Full Paper

ANALISIS DAN PERANCANGAN KEAMANAN JARINGAN MENGGUNAKAN OS UNTANGLE DENGAN METODE INTRUSION PREVENTION SYSTEM (IPS)

Muhammad Jufri[1]
[1]Program Studi Perdagangan Internasional, Institut Teknologi Batam, Indonesia

Informasi Artikel

Terbit: Juli 2025

Kata Kunci:

Instrusion Detection System (IDS)
Instrusion Prevention System (IPS)
Firewal

ABSTRAK

Seiring dengan Perkembangan Teknologi Informasi menjadikan keamanan suatu informasi sangatlah penting terlebih lagi pada suatu jaringan yang terkoneksi dengan internet. Namun yang cukup disayangkan adalah ketidak seimbangan antara setiap perkembangan suatu teknologi tidak diiringi dengan perkembangan pada sistem keamanan itu sendiri dengan demikian cukup banyak system - sistem yang masih lemah dan harus ditingkatkan keamanannya. Keamanan suatu jaringan seringkali terganggu dengan adanya ancaman dari dalam ataupun dari luar. Serangan tersebut berupa serangan Hacker yang bermaksud merusak Jaringan Komputer yang terkoneksi pada internet ataupun mencuri informasi penting yang ada pada jaringan tersebut. Hadirnya firewall telah banyak membantu dalam pengamanan, akan tetapi seiring berkembang teknolgi sekarang ini hanya dengan firewall keamanan tersebut belum dapat dijamin sepenuhnya. Karena itu telah berkembang teknologi IDS dan IPS sebagai pembantu pengaman data pada suatu jarigan komputer. Dengan adanya Intrusion Detection System (IDS) dan Instrusion Prevention System (IPS), maka serangan - serangan tersebut lebih dapat dicegah ataupun dihilangkan. IDS berguna untuk mendeteksi adanya serangan dari penyusup (serangan dari dalam), sedangkan IPS berguna untuk mendeteksi serangan dan menindak lanjutinya dengan pemblokan (filter) serangan.

Corresponding Author:

Muhammad Jufri

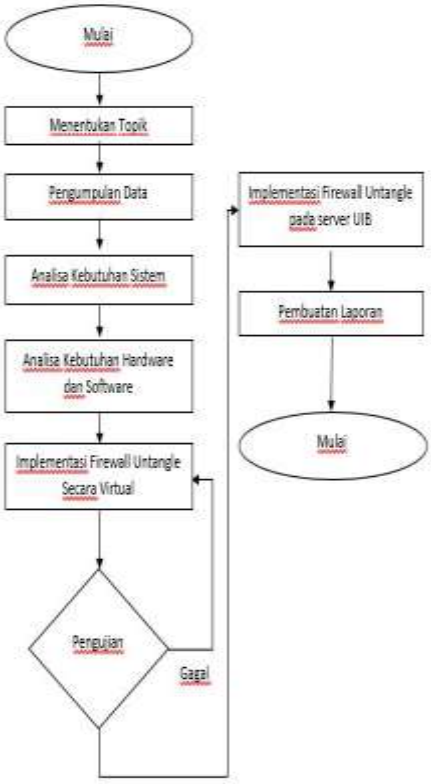
Email: jufrim43@gmail.com

1. PENDAHULUAN

Dengan perkembangan teknologi tersebut, kejahatan teknologi komunikasi dan informasi juga ikut berkembang. Keamanan data pada komputer yang terhubung dalam sebuah jaringan sangat penting untuk dijaga validitas dan integritasnya serta dijamin ketersediaannya bagi pengguna. Sistem harus dilindungi dari pengguna yang tidak berhak mengaksesnya. Sekarang ini sudah begitu banyak cara untuk seorang *intruder* (peretas) melakukan serangan terhadap suatu sistem jaringan komputer [1]. Sesuai dengan perkembangan jaman, cara – cara dalam melakukan intrusi sendiri pun ikut berkembang hingga sekarang. Sebelumnya untuk melakukan sebuah serangan terhadap sebuah sistem dibutuhkannya pengetahuan dan pemahaman teknis mengenai jaringan komputer yang mendalam, akan tetapi saat ini para peretas lebih mudah meretas sebuah sistem bahkan orang awam pun dapat melakukannya dengan mudah tanpa harus memiliki *skill* yang tinggi dikarenakan telah banyaknya *tools* gratis yang beredar di internet yang memudahkan *intruder* untuk meluncurkan serangan ke sebuah sistem [2]. Salah satu serangan yang sering digunakan yaitu serangan *Denial of Service* (DoS). Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman keamanan yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis langsung mengatasi penyusupan keamanan tersebut sehingga kemungkinan kerusakan akibat penyusupan keamanan jaringan dapat lebih diminimalisir. Sistem pencegahan penyusupan (*Intrusion Prevention System*) adalah sebuah sistem yang

bekerja secara otomatis untuk memonitor kejadian pada jaringan komputer dan dapat mengatasi masalah keamanan jaringan.

2. METODE PENELITIAN



Gambar 1. Kerangka Penelitian

Bentuk penelitian yang digunakan oleh penulis adalah penelitian terapan. Penelitian terapan adalah salah satu penelitian yang bertujuan untuk memberikan solusi atas permasalahan tertentu secara praktis. Penelitian ini tidak berfokus pada pengembangan sebuah ide, teori, atau gagasan, tetapi lebih berfokus kepada penerapan penelitian tersebut dalam kehidupan sehari-hari[3].

Teknik pengumpulan data yang digunakan dalam pembuatan laporan ini adalah teknik pengumpulan data dengan metode wawancara dan observasi. Teknik pengumpulan wawancara. wawancara yang peneliti lakukan adalah dengan cara mewawancarai *staff IT Center* Universitas Internasional Batam selaku pihak yang bertanggung jawab dalam penanganan jaringan di Universitas Internasional Batam. Metode observasi juga merupakan salah satu teknik yang digunakan oleh penulis dalam pembuatan laporan. Observasi adalah salah saatu teknik pengumpulan data yang menggunakan indra mata. Observasi dilakukan untuk memproleh gambaran nyata suatu peristiwa atau kejadian sebagai bahan untuk pembuatan laporan.

3. HASIL DAN PEMBAHASAN

Intrusion Prevention System (IPS) akan mengirimkan sebuah peringatan (alert) kepada network atau system administrator ketika suatu hal yang mencurigakan terdeteksi, memungkinkan administrator dapat memilih sebuah tindakan untuk diambil ketika terjadi sebuah event. Intrusion prevention system dapat memonitor seluruh jaringan, wireless network, perilaku jaringan (network behavior) dan traffic sebuah komputer. Setiap IPS menggunakan metode deteksi tertentu untuk menganalisa resiko.

Tergantung dari model IPS yang digunakan beserta fitur – fiturnya, sebuah intrusion prevention system dapat mendeteksi berbagai macam pelanggaran keamanan. Beberapa diantaranya

dapat mendeteksi penyebaran malware pada sebuah jaringan, duplikasi file – file besar diantara dua komputer, dan mendeteksi adanya aktivitas mencurigakan seperti aktivitas port scanning.

Setelah IPS membandingkan masalah yang muncul dengan aturan keamanan (security rule) yang telah dibuat, maka IPS akan mencatat setiap event dan akan mencatat frekuensi kemunculan event. Jika seorang network administrator mengkonfigurasikan IPS untuk menjalankan tindakan tertentu berdasarkan kejadian, intrusion prevention system kemudian akan menjalankan perintah yang telah diberikan tersebut. Sebuah basic alert akan dikirimkan pada administrator, sehingga administrator dapat merespon secara tepat atau melihat informasi tambahan pada IPS jika diperlukan [4]

Untangle merupakan sistem operasi *open source* pertama yang terintegrasi untuk menangani masalah *spam,spyware,adware,* dan *web content* yang tidak diinginkan pada jaringan komputer. *Untangle* memberikan solusi praktis dan sederhana untuk menggabungkan berbagai fungsi produk-produk keamanan jaringan yang dibutuhkan oleh sebuah organisasi yang menggunakan jaringan komputer yang nantinya diletakkan pada *network gateway*. *Untangle* juga memiliki sebuah fitur yang diterapkannya sebuah teknologi yang disebut dengan istilah *virtual pipelining technology*. *Virtual pipelining technology* adalah sebuah teknologi yang memungkinkan beberapa aplikasi dijalankan pada sebuah PC dengan *latency* atau kebutuhan *processor* yang rendah.

Selain itu keunggulan dari *untangle* adalah proses instalasi yang sangat mudah karena tidak dibutuhkan pengetahuan yang tinggi tentang keamanan jaringan dan dalam melakukan konfigurasi aplikasi keamanan yang akan digunakan. Tampilan *software untangle* sangat enak digunakan karena menu-menu yang tersedia bersifat informatif. Selain itu juga terdapat fitur untuk melakukan update secara otomatis [7].

Metode pengamanan yang banyak digunakan saat ini seiring berkembangnya teknologi mengenai jaringan komputer yaitu IDS (intrusion detection system) dan IPS (intrusion prevention system) yang dapat melakukan pengaturan agar keamanan informasi dalam jaringan tersebut dapat diatur atau dijaga dan juga keamanan jaringannya pun menjadi lebih aman.

IPS (intrusion prevention system) adalah metode pengamanan jaringan yang dapat berupa software ataupun hardware. IPS dapat melakukan monitoring terhadap seluruh aktifitas pada jaringan, IPS akan langsung melakukan pencegahan terhadap gangguan – gangguan atau intrusion seperti blocking atau drop program gangguan[8, 9].

Kelebihan dari IPS yaitu sistem yang dimilikinya mempunyai kecerdasan buatan sendiri yang dapat mempelajari dan mengenali serangan dan metode yang digunakan dalam penyerangan tersebut (triger). IDS dan IPS melakukan pendeteksian dan melakukan pencegahan terhadap gangguan atau intrusion berdasarkan signature atau pattern yang terdapat dalam rule yang dibuat. Paket data yang datang terlebih dahulu akan diperiksa kecocokannya terhadap rule yang dibuat, apabila terdapat kesamaan, maka secara IDS dan IPS akan melakukan peringatan (alert) dan selanjutnya akan melakukan pencegahan berupa blocking terhadap gangguan tersebut [10].

4. KESIMPULAN

Setelah melakukan Analisa dari penelitian yang telah dilakukan maka keamanan dengan menggunakan IPS dari untangle, dari hasil analisis yang telah dilakukan dapat diketahui bawah ketika *web server* belum diterapkan sistem IPS. Maka serangan membuat *web server* mengalami kenaikan pada *network*, dimana client tidak dapat mengakses *website* atau mengalami koneksi yang sangat lambat ketika mengakses *website* tersebut. Jika terkena serangan maka resource dan monitoring pada server akan naik secara *signifikan*. Implementasi dari intrusion prevention system dapat melindungi server dari ancaman attacker, karena IPS dapat mendeteksi dan mencegah adanya serangan yang mencurigakan pada jaringan

DAFTAR PUSTAKA

[1] Abriando, A., & Syafrizal, M. (2014). *Auto Capture File Log Pada Intrusion Prevention System (IPS) Saat Terjadi Serangan Pada Jaringan Komputer*. Yogyakarta. https://doi.org/10.1017/CBO9781107415324.004

[2] Alamsyah. (2011). Implementasi Keamanan Instrusion Detection System (IDS) Dan Instrusion Prevention System (IPS) Menggunakan Clearos. *SMARTek*, *9*(3), 223–229.

[3] Kalsum, T. U., & Khairil. (2014). Implementasi Intrusion Detection System Sebagai Keamanan Web Server Universitas Dehasen Bengkulu. *Pseudocode*, *2*(1), 155–169.

[4] Kristanto, Y. (2010). *Implementasi dan Unjuk Kerja Keamanan Jaringan Pada Infrastruktur Berbasis IDPS (Intrusion Detection Prevention System)*. Universitas Indonesia.
[5] Kusumawati, M. (2010). *Implementasi IDS (Intrusion Detection System) Serta Monitoring Jaringan Dengan Interface Web Berbasis Base Pada Keamanan Jaringan*. Universitas Indonesia.
[6] Mydza, D. maulidi. (2011). *Analisa Dan Konfigurasi Network Intrusion Prevention System (NIPS) Pada Linux Ubuntu 10 . 04 LTS*. Islam Negeri Sultan Syarif Kasim Riau.
[7] Pratama, M. S. (2012). *Pengamanan Jaringan Komputer Menggunakan Metode IPS (Intrusion Prevention System) Terhadap Serangan Backdoor Dan Synflood Universitas Pembangunan Nasional " Veteran " Jatim*. Pembangunan Nasional "Veteran" Jatim.
[8] Rurita, R. (2016). *Analisis dan Implementasi Intrusion Prevention System (IPS) terhadap serangan DoS (Denial of Service) berbasis Snort IDS dan IPtables pada Jaringan LAN*. Universitas Internasional Batam.
[9] Suhartono, D., Riyanto, A. D., & Astomo, Y. W. (2015). Intrusion Detection Prevention System (IDPS) pada Local Area Network (LAN). *Jurnal Telematika*, *8*(1), 24–42.
[10] Wibowo, R. A. (2014). *ANALISIS DAN IMPLEMENTASI IDS MENGGUNAKAN SNORT PADA CLOUD SERVER DI JOGJA DIGITAL VALLEY*. Yogyakarta