleh berupa waktu penyerangan, jenis serangan, tingkatan serangan, dan *IP Address* penyerang.

Kata Kunci: Raspberry Pi, Intrusion Detection System, keamanan jaringan.

Abstract

There's a chance that every network system could be vulnerable to hacker's attack. Therefore, a system to secure the network is needed. Intrusion Detection System is a system that could detect most of the attacks. Usually, Intrusion Detection System run on Personal Computer. But with BriarIDS, the system could run on single board computer such as Raspberry Pi. Intrusion Detection System functioned as a detector for incoming attack running in real time. The information collected from the system are attack time occurred, type of attack, the attack priority level, and attacker's IP Address.

Keywords: Raspberry Pi, Intrusion Detection System, network security

1. Pendahuluan

1.1 Latar Belakang

Seriring perkembangan teknologi dan informasi yang sangat pesat, kebutuhan akan teknologi jaringan komputer dan internet semakin meningkat. Selain sebagai media penyedia informasi, jaringan komputer dan internet dapat digunakan untuk bertukar data. Dengan mudahnya, informasi dan data dapat diperoleh dari pengguna ke pengguna lainnya. Namun dampak negatif pun tidak dapat dihindari. Semakin pesat perkembangan teknologi dapat menyebabkan munculnya kejahatan *cyber* atau disebut juga *cyber crime*. Beberapa kasus *cyber crime* seperti *credit card carding*, *site hacking*, penyadapan pada telepon dan email, *malware injection*, dan lainnya. Untuk menanggulangi permasalahan tersebut, terdapat beberapa solusi seperti *bot* dan juga *Intrusion Detection System (IDS)*.

IDS adalah metode yang dapat digunakan untuk mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Terdapat banyak jenis IDS yang bersifat *closed source* atau komersil dan *open source* atau jenis terbuka yang dapat dimodifikasi sedemikian rupa untuk memenuhi kebutuhan user. *BriarIDS* merupakan salah satu tools IDS berjenis *open source*. *BriarIDS* dapat dihubungkan dengan IDS lainnya seperti Bro untuk penambahan opsi log. *BriarIDS* dapat diimplementasikan di *Raspberry Pi* sehingga tidak perlu PC untuk memonitoring. Pada Proyek Akhir ini, penulis akan mengimplementasikan *BriarIDS* dan *Raspberry Pi* sebagai *Instrusion Detection System* dari suatu sistem jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, maka permasalahan yang dibahas adalah:

1. Bagaimana cara mengimplementasikan *BriarIDS* dengan *Raspberry Pi*?
2. Bagaimana cara *BriarIDS* dapat mendeteksi ketika terjadi serangan?

1.3 Batasan Masalah

Adapun tujuan dari proyek akhir ini adalah:

1. Sistem *BriarIDS* dapat berfungsi pada *Raspberry Pi*
2. Sistem *BriarIDS* dapat mendeteksi terjadinya serangan terhadap suatu jaringan

2. Tinjauan Pustaka

2.1 Teori

2.1.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) atau Sistem Pendeteksi Serangan adalah metode yang digunakan untuk memantau sistem komputer secara *real-time* untuk melihat aktivitas mencurigakan. Sistem ini mendeteksi pengguna yang tidak berwenang yang mencoba masuk ke dalam sistem dengan membandingkan perilaku pengguna dengan profil pengguna, mendeteksi kejadian yang menjadi indikasi peretasan, dan juga memberikan informasi secara langsung mengenai tipe serangan yang dilakukan serta IP dan perangkat penyerang [1]. Terdapat beberapa jenis IDS, diantaranya:

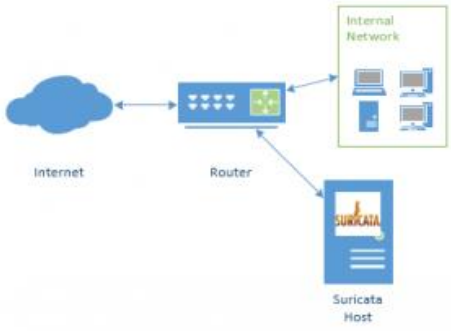
1. ***Host Based IDS***

   Jenis IDS ini memungkinkan user untuk menginstall sistem langsung pada PC pengguna yang dapat langsung dimonitor.

2. ***Passive IDS***

   Dalam Passive IDS, semua *traffic* yang keluar dan masuk pada router langsung dicopy datanya menuju IDS. Saat mendeteksi adanya aktivitas yang mencurigakan, IDS segera memberitahukan kepada Admin tentang informasi Penyerang.

Router yang menjadi jembatan antara internet dan jaringan internal, akan dimonitor oleh *host* yang telah terinstal IDS. Jika terdapat aktivitas mencurigakan dari luar (internet) atau jaringan internal, maka sistem IDS akan langsung memberikan informasi terkait info penyerang, mulai dari IP hingga tipe serangan. Contohnya *user* yang tidak berwenang mencoba masuk ke dalam server. Cara kerja IDS dijelaskan pada **Gambar 1**.



Gambar 1: Cara Kerja IDS

1.4 Raspberry Pi

Raspberry Pi adalah sebuah komputer papan tunggal (*Single Board Computer*) berukuran kartu kredit yang dihubungkan ke TV (via *HDMI*) dan keyboard. Sebagai *IoT (Internet of Things)*, seperti layaknya sebuah *desktop*. Desain *Raspberry Pi* 2 model B didasarkan seputar SoC *(System on a chip*) *Broadcom BCM2835*, yang telah menanamkan prosesor *quad-core ARM Cortex-A7* dengan 900 MHz, VideoCore IV GPU, dan 1 Gigabyte RAM. Penyimpanan data didesain tidak untuk menggunakan hard disk atau solid-state drive, melainkan mengandalkan kartu SD (SD memory card) untuk booting dan penyimpanan jangka panjang. Raspberry Pi utamanya menjalankan sistem operasi berbasis kernel Linux [2]. Bentuk *Raspberry Pi* seperti pada **Gambar 2**.

Gambar 2: Raspberry Pi

1.5 BriarIDS

BriarIDS adalah salah satu *Intrusion Detection System* berbasis Raspberry Pi. *BriarIDS* merupakan *tools* IDS yang memiliki beberapa aplikasi, diantaranya Suricata. Selain itu *BriarIDS* dapat juga diintegrasikan dengan *Snorby*. *BriarIDS* dibuat menggunakan PyQT GUI yang memungkinkan software ini mempunyai kelebihan yaitu adanya GUI (*Graphical User Interface).* Kelebihan lain dibanding IDS lainnya adalah proses konfigurasinya yang mudah. Meskipun *BriarIDS* dapat digunakan untuk memonitoring jaringan WAN, tetapi *BriarIDS* dirancang untuk jaringan rumah, karena instalasi dan

pengaturan yang mudah [3]. Tampilan GUI pada *BriarIDS* seperti **Gambar 3**.

Gambar 3: Tampilan GUI pada *BriarIDS*

1.6 Router

Router adalah sebuah alat yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Proses routing terjadi pada lapisan 3 (Lapisan jaringan seperti *Internet Protocol*) dari *stack protokol* tujuh lapis OSI [4]. Bentuk *Raspberry Pi* seperti pada **Gambar 4**.

Gambar 4: Router

2.2 Analisis Sistem

2.2.1 Gambaran Sistem Saat Ini

Terdapat kondisi dimana ada serangan. Jika tidak ada serangan admin akan selalu siaga mengawasi jaringan, jika admin mendeteksi aktivitas mencurigakan, admin akan segera menganalisa dan langsung mengambil langkah tepat untuk menghentikan serangan. Blok Diagram dijelaskan pada **Gambar 5**.

Gambar 5: Blok Diagram Saat Ini

2.2.2 Analisis Kebutuhan Sistem

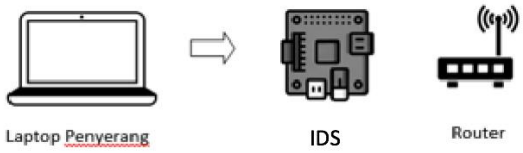
Adapun kebutuhan yang dibutuhkan sistem dalam pembahasan proyek akhir ini. Sistem ini membutuhkan:

1. *Wireless Router* untuk mengirimkan paket melalui jaringan internet untuk disalurkan ke perangkat lain.
2. *Raspberry Pi* sebagai alat untuk memproses dan menganalisa jaringan

2.3 Perancangan

2.3.1 Gambaran Sistem Usulan

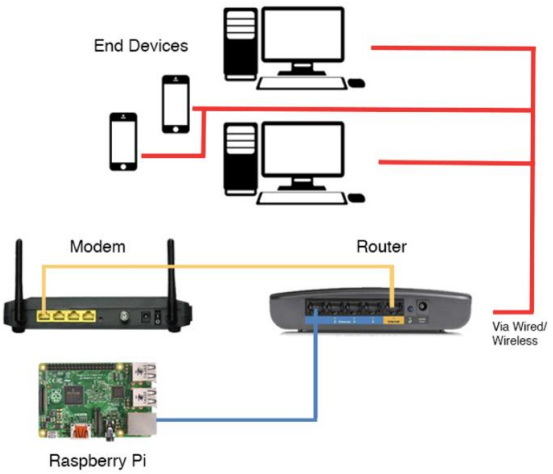
Terdapat kondisi dimana ada serangan. Terdeteksinya serangan atau tidak berdasarkan hasil analisa dari *Raspberry Pi*. Jika terdapat serangan, *Raspberry Pi* akan segera menginfokan user *IP Address* penyerang, perangkat penyerang, dan jenis serangan yang dilakukan. Dengan begitu admin dapat mengambil langkah tepat untuk menghentikan serangan. Blok diagram dijelaskan pada **Gambar 6**.



Gambar 6: Gambaran Sistem Usulan

2.3.2 Topologi Sistem

Modem menyalurkan internet ke *Wireless Router* dan *Wireless Router* menyebarkannya ke perangkat secara *wireless* atau dengan kabel. *Raspberry Pi* dihubungkan dengan salah satu *port* pada *router* sebagai sistem pendeteksi serangan. Topologi dijelaskan pada **Gambar 7**.



Gambar 7: Topologi Sistem

2.3.3 Cara Kerja

Ketika terjadinya serangan, maka *Raspberry Pi* akan menganalisa secara langsung jenis serangan yang terjadi dan menginformasikannya kepada admin. Lalu admin akan dengan mudah mencari solusi yang tepat untuk menghentikan serangan tersebut.

2.3.4 Spesifikasi Sistem

Adapun spesifikasi minimal yang dibutuhkan yaitu:

2.3.4.1 Perangkat Keras

Tabel 1 Perangkat Keras (Hardware)

No	Perangkat Keras	Jumlah	Keterangan
1	*Raspberry Pi*	1 Buah	*Raspberry Pi Unit B model* versi *3*
2	*Router (Linksys E1200v2)*	1 Buah	*Router* yang mendukung *Tomato* agar paket sampai ke antarmuka *BriarIDS*
3	*SD Card*	1 Buah	Untuk memory *Raspberry Pi*, minimal 16 GB
4	*USB Wifi Dongle*/Kabel *Ethernet*	1 Buah	Untuk menghubungkan *Raspberry Pi* dengan *Router*
5	*Macbook Air*	1 Buah	Untuk pembuatan laporan dan konfigurasi router

2.3.4.2 Perangkat Lunak

Tabel 2 Perangkat Lunak (Software)

No	Perangkat Lunak	Keterangan
1	Raspbian	Sistem Operasi untuk *Raspberry Pi*
2	*BriarIDS*	*Software* untuk sistem pendeteksi serangan
3	*Tomato by Shibby*	*Firmware open source* untuk *router*
4	*Kali Linux*	Untuk tes serangan ke *router*
5	macOS Sierra	Untuk pembuatan laporan dan konfigurasi router

3. Kesimpulan dan Saran

3.1 Kesimpulan

Kesimpulan dari Proyek Akhir ini yaitu:

1. Sistem *BriarIDS* dapat berfungsi sebagai pendeteksi serangan dalam jaringan pada Raspberry Pi dengan *real time*, mendeteksi tiga tipe serangan dengan *IP Address* yang sama pada *scanning nmap* dan *metasploit*. *IP Address* penyerang pada serangan *Hydra* menuju *web server* berbeda karena pengujian yang dilakukan pada waktu yang berbeda.

2. Sistem *BriarIDS* berhasil mendeteksi terjadinya serangan terhadap suatu jaringan dengan informasi berupa waktu serangan, tipe serangan, tingkatan serangan, hingga *IP Address* penyerang.

3.2 Saran

Adapun saran dari penulis untuk dapat mengembangkan sistem ini adalah sebagai berikut:

1. Menampilkan notifikasi detail mengenai tipe serangan, *IP Address* penyerang, dan waktu penyerangan ke PC atau menuju smartphone seperti *WhatsApp*, *Telegram*, atau *Line*.

2. Sistem dapat menangani sendiri serangan yang ada

4. Daftar Pustaka

[1] Rowland, Craig H. "Intrusion detection system." U.S. Patent No. 6,405,318. 11 Jun. 2002.

[2] Maulana Andang Rosidi, R. Rumani M. , Randy Erfa Saputra, 2017 "Perancangan dan Pengontrolan Sistem Kendali Mekanika Keranjang Bayi Pada Sistem *Smart Baby Monitoring* dengan *Raspberry Pi*" eProceedings of Engineering, vol. 4, no. 2, pp. 2382-2383.

[3] Musicmancorley. "musicmancorley/BriarIDS." GitHub. n.d. Web. 5 Dec. 2017. <https://github.com/musicmancorley/BriarIDS>

[4] Kusniadi. "Pengertian, Jenis, Fungsi dan Cara Kerja Router | UNBAJA." Unbaja.ilearning.me. 18 Nov. 2015. Web. 5 Dec. 2017. http://unbaja.ilearning.me

[5] Lyon, Gordon. Chapter 15. Nmap Reference Guide." Implementation Details | Nmap Network Scanning, nmap.org/book/man.html.

[6] "Hydra: Password Cracking Tool (Summary, Tutorial and Resources)." Concise Courses, www.concise-courses.com/security/what-is-hydra/.

[7] Maynor, David. Metasploit toolkit for penetration testing, exploit development, and vulnerability research. Elsevier, 2011