ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.2 No.1 Tahun 2023
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-2 2023
Fakultas Teknik, Universitas Pelita Bangsa, Februari 2023

Metode Keamanan Internet Menggunakan IPS
Internet Security Methods Using IPS

Yoga Pratama
Prodi Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
yogafrtm25@gmail.com

Abstract

Public security use cases introduce their own special needs for communications and cybersecurity. Tactical networks often need to operate in isolated situations with limited connections to centralized security services in the cloud and without the help of remote security administrators and analysts. Security solutions cannot interfere with rescue operations by blocking users even if they will communicate in an unnatural and potentially suspicious manner. Security solutions should aim to guarantee the availability of connectivity services even in hostile situations where the network is under attack. Tactical networks often need to operate in isolated situations with limited connections to centralized security services in the cloud and without the help of remote security administrators and analysts. Therefore, the solution should minimize configuration efforts in the field or be fully autonomous. Furthermore, security solutions cannot interfere with rescue operations by blocking users even if they will communicate in an unnatural and potentially suspicious way. On the other hand, security solutions should aim to guarantee the availability of connectivity services even in hostile situations where the network is under attack. The use of multiple filters on IPS makes it significantly more effective when inspecting, identifying and blocking attacks based on time sequences. IPS creates a new filter when a new attack method is identified.

Keywords: Cyber, Security, and IPS

Abstrak

Kasus penggunaan keamanan publik memperkenalkan kebutuhan khusus mereka sendiri untuk komunikasi dan keamanan siber. Jaringan taktis seringkali perlu beroperasi dalam situasi terisolasi dengan koneksi terbatas ke layanan keamanan terpusat di cloud dan tanpa bantuan administrator dan analis keamanan jarak jauh. Solusi keamanan tidak dapat mengganggu operasi penyelamatan dengan memblokir pengguna bahkan jika mereka akan berkomunikasi dengan cara yang tidak wajar dan berpotensi mencurigakan. Solusi keamanan harus bertujuan untuk menjamin ketersediaan layanan konektivitas bahkan dalam situasi yang tidak bersahabat di mana jaringan sedang diserang. Jaringan taktis seringkali perlu beroperasi dalam situasi terisolasi dengan koneksi terbatas ke layanan keamanan terpusat di cloud dan tanpa bantuan administrator dan analis keamanan jarak jauh. Oleh karena itu, solusinya harus meminimalkan upaya konfigurasi di lapangan atau sepenuhnya otonom. Selanjutnya, solusi keamanan tidak dapat mengganggu operasi penyelamatan dengan memblokir pengguna bahkan jika mereka akan berkomunikasi dengan cara yang tidak wajar dan berpotensi mencurigakan. Di sisi lain, solusi keamanan harus bertujuan untuk menjamin ketersediaan layanan konektivitas bahkan dalam situasi yang tidak bersahabat di mana jaringan sedang diserang. Penggunaan multiple filter pada IPS membuatnya secara signifikan lebih efektif ketika menginspeksi, mengidentifikasi dan memblokir serangan berdasarkan urutan waktu. IPS membuat filter baru ketika sebuah metode serangan baru diidentifikasi.

Kata kunci: Cyber, Keamanan, dan IPS

Pendahuluan

Perkembangan teknologi kini semakin pesat dan pemanfaatannya semakin luas dalam kehidupan sehari-hari. Hal tersebut tidak terlepas dari pengaruh semakin mudahnya dalam mengakses internet, sehingga dapat memperoleh informasi secara cepat, tanpa terbatas waktu dan tempat. Salah satu aspek yang memanfaatkan perkembangan teknologi adalah penyelenggaraan pemerintahan di Indonesia yaitu dengan ditetapkannya Peraturan Presiden Nomor 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik.

Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE. SPBE diperlukan untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya [1].

Sistem keamanan komputer, dalam beberapa tahun ini telah menjadi fokus utama dalam dunia jaringan komputer, hal ini disebabkan tingginya ancaman yang mencurigakan (Suspicious Threat) dan serangan dari Internet. Keamanan Komputer (Security) merupakan salah satu kunci yang dapat mempengaruhi tingkat Realibility (keandalan) termasuk Performance (kinerja) dan Availability (tersedianya) suatu Internetwork. Kerusakan yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada jaringan tersebut akan melambat atau bahkan akan merusak suatu sistem jaringan. Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang memberikan dampak terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan security policy sistem tersebut [2]

Kasus penggunaan keamanan publik memperkenalkan kebutuhan khusus mereka sendiri untuk komunikasi dan keamanan siber. Jaringan taktis seringkali perlu beroperasi dalam situasi terisolasi dengan koneksi terbatas ke layanan keamanan terpusat di cloud dan tanpa bantuan administrator dan analis keamanan jarak jauh. Oleh karena itu, solusinya harus meminimalkan upaya konfigurasi di lapangan atau sepenuhnya otonom. Selanjutnya, solusi keamanan tidak dapat mengganggu operasi penyelamatan dengan memblokir pengguna bahkan jika mereka akan berkomunikasi dengan cara yang tidak wajar dan berpotensi mencurigakan. Di sisi lain, solusi keamanan harus bertujuan untuk menjamin ketersediaan layanan konektivitas bahkan dalam situasi yang tidak bersahabat di mana jaringan sedang diserang [3].

Untuk membangun arsitektur keamanan IPS, perlu untuk melanjutkan dari tugas utama yang dilaksanakan oleh pusat ini. Ini, misalnya, pencegahan akses ilegal ke informasi yang diproses di intranet, penghancuran informasi tersebut, modifikasi, pemblokiran, penyalinan, penyediaan dan distribusi, serta tindakan ilegal lainnya dengan informasi ini; pencegahan dampak pada alat pengolah informasi teknis, akibatnya fungsi intranet dapat terganggu dan (atau) dihentikan memulihkan fungsi intranet, asalkan, antara lain, dengan membuat dan menyimpan salinan cadangan dari informasi yang diperlukan untuk ini, dll [4].

Metode Penelitian

Dalam penulisan ini dibuat dalam metode literatur review yang mana memberikan output terhadap data yang ada, serta penjabaran dari suatu penemuan sehingga dapat dijadikan suatu contoh untuk sebuah Jurnal dalam menyusun atau membuat pembahasan yang jelas dari isi masalah yang akan di jabarkan. Penulis mencari data atau bahan literatur dari jurnal atau artikel dan juga referensi dari berbagai jurnal sehingga dapat dijadikan suatu landasan yang kuat dalam isi atau pembahasan. Dari pembahasan ini adapun isi terkait dengan penggunaan metode literatur riview. Kajian ini mencari dan mengumpulkan beberapa jurnal-jurnal serta diambil beberapa kesimpulan lalu ditelaah secara mendalam melalui cara yang rinci agar terdapat suatu hasil akhir yang baik dan sesuia dengan apa yang diharapkan.

Hasil Pembahasan

Seperti yang kita semua tahu, jaringan komputer itu sendiri dibangun dalam keadaan virtual, begitu kerentanan informasi jaringan benar-benar muncul, di lingkungan konstruksi jaringan virtual, lebih mudah untuk menyembunyikannya, sehingga sulit ditemukan, jadi sulit untuk mengendalikannya dengan cara yang efektif. Ketika kelemahan keamanan menyerang jaringan komputer, itu dapat menyebar sepenuhnya dalam sekejap atau waktu yang sangat singkat, Biasanya, karena penyembunyian yang tiba-tiba dan tinggi, pengguna tidak dapat mencari solusi yang relevan dan efektif pada waktunya untuk mengontrol dan memperbaiki mereka. Kerentanan keamanan jaringan juga menggunakan fitur ini, meningkatkan ruang lingkup pengaruh, mengakibatkan dampak kualitas keamanan seluruh jaringan, mempengaruhi penggunaan normal orang, dan bahkan mempengaruhi urutan keamanan keseluruhan masyarakat [5].

Pengguna komputer sangat menyadari bahwa kenyamanan penggunaan komputer dalam kehidupan kita

sehari-hari adalah hal yang paling dasar, karena funginya seperti otomatisasi, kedirgantaraan, kedokteran dan kesehatan, penelitian ilmiah, investigasi kriminal dan sebagainya, komputer memiliki peran penting yang tidak tergantikan. Terdapat banyak informasi dalam industri yang sifatnya sangat rahasia, karena ini informasi tidak dapat dipahami oleh orang yang tidak relevan, jika tidak maka akan menyebabkan kerugian yang tidak dapat diperbaiki. Tepatnya karena tingginya rahasia informasi komputer sehingga beberapa orang yang berniat jahat memiliki ide untuk melakukan kejahatan dan selalu berharap untuk mendapatkan beberapa manfaat dari kerentanan keamanan jaringan komputer. Jaringan komputer teknologi keamanan terus berkembang, dan teknologi kriminal dari para penjahat ini juga terus menerus berkembang.[6]

Bahkan beberapa teknologi kriminal lebih tinggi dari level ahli komputer, sehingga jaringan keamanan tidak bisa dijamin. Karena bukti dalam proses kejahatan komputer sulit untuk dipahami, komputer kejahatan keamanan jaringan semakin sering terjadi. Ada hal penting yang perlu dilakukan yaitu melakukan pekerjaan dengan baik dalam pencegahan keamanan jaringan komputer, untuk meminimalkan kemungkinan terjadinya kejahatan computer.[6]

Keamanan jaringan komputer melibatkan empat hubungan yang berbeda, yaitu potensi hubungan dengan empat aspek utama ketika menggambarkan bentuk-bentuk ancaman terhadap keamanan jaringan komputer. Ada empat bentuk utama ancaman terhadap keamanan jaringan komputer: penyalahgunaan informasi Internet of Things, penolakan layanan serangan latar belakang, kerusakan pada integritas lingkungan jaringan komputer, dan kebocoran informasi komputer. Pertama Kesalahan Informasi Internet of Things, Biasanya, dalam proses menggunakan komputer, banyak pengguna lebih tenang saat mengklik situs web dan mengunduh gambar, file, dan sebagainya, dan tidak akan digunakan setelah pemakaian. Hal ini akan menyebabkan bahaya besar yang tersembunyi pada keamanan jaringan komputer, karena setiap situs web, file, tautan dan sebagainya sangat mungkin mengandung virus atau ada file yang disembunyikan serta hal lainnya yan berbahaya, jika tidak ada aplikasi untuk menyaring virus atau file yang tersembunyi, maka dapat menyebabkan kebocoran informasi atau infeksi terhadap komputer. Kedua serangan pada layanan latar belakang, serangan latar belakang berupa ada banyak faktor yang mengancam keamanan jaringan komputer, yang dapat dibagi menjadi faktor subyektif dan faktor obyektif. Untuk menggambarkan faktor-faktor yang mengancam keamanan jaringan komputer agar lebih komprehensif [6].

Serangan jaringan dapat dibagi menjadi dua kategori: serangan aktif dan serangan pasif. Serangan aktif adalah serangan jaringan yang diprakarsai oleh penyerang, biasanya dengan bantuan alat serangan profesional. Serangan aktif termasuk merusak informasi, memalsukan pesan, dan penolakan layanan. Serangan pasif adalah metode serangan di mana penyerang mencegat atau menguping informasi objek target tanpa persetujuan dan persetujuan pengguna. Penyerang tidak secara aktif mengubah informasi dari objek target. Serangan pasif terutama mencakup penyadapan, analisis lalu lintas, dan peretasan aliran data [7]

Deteksi ancaman adalah solusi keamanan prioritas yang harus diintegrasikan bahkan di platform keamanan utama. Ini dirancang untuk mendeteksi dan mencegah aktivitas jahat di jaringan. Idenya adalah untuk mendeteksi ancaman sebelum dieksploitasi sebagai serangan, mendapatkan akses tidak sah ke sistem internal, dan menyebabkan kerusakan. Ini memainkan peran penting dalam keamanan dunia maya, terutama dalam konteks Big data. Ini memungkinkan melindungi kerahasiaan, integritas, dan ketersediaan Big data dari serangan malware tingkat lanjut dan persisten di lingkungan jaringan [8].

Perangkat router mikrotik pada manajemen jaringan tidak tau bahwa ada bahaya yang akan muncul bagi pemakai hotspot, disebabkan oleh konfigurasi standar pada layanan hotspot dan ARP. Ini menjadi sebuah permasalahan bagi pihak penyedia layanan hospot karena dalam pengaturan jaringan hospot memakai router mikrotik [9].

Terdapat beberapa metode dalam mengamankan jaringan komputer dari adanya serangan. Salah satunya adalah IPS, sistem ini selain mendeteksi adanya serangan juga dapat melakukan pencegahan secara aktif. Berbeda dengan Intrusion Detection System (IDS) yang hanya mampu mendeteksi adanya serangan tanpa

bisa melakukan pencegahan [10]

Portabel IPS yang telah dilakukan instalasi dan konfigurasi kemudian akan dilakukan pengujian menggunakan topologi seperti yang ditunjukan pada dibawah ini

Gambar 1. Skema Jaringan

Pada Gambar tampak skema jaringan untuk melakukan pengujian portabel IPS. Perangkat portabel IPS terhubung melalui Wireless Router dengan Service Set Identifier (SSID) berupa "admin" menggunakan interface wlan0 dengan mode client. Host 1 dan 2 merupakan perangkat yang ingin dilindungi dari adanya serangan, dapat berupa laptop dan smartphone. Perangkat tersebut terhubung secara tidak langsung ke WiFi publik, akan tetapi melalui portabel IPS yang dikonfigurasi sebagai Access Point mode dengan menggunakan interface uap0. SSID yang digunakan adalah "AP-IPS" dengan frekuensi mengikuti frekuensi yang ada pada wireless router. Catu daya portabel IPS diperoleh dari power bank dengan tegangan output 5 volt, arus 1 ampere, sedangkan kapasitasnya 10.000 mAh. Pengujian serangan ke client dilakukan menggunakan komputer Attacker yang sudah terinstall aplikasi Zenmap. Perangkat portabel IPS terdiri dari dua komponen utama yaitu Raspberry Pi 4 Model B dan power bank.

Wireless router dikonfigurasi sebagai Dynamic Host Configuration Protocol (DHCP) server dengan network 192.168.100.0/24. Alokasi alamat IP yang akan diberikan kepada client mulai dari 192.168.100.2 sampai 192.168.100.254. Default gateway dan Domain Name System (DNS) server adalah 192.168.100.1. Berdasarkan Gambar 2, maka Attacker dan portabel IPS akan memperoleh alamat IP dari wireless router tersebut, sehingga konfigurasi alamat Internet Protocol (IP) pada interface wlan0 portabel IPS dan laptop Attacker dikonfigurasi secara dynamic.

System juga dijadikan sebagai router dengan menggunakan network 192.168.4.0/24. Virtual interface uap0 dijadikan sebagai Access Point dengan "AP-IPS" sebagai SSIDnya, frekuensi yang digunakan mengikuti frekuensi yang diterima oleh wlan0. Alokasi alamat IP setiap perangkat.

Serangan berupa port scanning dilakukan menggunakan aplikasi Zenmap. Skenario serangan dilaksanakan melalui mekanisme penyerangan terhadap portabel IPS dan client. Alamat IP Attacker mempunyai alamat IP jaringan yang sama dengan portabel IPS. Rule yang digunakan pada pengujian ini adalah Emerging Scan Rule.

Kesimpulan

Penggunaan multiple filter pada IPS membuatnya secara signifikan lebih efektif ketika menginspeksi, mengidentifikasi dan memblokir serangan berdasarkan urutan waktu. IPS membuat filter baru ketika sebuah metode serangan baru diidentifikasi. Mesin inspeksi paket data IPS normalnya terdiri dari integrated circuit yang didesain untuk inspeksi data mendalam. Setiap serangan yang mencoba mengeksploitasi kelemahan dari layer 2 sampai layer 7 OSI akan difilter oleh mesin IPS yang mana, secara tradisional, kemampuan firewall hanya terbatas sampai modul 3 atau 4 saja. Teknologi packet-filter dari firewall tradisional tidak menerapkan inspeksi untuk setiap byte dari segmen data yang bermakna tidak semua serangan dapat diidentifikasikan

olehnya. Secara kontras, IPS mampu melakukan inspeksi tersebut dan semua paket data diklasifikasikan dan dikirim ke filter yang sesuai menurut informasi header yang ditemukan di segmen data, seperti alamat asal, alamat tujuan, port, data field dan sebagainya. Setiap filter bertanggung jawab untuk menganalisis paketpaket yang berkaitan, dan yang mengandung tanda-tanda membahayakan akan didrop dan jika dinyatakan tidak berbahaya akan dibiarkan lewat. Paket yang belum jelas akan diinspeksi lebih lanjut. Untuk setiap tipe serangan berbeda, IPS membutuhkan sebuah filter yang bersesuaian dengan aturan filtering yang sudah ditentukan sebelumnya. Aturan-aturan ini mempunyai definisi luas untuk tujuan akurasi, atau memastikan bahwa sebisa mungkin jangkauan aktifitas yang luas dapat terenkapsulasi di dalam sebuah definisi. Ketika mengklasifikasikan sebuah aliran data, mesin filter akan mengacu pada informasi segmen paket, menganalisa konteks dari field tertentu dengan tujuan untuk mengimprovisasi akurasi dari proses filtering.

Daftar Rujukan

[1] M. I. Triwahyudi and I. Veritawati, "Sistem Informasi Pelayanan Jaringan Komputer," *Format J. Ilm. Tek. Inform.*, vol. 11, no. 1, p. 55, 2022, doi: 10.22441/10.22441/format.2022.v11.i1.006.

[2] B. Wijaya and A. Pratama, "Deteksi Penyusupan Pada Server Menggunakan Metode Intrusion Detection System (Ids) Berbasis Snort," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 9, no. 1, pp. 97–101, 2020, doi: 10.32736/sisfokom.v9i1.770.

[3] J. Suomalainen, J. Julku, A. Heikkinen, S. J. Rantala, and A. Yastrebova, "Security-driven prioritization for tactical mobile networks," *J. Inf. Secur. Appl.*, vol. 67, no. May, p. 103198, 2022, doi: 10.1016/j.jisa.2022.103198.

[4] N. Miloslavskaya *et al.*, "ScienceDirect ScienceDirect 2022 Annual International Conference on Brain- Inspired Cognitive Architectures for Security Architecture of Network Security Centers Security Architecture of Network Security Centers as Part of Modern Intranets as Part of Moder," *Procedia Comput. Sci.*, vol. 213, pp. 58–63, 2022, doi: 10.1016/j.procs.2022.11.038.

[5] J. Sun, "Computer Network Security Technology and Prevention Strategy Analysis," *Procedia Comput. Sci.*, vol. 208, pp. 570–576, 2022, doi: 10.1016/j.procs.2022.10.079.

[6] Z. Munawar, M. Kom, and N. I. Putri, "Keamanan Jaringan Komputer Pada Era Big Data," *J. Sist. Informasi- J-SIKA*, vol. 02, pp. 14–20, 2020.

[7] G. Dong, F. Liu, and G. Wu, "A Website's Network Attack Analysis and Security Countermeasures," *Procedia Comput. Sci.*, vol. 208, pp. 577–582, 2022, doi: 10.1016/j.procs.2022.10.080.

[8] I. El Alaoui and Y. Gahi, "Network security strategies in big data context," *Procedia Comput. Sci.*, vol. 175, pp. 730–736, 2020, doi: 10.1016/j.procs.2020.07.108.

[9] R. N. Dasmen, A. R. Syarif, H. Saputra, and R. Amrullah, "Perancangan Keamanan Internet Jaringan Hotspot Mikrotik pada Winbox dan Wireshark," *DoubleClick J. Comput. Inf. Technol.*, vol. 5, no. 2, p. 71, 2022, doi: 10.25273/doubleclick.v5i2.11751.

[10] Y. Ardiyanto, "Portabel Intrusion Prevention System Untuk Mengamankan Koneksi Internet Saat Menggunakan WiFi Publik," *J. Sisfokom (Sistem Inf. dan Komputer)*, vol. 11, no. 1, pp. 107–113, 2022, doi: 10.32736/sisfokom.v11i1.1223.

[11] Budiman, S. A., Iswahyudi, C., & Sholeh, M. (2014). IMPLEMENTASI INTRUSION DETECTION SYSTEM (IDS) PADA SERVER DEBIAN. *Jurnal JARKOM* Vol. 2 No. 1 ISSN:2338-6313, 36-40. [2]

[12] Homenta, J. I., & Efendi, R. (2015). MENGANALISA SISTEM KEAMANAN JARINGAN BERBASIS INTRUSION PREVENTION SYSTEM DAN HONEYPOT SEBAGAI PENDETEKSI DAN PENCEGAH MALWARE. *Jurnal Teknologi Informasi dan Komunikasi*, 1-8. [3]

[13] Wiyanto, P., Hamzah, A., & Sholeh, M. (2014). APLIKASI MONITORING KEAMANAN JARINGAN DENGAN MENGGUNAKAN IDS DAN. *Jurnal JARKOM* Vol. 2 No. 1 ISSN:2338-6313, 89-91. [4]

[14] Gunawan, Indra. "Penggunaan Brute Force Attack Dalam Penerapannya Pada Crypt8 Dan CSA-Rainbow Tool Untuk Mencari BISS." InfoTekJar*: Jurnal Nasional Informatika dan Teknologi Jaringan* 1.1 (2016): 52-55. [5]

[15] Rahmatullah, Tansah. "Perlindungan Hukum Terhadap Privacy Dari Spamming Berdasarkan Undang-Undang No. 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik." *Jurnal Hukum Media Justitia Nusantara* 4.2 (2019).