JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

SISTEM DETEKSI INTRUSI DAN PREVENSI BERBASIS OPEN SOURCE

ANDI MUHAMMAD NUR HIDAYAT

Teknik Informatika Fakultas Sains dan Teknologi
Universitas Islam Negeri Alauddin Makassar

E-mail: andi.nurhidayat@uin-alauddin.ac.id

ABSTRAK

Dalam infrastruktur pembuat jaringan nirkabel menjadi dilirik oleh semua orang. Hal ini menimbulkan resiko yang dapat terjadi dikarenakan setiap pengguna yang mampu menangkap gelombang elektromagnetik yang ditransmisikan oleh *Access Point*. Pengguna disini bisa memanfaatkan celah yang terjadi pada jaringan Nirkabel. Celah yang dimaksud adalah serangan yang dilakukan oleh orang yang tidak bertanggung jawab, sehingga membuat pengguna lain kehilangan data, informasi penting dan sebagainya. Maka perlu adanya aplikasi yang dapat mendeteksi dan mencegah serangan yang dapat terjadi. Salah satu aplikasi yang cukup baik yaitu WAIDPS berbasis *opensource* sehingga dapat dikembangkan lebih lanjut oleh penggunanya. Pada penelitian kali ini, aplikasi WAIDPS digunakan untuk mendeteksi serangan yang terjadi, terlebih dahulu dibuat scenario untuk menguji aplikasi tersebut. Saat pengujian scenario serangan yang dilakukan mampu dideteksi oleh aplikasi WAIDPS dan aplikasi WAIDPS dapat berjalan pada komputer dengan *resource memory* yang cukup kecil.

Kata Kunci*: WAIDPS, Sistem Deteksi Intrusi, Open Source, Security;*

I. PENDAHULUAN

Perkembangan teknologi khususnya dibidang jaringan sangatlah pesat, saat ini semua perangkat terbaru sudah memiliki sebuah alat yang mentransmisikan data secara nirkabel. Teknologi nirkabel ini membuat semua infrastruktur jaringan yang awalnya menggunakan kabel beralih menjadi jaringan nirkabel. Sifatnya yang fleksibel dan lebih mudah dalam melakukan perancangan ataupun penambahan dalam infrastrukturnya membuat jaringan nirkabel menjadi dilirik oleh semua orang. Kemudahan dalam mobilitas jaringan nirkabel (Gast, 2005). Pengguna dari jaringan nirkabel dapat berpindah tempat tanpa harus kesulitan perlu terhubung

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

dengan kabel, asalkan perangkat tersebut masih mampu menangkap gelombang elektromagnetik yang dipancarkan oleh antena dari perangkat tersebut. Namun sifat yang fleksibel dan mempunyai mobilitas tinggi ini memiliki kelemahan, setiap perangkat yang memancarkan gelombang elektromagnetik sangat rentan terkena gangguan ataupun serangan. Transmisi atau pengiriman ke semua arah merupakan sifat dari jaringan nirkabe;. Kelemahan ini menjadi salah satu celah dari jaringan nirkabel (Liao, Richard Lin, Lin, & Tung, 2012).

Pada jaringan komputer, kelemahan yang terjadi bisa dimanfaatkan oleh orang yang tidak bertanggung jawab untuk melakukan serangan. Pada dasarnya serangan ini dibagi menjadi dua yaitu serangan pasif dan serangan aktif. Serangan bertipe pasif biasanya hanya melakukan pemantauan terhadap targetnya tanpa dapat dideteksi oleh pengguna, attacker adalah orang yang melakukan serangan pada jaringan. Sedangkan serangan aktif biasanya terlebih dahulu melakukan pemantauan kemudian melakukan modifikasi terhadap aliran data yang melewati jaringan. Sehingga diperlukan sistem untuk memonitoring sebuah jaringan nirkabel. Sistem keamanan tersebut selain mampu mendeteksi juga mampu melakukan pencegahan terhadap serangan tersebut (Sharma, Sharma, & Singh, 2012).

Salah satu langkah yang bisa dilakukan yaitu melindungan jaringan nirkabel dengan memanfaatkan Sistem Deteksi Intrusi dan Prevensi (Deng, Cushman, & Delleur, 1993).Terdapat beberapa aplikasi yang bisa digunakan untuk memantau serangan yang terjadi pada sebuah jaringan seperti *wireshark, shareAlarm, dan X-Ray.* Aplikasi yang digunakan pada penelitian ini adalah aplikasi berbasis *open source* yang bernama WAIDPS. Keunggulan aplikasi yang bersifat *opensource* yaitu dapat dilakukan pengembangan sesuai dengan keinginan dari pengguna (Timofte, 2008). Selain itu aplikasi WAIDPS ini penggunaan memory pada komputer cukup kecil sehingga tidak membutuhkan komputer yang memiliki spesifikasi tinggi.

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

II.METODE PENELITIAN

A. SISTEM DETEKSI INTRUSI DAN PREVENSI

Sistem Deteksi Intrusi adalah sebuah sistem yang mempunyai beberapa klasifikasi perkembangan teknologi. Sistem Deteksi Intrusi dapat dikategorikan menjadi dua, yaitu Network Based Intrusion Detection (NIDS) dan Host-Based Intrusion Detection (HIDS) (Liao et al., 2012). NIDS dalam prosesnya melakukan evaluasi informasi yang diperoleh dari sebuah jaringan komunikasi, informasi tersebut kemudian dianalisis. NIDS juga dikembangkan untuk membantu mendeteksi kelemahan yang ada pada cloud computing (Modi, Patel, Patel, & Rajarajan, 2012). Sedangkan HIDS melakukan evaluasi informasi yang ditemukan pada komputer host (Yeung & Ding, 2003). Pada penelitian kali ini penulis menggunakan Wireless Auditing, Intrusion Detection and Prevention System sebagai aplikasi untuk mendeteksi intrusi atau serangan yang terjadi. Proses kerja WAIDPS yaitu dengan melakukan pemantauan aktifitas-aktifitas yang mencurigakan pada jaringan nirkabel. WAIDPS juga melakukan proses sniffing terhadap packet data yang berjalan pada jaringan (Alhomoud, Munir, Disso, Awan, & Al-Dhelaan, 2011).

B. GANGGUAN/SERANGAN PADA JARINGAN

Pada jaringan nirkabel, terdapat beberapa gangguan atau serangan yang sering terjadi. Serangan yang umum terjadi yaitu *Denial of Service, Remote User Attack, Probing*, dan *User Root Attack* (Hoque, Mukit, & Bikas, 2012). Berikut penjelasannya:

1. *Denial of Service*

   Teknik yang menyerang langsung ke server, cara paling umum yang dilakukan adalah dengan membanjiri lalu lintas data ke server, pada akhirnya server tidak dapat menangani permintaan dikarenakan *overload* jaringan (Mohammed & Sulaiman, 2012).

2. *Remote User Attack*

   Serangan ini bertujuan untuk mengendalikan targetnya dari jarak jauh kemudian akan mengeksploitasi komputer yang terlah dikuasai oleh *attacker*

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

(Elbasiony, Sallam, Eltobely, & Fahmy, 2013). Biasanya akan mengambil data-data penting yang terdapat pada komputer target.

3. *Probing*

   Teknik dimana *attacker* melakukan pemindaian perangkat yang sedang terhubung pada sebuah jaringan (Sharma et al., 2012). Setelah itu perangkat yang telah dideteksi, akan dicari kelemahannya.

4. *User Root Attack*

   Teknik yang mengeksploitasi targetnya, *attacker* akan mencoba masuk sebagai akun biasa (Hoque et al., 2012). Setelah itu, attacker akan berusaha memperoleh hak akses *Root* pada sebuah sistem.

C.TAHAPAN PENELITIAN

Pada penelitian ini, proses pengumpulan data dilakukan menjadi dua tahap yaitu dengan metode kepustakaan dan eksperimental. Data yang dikumpulkan dapat berupa data primer serta data sekunder yang mampu menunjang penelitian yang dilakukan penulis. Berikut pengertian dari metode kepustakaan dan metode eksperimental pada penelitian ini yaitu:

1. Metode Kepustakaan

   Metode ini merupakan metode dimana penulis membaca data tertulis yang terdapat di buku, jurnal-jurnal ilmiah serta tutorial yang tersebar di internet. Data tersebut kemudian akan diproses dan dijadikan bahan penunjang penelitian.

2. Metode Eksperimental

   Metode ini digunakan dengan cara melakukan eksperimen terhadap objek yang diteliti. Jika ingin menguji pendapat dari penulis ataupun orang lain maka dilakukan eksperimen yang berhubungan dengan sistem deteksi intrusi dan prevensi pada jaringan nirkabel. Tujuan agar dapat mengetahui sistem tersebut dapat berjalan sesuai dengan fungsinya.

III.HASIL DAN PEMBAHASAN

Setelah dilakukan pengumpulan data, maka dilakukan pengujian untuk menguji aplikasi WAIDPS, penulis membuat skenario serangan untuk menguji

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

sistem tersebut. Proses pengujian dilakukan untuk mengetahui apakah aplikasi ini dapat mendeteksi skenario serangan yang diberikan. Daftar skenario serangan yang akan dilakukan dapat dilihat pada tabel 1.

Tabel 1. Skenario pengujian serangan

Skenario Serangan	Keterangan
Beacon Flood Attack	*Attacker* melakukan serangan dengan cara mengirimkan *Beacon Frames* dengan membuat banyak *Access Point* palsu. Hal ini akan menyebabkan jaringan nirkabel menjadi *crash*.
Autentication DoS Mode	*Attacker* melakukan penyerangan dengan caramengirimkan *Frame Auth* ke semua *Access Point* yang terlacak dalam jaringan nirkabel. Pengguna tidak dapat terhubung ke *Access Point*, bahkan pengguna yang sudah terkoneksi menjadi *disconnect*.
Murder Death Kill 3	*Attacker* melakukan penyerangan dengan cara membanjiri lalu lintas jaringan nirkabel yang tertuju ke *Access Point*. Akhirnya pengguna akan terhalang dan tidak dapat terhubung pada *Access Point*.
WPA Downgrade	*Attacker* melakukan serangan pengiriman paket enkrispsi kemudian semua pengguna yang ada akan mengalami proses *deauthenticates*.
WPA and WEP All Cracking Method	*Attacker* melakukan penyerangan dengan memanfaatkan konfigurasi jaringan yang buruk. Sehingga *Attacker* dapat mengambil alih *Access Point* yang sedang digunakan oleh pengguna.

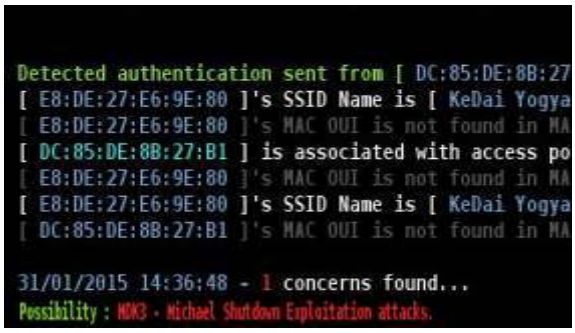
Pada proses pengujian, penulis ingin mengetahui kemampuan dari sistem dalam mendeteksi scenario serangan yang telah dirancang sebelumnya. Langkah selanjutnya menjalankan aplikasi WAIDPS pada terminal di *Linux.* Aplikasi ini harus berjalan selama proses serangan dilakukan, sehingga aplikasi ini dapat memonitoring lalulintas yang terjadi pada jaringan nirkabel.

Setelah aplikasi WAIDPS berjalan, maka aplikasi ini akan memonitoring jaringan yang telah kita tentukan.

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

Gambar 1. Proses WAIDPS melakukan monitoring

Pada gambar 1, terdapat pesan *alert* karna proses pengguna melakukan koneksi ke *Access Point.* Pada angka 2 WAIDPS belum mendeteksi terjadinya serangan pada jaringan. Selanjutnya proses serangan akan dilakukan sesuai dengan skenarionya. Saat proses serangan berjalan, maka akan ada informasi terjadi terkait serangan yang dideteksi oleh WAIDPS



Gambar 2. Aplikasi Mendeteksi Serangan yang Terjadi.

Pada gambar 2, aplikasi WAIDPS mulai mendeteksi serangan yang terjadi dan mengklasifikasikan serangan tersebut sebagai *MDK3 – Michael Shutdown Exploitation Attacks*. Setelah semua scenario serangan dilakukan, WAIDPS dapat mendeteksi scenario serangan yang dilakukan, sehingga pengujian dapat dikatakan berhasil.

IV.KESIMPULAN

Berdasarkan hasil pengujian dengan skenario serangan yang dibuat aplikasi WAIDPS mampu mendeteksi dan mengklasifikasikan serangan yang terjadi. Bahkan proses authentikasi dan deauthentikasi yang dilakukan oleh pengguna jaringan semua bisa dimonitoring oleh aplikasi. Setelah itu administrator

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

jaringan bisa segera melakukan pencegahan agar tidak terjadi kerugian pada pengguna. Aplikasi WAIDPS mampu dikembangkan untuk selanjutnya diterapkan pada jaringan komputer yang sesuai dengan kebijakan masing-masing. Proses monitoring dari WIDPS ini bersifat *real-time* sehingga dibutuhkan proses pengawasan oleh administrasi jaringan.

DAFTAR PUSTAKA

Alhomoud, A., Munir, R., Disso, J. P., Awan, I., & Al-Dhelaan, A. (2011). Performance evaluation study of Intrusion Detection Systems. *Procedia Computer Science*, *5*, 173–180. https://doi.org/10.1016/j.procs.2011.07.024

Deng, F. -W, Cushman, J. H., & Delleur, J. W. (1993). A Fast Fourier transform stochastic analysis of the contaminant transport problem. *Water Resources Research*, *29*(9), 3241–3247. https://doi.org/10.1029/93WR01236

Elbasiony, R. M., Sallam, E. a., Eltobely, T. E., & Fahmy, M. M. (2013). A hybrid network intrusion detection framework based on random forests and weighted k-means. *Ain Shams Engineering Journal*, *4*(4), 753–762. https://doi.org/10.1016/j.asej.2013.01.003

Gast, M. (2005). *802.11 Wireless Networks: the Definitive Guide*. Retrieved from http://books.google.com/books?hl=en&lr=&id=9rHnRzzMHLIC&oi=fnd&pg=PR3&dq=802.11+Wireless+Networks:+The+Definitive+Guide&ots=3xwTL5_6Dw&sig=aaTEwEJTPRr3JxIsdLGG0fZYFfE

Hoque, M., Mukit, A., & Bikas, A. (2012). An Implementation of Intrusion Detection System Using Genetic Algorithm. *International Journal of Network Security & Its Applications*, *4*(March), 109–120.

Liao, H.-J., Richard Lin, C.-H., Lin, Y.-C., & Tung, K.-Y. (2012). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Modi, C. N., Patel, D. R., Patel, A., & Rajarajan, M. (2012). Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing. *Procedia Technology*, *6*, 905–912. https://doi.org/10.1016/j.protcy.2012.10.110

Mohammed, M. N., & Sulaiman, N. (2012). Intrusion Detection System Based on SVM for WLAN. *Procedia Technology*, *1*, 313–317. https://doi.org/10.1016/j.protcy.2012.02.066

JURNAL INSTEK
INFORMATIKA SAINS DAN TEKNOLOGI
Volume 6 Nomor. 1, April 2021
P –ISSN : 2541-1179, E-ISSN : 2581-1711
Ojs :http://journal.uin-alauddin.ac.id/index.php/instek/index
Email : instek@uin-alauddin.ac.id

Sharma, P., Sharma, N., & Singh, R. (2012). A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network. *International Journal of Computer Applications*, *41*(March), 16–21. https://doi.org/10.5120/5824-8064

Timofte, J. (2008). Intrusion Detection using Open Source Tools. *Informatica Economica Journal*, *2*(46), 75–79. Retrieved from http://www.revistaie.ase.ro/content/46/Timofte.pdf

Yeung, D., & Ding, Y. (2003). Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognition*, *36*(1), 1–34.