Teknika 19 (1): 249-259

JURNAL TEKNIKA
ISSN: 0854-3143
e-ISSN: 2622-3481
Journal homepage: http://jurnal.polsri.ac.id/index.php/teknika
Journal Email: teknika@polsri.ac.id

Strategi Penguatan Keamanan Jaringan dengan IDS dan IPS di PT. Toppan Plasindo Lestari Cibitung

Taufik Rahman*[1], Ilham Rozen[2]

[*1,2] Program Studi Teknologi Informasi, Universitas Bina Sarana Informatika, Jakarta, Indonesia
*Email Penulis Korespondensi: taufik@bsi.ac.id

Abstrak

IDS (Intrusion Detection System) dan IPS (Intrusion Prevention System) merupakan teknologi keamanan jaringan yang esensial. IDS memantau lalu lintas jaringan dan aktivitas mencurigakan, IPS mengintegrasikan fungsi firewall dan IDS untuk menolak serangan yang teridentifikasi. Penelitian ini berfokus pada strategi penguatan keamanan jaringan di PT. Toppan Plasindo Lestari Cibitung melalui implementasi sistem Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS). Masalah utama yang dihadapi adalah meningkatnya ancaman siber, seperti malware dan serangan DDoS, serta keterbatasan sistem keamanan tradisional dalam mendeteksi dan mencegah serangan secara efektif. Tujuan penelitian adalah merancang dan mengimplementasikan IDS dan IPS meningkatkan kemampuan deteksi dini dan pencegahan serangan. Metode pendekatan deskriptif dengan pengujian implementasi IDS dan IPS pada infrastruktur jaringan perusahaan, serta analisis kinerja sistem dalam menangani berbagai jenis ancaman. Pengujian menunjukkan komputer dengan Snort terinstal memberikan peringatan seperti deteksi aktivitas ping, percobaan koneksi server SSH, dan FTP. Hasil deteksi ini kemudian dicegah menggunakan iptables, memastikan penyusup tidak melakukan aktivitas yang ditentukan dalam aturan Snort. Hasil penelitian menunjukkan penggunaan IDS dan IPS secara signifikan meningkatkan deteksi dan pencegahan ancaman, mengurangi risiko serangan siber yang berdampak pada operasional perusahaan. Implementasi berhasil terintegrasi dengan infrastruktur tanpa mengganggu kinerja jaringan, memberikan perlindungan yang lebih komprehensif terhadap ancaman siber.

Kata kunci*—Keamanan Jaringan, IDS, IPS, Ancaman Siber, Deteksi Dini*

Abstract

IDS (Intrusion Detection System) and IPS (Intrusion Prevention System) are essential network security technologies. IDS combines network traffic and suspicious activities, IPS integrates firewall and IDS functions to reject identified attacks. This study focuses on network security strengthening strategies at PT. Toppan Plasindo Lestari Cibitung through the implementation of the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). The main problems faced are the increasing cyber threats, such as malware and DDoS attacks, as well as the limitations of traditional security systems in detecting and preventing attacks effectively. The purpose of the study is to design and implement IDS and IPS to improve early detection and prevention capabilities. The descriptive approach method with testing the

Online Available: November 21, 2024

implementation of IDS and IPS on the company's network infrastructure, as well as analyzing system performance in handling various types of threats. Tests show that computers with Snort installed provide warnings such as ping activity detection, SSH server connection attempts, and FTP. The results of this discovery are then prevented using iptables, ensuring that intruders do not carry out activities specified in the Snort rules. The results of the study show that the use of IDS and IPS significantly improves threat detection and prevention, reducing the risk of cyber attacks that impact company operations. The implementation is successfully integrated with the infrastructure without disrupting network performance, providing more comprehensive protection against cyber threats.

Keywords—*Network Security, IDS, IPS, Cyber Threats, Early Detection*

1. PENDAHULUAN

Teknologi informasi (TI) ini telah berkembang pesat, terutama karena hadirnya jaringan *online* yang dapat memudahkan komunikasi dengan pihak lain. Saat ini, *internet* telah menjadi salah satu bagian terpenting dalam kehidupan dan gaya hidup masyarakat di seluruh dunia [1]. Karena *internet* telah menjangkau semua aspek kehidupan, mulai dari dunia hiburan, dunia pendidikan, penunjang pekerjaan dan lain-lain, maka ketika informasi tersebut mudah didapat maka muncullah permasalahan baru yaitu pihak-pihak yang tidak bertanggung jawab dapat mengambil manfaat semata. Oleh karena itu sistem keamanan jaringan menjadi aspek yang penting [2].

Administrator Network dan *Administrator System* terkadang memiliki tanggung jawab atas keamanan sistem, yang menjamin perlindungan sistem dan jaringan yang dikelola terhadap berbagai potensi ancaman [3]. Perusahaan merupakan tempat di mana penggunaan internet terbuka bagi penggunanya. Hal ini disebabkan oleh semakin banyaknya data dan informasi yang disimpan secara digital, baik di komputer pribadi, *server*, maupun *cloud* [4]. Data dan informasi ini dapat menjadi target serangan bagi para pelaku kejahatan siber, yang dapat menyebabkan kerugian finansial, reputasi, dan bahkan operasional bisnis [5].

PT. Toppan Plasindo Lestari Divisi Cibitung merupakan perusahaan yang bergerak di bidang manufaktur dan percetakan. Dalam menjalankan operasinya, perusahaan ini sangat bergantung pada jaringan komputer untuk mengelola data dan komunikasi. Keamanan jaringan kini menjadi semakin penting dalam konteks bisnis dan industri karena meningkatnya kompleksitas serangan *cyber* dan dampak negatif yang dapat dihasilkan [6]. Mereka juga beresiko terkena serangan yang mengancam keamanan jaringan [7]. Oleh karena itu, sebagai bagian dari usaha untuk menjaga keamanan dan integritas infrastruktur IT mereka, PT. Toppan Plasindo Lestari Divisi Cibitung perlunya menyadari untuk mengadopsi solusi keamanan jaringan yang canggih dan proaktif.

Dengan pertumbuhan teknologi informasi yang pesat dan peningkatan ketergantungan pada sistem jaringan, resiko serangan *cyber* juga mengalami peningkatan yang signifikan [8]. Ancaman-ancaman seperti peretasan data, pencurian informasi, perangkat lunak berbahaya, dan serangan DDoS (*Distributed Denial of Service*) dapat menyebabkan gangguan operasional, kebocoran data sensitif, dan dampak finansial yang serius bagi perusahaan [9]. Karena itu, perlindungan terhadap jaringan menjadi prioritas utama bagi PT. Toppan Plasindo Lestari Divisi Cibitung.

Snort adalah IDS *open source* yang umum digunakan untuk memantau dan mendeteksi intrusi, serta dapat ditingkatkan menjadi IPS dengan mode inline menggunakan DAQ untuk menganalisis paket data. Hasil deteksi disimpan sebagai alert. Dalam penelitian ini, Snort dikonfigurasi sebagai IPS dengan DAQ AFPACKET di Linux Ubuntu karena kemudahannya dan fleksibilitas pengembangannya [10].

Sistem informasi rumah sakit, melalui SIMRS, penting untuk pelayanan dan pengelolaan data mutu. Keamanan jaringan internet sangat penting, namun seringkali tidak sebanding dengan kemajuan teknologi. Penelitian ini menggunakan *Snort* untuk mengamankan jaringan dengan IDS

dan IPS, menghasilkan akurasi deteksi 99,97% dan waktu respon *server* yang optimal (1 *client*: 0,50 detik; 2 client: 0,32 detik) [11].

MStore-API dikategorikan sebagai *critical* dengan risiko kebocoran data, yang menunjukkan urgensi penerapan mekanisme keamanan secara cepat. Meskipun *Brute Force* juga termasuk dalam kategori *OWASP* yang sama dan digolongkan sebagai medium, perhatian utama harus diberikan pada kerentanan *critical* terlebih dahulu [12].

Penerapan *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) krusial untuk keamanan jaringan. Penelitian ini menguji efektivitas IDS dan IPS dalam mendeteksi dan mencegah serangan *TCP Port Scanning* serta *ICMP Flooding*, memberikan notifikasi *real-time* melalui Telegram. Hasilnya menunjukkan IDS mendeteksi aktivitas mencurigakan dengan akurasi tinggi, sedangkan IPS efektif memblokir serangan, sehingga meningkatkan keamanan jaringan [13].

Untuk menghadapi tantangan tersebut, implementasi sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) telah dianggap sebagai solusi yang efektif [14]. IDS akan membantu dalam mendeteksi aktivitas mencurigakan atau serangan terhadap jaringan, sementara IPS akan bertindak secara proaktif untuk mencegah serangan tersebut mencapai tujuannya [15]. Dengan mengadopsi teknologi IDS dan IPS, PT. Toppan Plasindo Lestari Divisi Cibitung berharap dapat meningkatkan kemampuan mereka untuk mendeteksi, melaporkan, dan merespons dengan cepat terhadap ancaman *cyber* yang mungkin mengancam keamanan jaringan mereka.

Dari permasalahan diatas, peneliti tertarik untuk melakukan penelitian ini yang bertujuan untuk mengimplementasikan IDS dan IPS guna meningkatkan keamanan jaringan PT. Toppan Plasindo Lestari.

2. METODE PENELITIAN

2.1 Spesifikasi Hardware

Server adalah komputer dengan spesifikasi dan kemampuan yang lebih tinggi dibandingkan komputer biasa. Dalam jaringan, server berfungsi untuk mengatur akses ke komputer lain dan mengelola sumber daya jaringan. Perangkat keras yang digunakan sebagai *server* di PT. Toppan dapat dilihat pada Tabel 1.

Tabel 1 *Spesifikasi Hardware*

No	Alat-Alat	Keterangan
1	Model	*Dell PowerEdge R740*
2	*Processor*	*Intel® Xeon® Silver 4208 CPU @ 2.10GHz*
3	Memori	64 GB
4	*Hardisk*	24,5 TB
5	Sistem Operasi (OS)	*Windows Server 2019 Standard*
6	*Switch Manage*	*D-Link DGS-1210-52*
7	*Router*	*RB-1100AHX2*
8	Konektor	*Konektor RJ-45 CAT5*

2.2 Spesifikasi Software

Adapun perangkat lunak (*software*) yang digunakan dalam membangun sistem keamanan jaringan IDS *snort* pada Tabel 2.

Tabel 2 *Spesifikasi Software*

No	Keterangan
1	*Linux Ubuntu 15.10*
2	*Snort*

3	*IPtable*
4	*Windows* (Penyerang)
5	*Barnyard*
6	*Apache Web Server*
7	*Database MySQL Server*

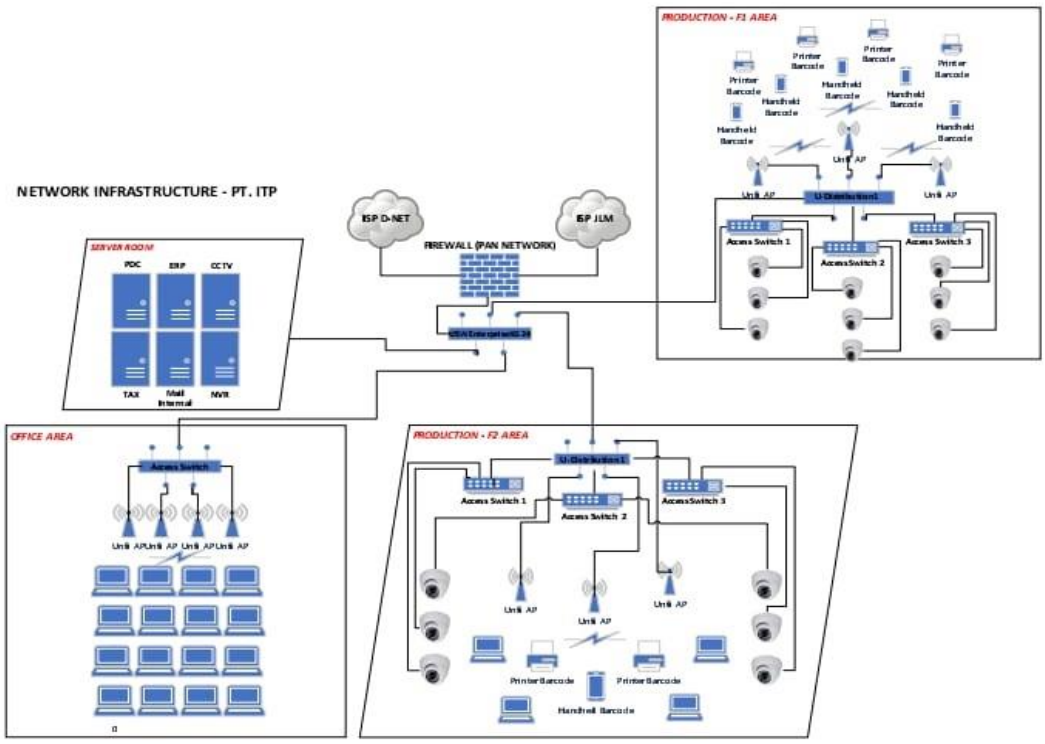
2.3 Pengumpulan Data

Penelitian ini mengumpulkan data melalui komunikasi dengan PT. Toppan Plasindo Lestari. Tahapan pengumpulan data meliputi:

1. Wawancara: dilakukan untuk mendapatkan data yang dapat menjelaskan atau menjawab masalah penelitian melalui pertanyaan-pertanyaan yang diajukan kepada responden.
2. Pengamatan (Observasi): metode ini melibatkan pencatatan dan pemantauan subjek penelitian tanpa partisipasi aktif dari peneliti. Observasi digunakan untuk mengamati dan memahami kondisi subjek tertentu, dengan fokus pada pengumpulan data atau informasi yang ada di perusahaan.
3. Studi Pustaka: melibatkan penelaahan literatur terkait penelitian, seperti artikel dan jurnal, untuk menjadi referensi dan landasan teori dalam penelitian.

Ringkasnya, data dikumpulkan melalui wawancara, pengamatan pasif, dan studi pustaka untuk memahami dan menjawab masalah penelitian di PT. Toppan Plasindo Lestari.

2.4 Network Topology



Gambar 1 Topologi Jaringan

Strategi pengujian dilakukan pada infrastruktur jaringan terdapat perangkat keras dan perangkat lunak yang digunakan, mengkonfigurasi sistem IDS dan IPS, seperti *Snort*, untuk mendeteksi dan mencegah serangan seperti *TCP Port Scanning* dan *ICMP Flooding*. Selanjutnya, simulasi berbagai serangan dilakukan untuk menguji respons IDS dan IPS, dengan pengumpulan *data log* untuk analisis frekuensi deteksi dan waktu respons. Hasil analisis digunakan untuk mengevaluasi kinerja sistem serta menyusun rekomendasi untuk penguatan keamanan jaringan,

termasuk penyesuaian konfigurasi dan pelatihan staf. Dengan strategi ini, diharapkan dapat diperoleh pemahaman mengenai efektivitas IDS dan IPS dalam melindungi jaringan PT. Toppan Plasindo Lestari dari ancaman siber.

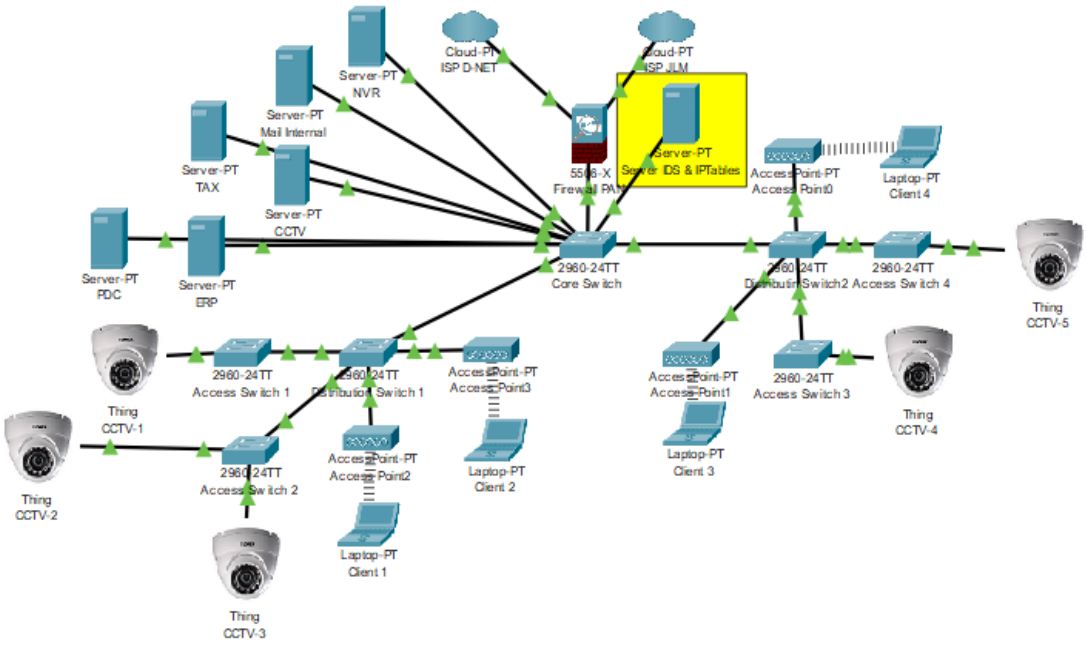
PT. Toppan menerapkan topologi star dalam jaringan komputernya, yang melibatkan beberapa *switch*. Gedung kantor mereka dilengkapi dengan Router Board 1100 AHX2 dan D-link Switch DGS-1210-52, namun belum sepenuhnya membentuk LAN (*Local Area Network*). D-link Switch DGS-1210-52 digunakan untuk mengelompokkan pengguna berdasarkan departemen atau kelompok kerja di setiap lantai. Jaringan LAN, dengan banyak port, menghubungkan berbagai titik atau node dalam jaringan, membentuk topologi star seperti pada Gambar 1.

3. HASIL DAN PEMBAHASAN

Pada bagian ini penulis akan menjelaskan secara rinci mengenai jaringan usulan yang bertujuan meningkatkan keamanan jaringan tanpa merubah topologi jaringan yang sudah ada. Rancangan jaringan usulan ini difokuskan pada penerapan sistem perlindungan jaringan menggunakan sistem pencegahan intrusi dari *snort* dan *Intrusion Prevention System* dari IPTables. Dengan adanya usulan ini, diharapkan mampu memberikan solusi yang efektif dalam menyelesaikan berbagai masalah pada keamanan jaringan yang ada saat ini.

3.1 Skema Jaringan

Berdasarkan penelitian, penulis tidak akan merubah skema jaringan yang sudah ada di Perusahaan tetapi hanya menambahkan perangkat *server* yang akan digunakan untuk server *IDS* dan *IP*S yang berfungsi untuk mendeteksi atau memonitoring jaringan dan mencegah adanya serangan yang tidak bertanggung jawab ke perusahaan dapat dilihat pada Gambar 2.



Gambar 2 Skema Jaringan

3.2 Keamanan Jaringan

Dari segi keamanan jaringan perusahaan, penulis menyarankan untuk menambahkan perangkat PC untuk menjaga keamanan *server* dan jaringan. Salah satu solusi yang disarankan adalah dengan mengimplementasikan sistem operasi IDS dan *IP*S menggunakan aplikasi *Snort* dan *IPTables*. *Snort* dirancang khusus untuk mendeteksi upaya membobol jaringan komputer, dan membantu meningkatkan keamanan sistem jaringan dari DDoS, *Port Scanning*, Akses SSH, Akses FTP dll. *IPTables* dirancang untuk mencegah aktivitas mencurigakan di jaringan komputer.

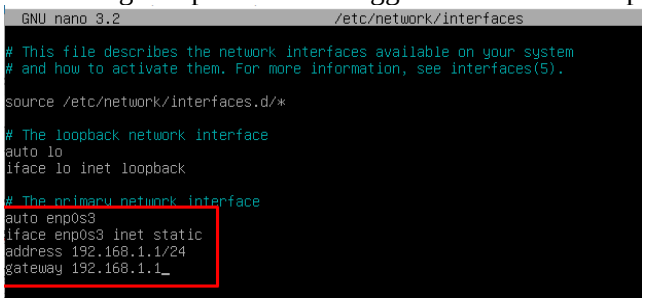
3.3 Rancangan Aplikasi

Dalam perancangan sistem ini penulis melakukan pengujian yang mendeteksi adanya penyusup menggunakan *Intrusion Detection System* dari *Snort* dan mencegah adanya penyusup menggunakan *Intrusion Prevention System* dari *IPTables*. Tools yang digunakan sebagai berikut:

1. *Virtual Box*: Digunakan untuk *server virtual machine*
2. *Debian 10*: OS server yang digunakan untuk instalasi *Snort* dan *IPTables*
3. *Snort*: *Tools Intrusion Detection System* untuk mendeteksi adanya serangan dari penyusup.
4. *IPTables*: *Tools Intrusion Prevention System* untuk mencegah adanya serangan dari penyusup.

Berikut cara instalasi dan konfigurasi *Snort* dan *IPTables* pada Debian 10:

1. Buka terminal lalu perbarui sistem anda dengan mengetik *Sudo su*, digunakan untuk memasuki hak akses root atau *super user*.
2. Ketikkan *apt update&& upgrade* untuk memperbaharui daftar paket yang tersedia pada *repository* dan memperbaharui versi dari aplikasi yang digunakan saat ini jika tersedia pada *repository*.
3. Ketik perintah *nano /etc/network/interfaces* (dilihat pada Gambar 3) untuk mengatur ip jaringan yang digunakan. Jangan lupa dissave menggunakan *ctrl+o* lalu pencet *enter*.

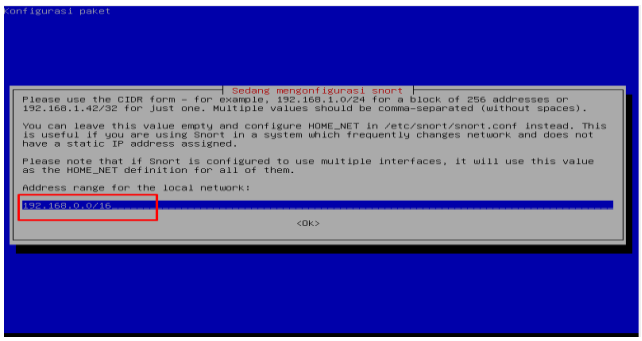


Gambar 3 *Network Interfaces*

Sesuaikan *interface* yang terbaca pada *server* anda. Contoh bisa *eth0*, *eth1* atau *enp0s3 enp0s8* tergantung *interface* yang terbaca pada perangkat (dilihat pada Gambar 4). Bisa dicek menggunakan command *ip a*.

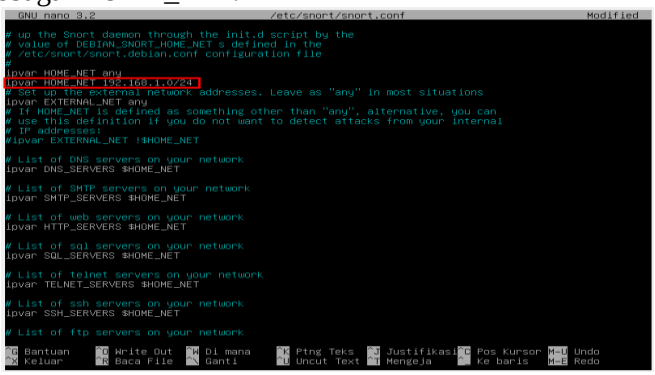
Gambar 4 Cek *Interface*

4. Lalu ketik *apt install snort* (dilihat pada Gambar 5) untuk menginstall *tools snort.*



Gambar 5 *Setting IP Local Snort*

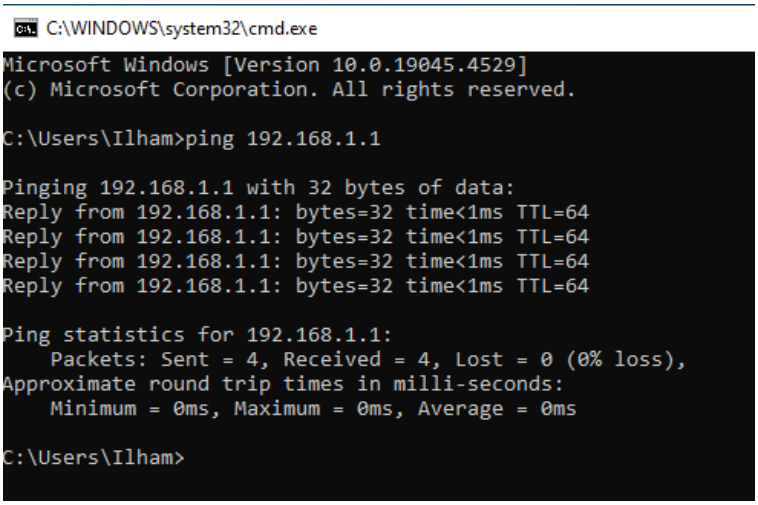
5. Selanjutnya kita akan konfigurasi *intrusion detection system* (dilihat dari Gambar 6) dari *snort*. Ketikkan perintah *nano /etc/snort/snort.conf*, lalu tambahkan *ip local network* kita yang diidentifikasikan sebagai *HOME_NET*.



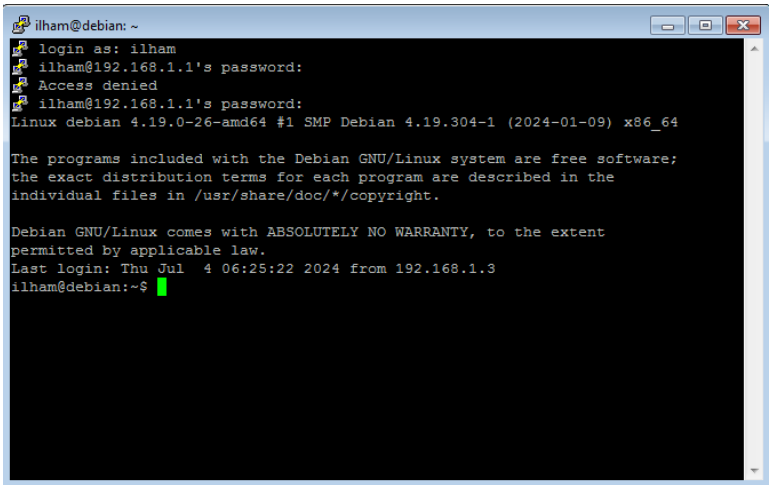
Gambar 6 *Setting Snort.conf*

3.4 Pengujian Jaringan Awal

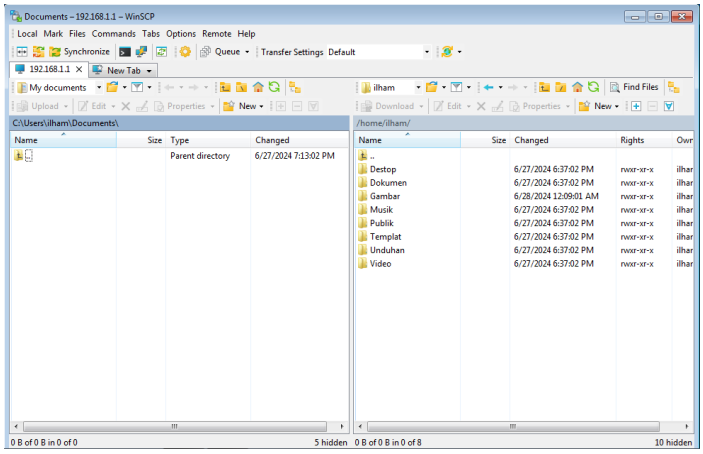
Pada tahap pengujian sebelum di pasang IDS dan IPS kita dapat melihat kerentanan pada jaringan yang dimana orang lain bisa dengan mudah menscan jaringan kita, mencoba me-*remote* server kita, mencoba akses file pada server dan aktivtias berbahaya lainnya. Contoh aktivitas *ping*. *ssh* dan *FTP* dapat dilihat pada Gambar 7, Gambar 8, dan Gambar 9.



Gambar 7 Pengaturan Jaringan Awal



Gambar 8 Aktivitas SSH

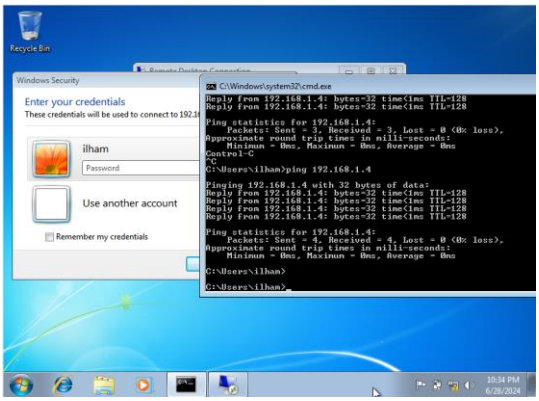


Gambar 9 Aktivitas FTP

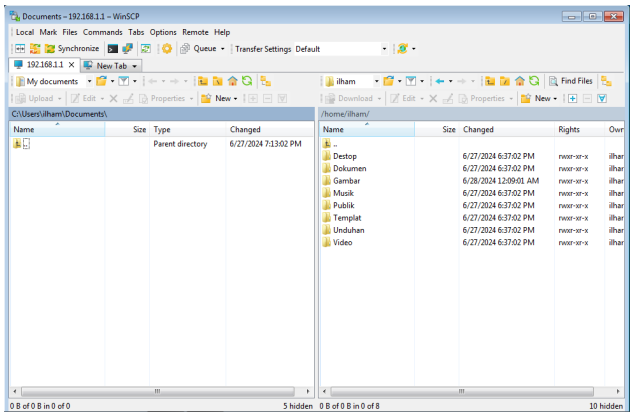
Ketika tidak menerapkan *IDS (Intrusion Detection Systems)* dan *IPS (Intrusion Prevention Systems)* pada jaringan komputer. Kita dapat melihat bahwa penyusup dapat melakukan aktivitas berbahaya tanpa terdeteksi oleh kita yang dimana sebagai contoh diatas penyusup telah melakukan *scanning ip* lalu mencoba akses ke *server* kita berupa SSH dan FTP maupun layanan lainnya Oleh karena itu, penerapan IDS dan IPS sangat diperlukan untuk melindungi keamanan dan integritas jaringan dan sistem informasi.

3.5 Pengaturan Jaringan Akhir

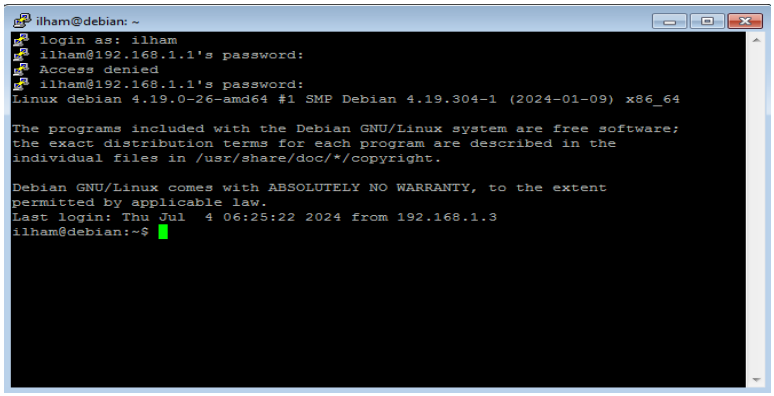
Pada tahap pengujian terakhir ini, komputer sudah dilengkapi dengan sistem *snort* dan iptables yang sudah terpasang. Sistem *snort* dan iptables diuji dengan simulasi serangan untuk pendeteksiannya dapat dilihat pada Gambar 10, Gambar 11, dan Gambar 12.



Gambar 10 *Tes Ping* dan *Remote Desktop*

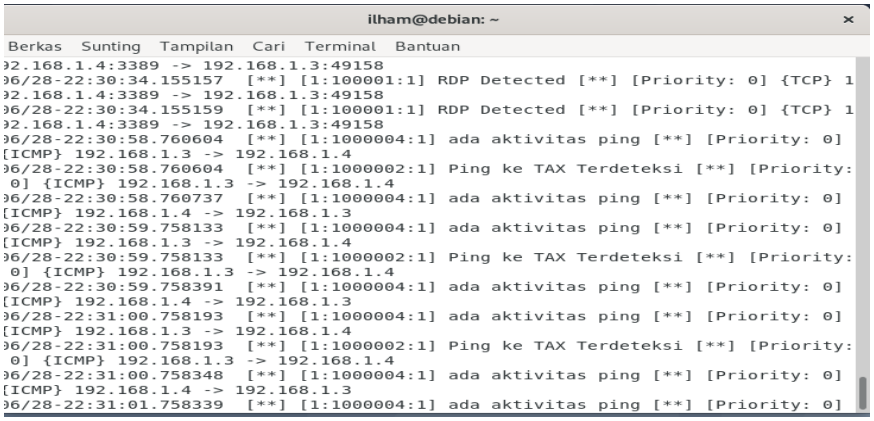


Gambar 11 Akses FTP

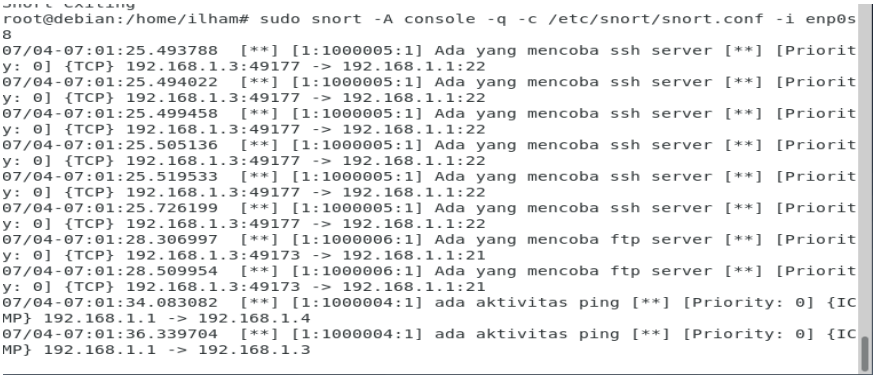


Gambar 12 Akses SSH

Pada pengujian Gambar 12 dilakukan pengujian menggunakan ping pada *command prompt* (CMD) yang dianalogikan sebagai *scanning ip* maupun sebagai aktivitas *DDoS* pada *windows*, aktivitas *remote desktop*. Aktivitas mencoba akses file server menggunakan FTP dan akses *remote server* menggunakan ssh dapat dilihat pada Gambar 13 dan Gambar 14.

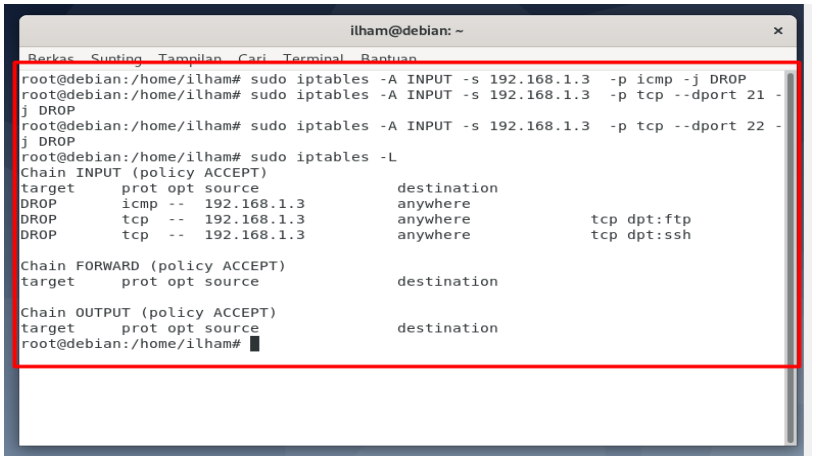


Gambar 13 Hasil Deteksi *Snort*



Gambar 14 Hasil Deteksi FTP SSH

Disini diperoleh *alert* bahwa telah ada aktivitas *ping* ke *tax*, dan RDP yang terdeteksi yang berasal dari ip 192.168.1.3 yang mencoba *ping* ke 192.168.1.4 dan percobaan *remote desktop* ke ip 192.168.1.4 dari sumber ip 192.168.1.3. Adanya aktivitas percobaan akses pada *file server* dari *ftp* dan percobaan akses *remote server* menggunakan *ssh*. Selanjutnya kita coba blokir akses *ping*, akses file *server* dari ftp dan akses *remote* menggunakan ssh dari sumber ip 192.168.1.3 menuju jaringan local, kita menggunakan *iptables* menggunakan perintah, dapat dilihat pada Gambar 15.



Gambar 15 Blok Penyusup *IPTables*

4. KESIMPULAN

Penelitian ini telah berhasil dilakukan dengan efektif. Masalah yang dihadapi termasuk meningkatnya ancaman siber seperti *malware* dan serangan DDoS, serta keterbatasan sistem keamanan tradisional dalam mendeteksi dan mencegah serangan secara efektif. Selama pengujian, IDS dan IPS mampu mendeteksi ancaman seperti serangan *TCP Port Scanning* dan *ICMP Flooding* yang terjadi selama simulasi serangan. Ancaman ini terbukti berbahaya bagi jaringan, karena dapat mengganggu ketersediaan layanan dan mengakibatkan kebocoran data. Dengan menerapkan strategi keamanan yang tepat, jaringan di PT. Toppan Plasindo Lestari dapat bertahan dari serangan ini, berkat kemampuan IDS dalam mendeteksi aktivitas mencurigakan secara *real-time* dan IPS yang efektif dalam memblokir serangan sebelum menyebabkan kerusakan. Implementasi mekanisme keamanan ini memberikan perlindungan yang signifikan terhadap potensi ancaman siber, sehingga meningkatkan integritas dan ketersediaan sistem jaringan perusahaan.

5. SARAN

Penelitian memiliki keterbatasan waktu, untuk menutup keterbatasan waktu penelitian "Strategi Penguatan Keamanan Jaringan dengan IDS dan IPS di PT. Toppan Plasindo Lestari Cibitung," beberapa saran untuk penelitian lebih lanjut adalah menguji serangan siber lainnya, seperti *DDoS*, *ransomware*, atau *phishing*, untuk mengevaluasi efektivitas IDS dan IPS dalam mendeteksi ancaman kompleks. Penelitian selanjutnya juga dapat fokus pada pengoptimalan konfigurasi IDS dan IPS guna meningkatkan akurasi deteksi dan kecepatan respons. Integrasi IDS dan IPS dengan solusi keamanan lain, seperti *firewalls* dan sistem manajemen keamanan informasi, akan menciptakan pendekatan yang lebih holistik. Selain itu, pengujian di berbagai lingkungan jaringan, seperti *cloud* atau jaringan kecil, penting untuk memahami kinerja IDS dan IPS. Terakhir, analisis dampak penggunaan IDS dan IPS terhadap kinerja jaringan akan memastikan mekanisme keamanan tidak mengganggu operasi jaringan. Dengan melaksanakan saran-saran ini, penelitian selanjutnya diharapkan memberikan gambaran lebih komprehensif mengenai efektivitas strategi keamanan jaringan di PT. Toppan Plasindo Lestari dan meningkatkan perlindungan terhadap ancaman siber.

UCAPAN TERIMA KASIH

Kami mengucapkan terima kasih yang sebesar-besarnya kepada PT. Toppan Plasindo Lestari Cibitung atas dukungan dan kesempatan yang diberikan dalam penelitian ini. Kerjasama tim di perusahaan sangat berkontribusi terhadap keberhasilan penelitian mengenai penguatan

keamanan jaringan dengan IDS dan IPS. Semoga hasil penelitian ini bermanfaat bagi pengembangan keamanan jaringan di PT. Toppan Plasindo Lestari dan membantu menghadapi tantangan siber di masa depan.

DAFTAR PUSTAKA

[1] L. M. Silalahi and A. Kurniawan, "Analisis Keamanan Jaringan Menggunakan Intrusion Prevention System (Ips) Dengan Metode Traffic Behavior," *Electr. J. Rekayasa dan Teknol. Elektro*, vol. 17, no. 1, pp. 71–76, 2023, doi: 10.23960/elc.v17n1.2296.

[2] T. Ariyadi, M. Rizky, M. K. Hadi, and A. A. Widodo, "Implementasi Firewall Pada Protokol SSH Linux Ubuntu Menggunakan Iptables," *Semin. Ris. Mahasiswa-Computer Electr. (SERIMA-CE*, vol. 1, no. 1, pp. 170–175, 2023.

[3] U. Sultan Ageng Tirtayasa, "Sistem Keamanan Operasi Linux Ubuntu Iptables Sebagai Firewall Di Dinas Pendidikan Kabupaten Serang," *J. Khatulistiwa Inform.*, vol. 9, no. 1, pp. 17–22, 2021.

[4] Nuroji, "Penerapan Intrusion Detection and Prevention System (IDPS) pada Jaringan komputer sebagai pencegahan serangan Port-Scanning," *J. Data Sci. Inf. Syst.*, vol. 1, no. 2, pp. 41–49, 2023, doi: https://doi.org/10.58602/dimis.v1i2.35.

[5] R. Dody Hidayat, "Mengoptimalkan Pencegahan Serangan Brute Force pada Linux Melalui Penerapan Metode Aplikasi IDS Snort," *J. Ilm. Teknol. Harapan*, vol. 11, no. 2, pp. 57–61, 2023.

[6] A. Irfan, A. Z. Nusri, Z. Rachmat, and S. Wulandari, "Analisis Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System (WIDS)," *J. Ilm. Sist. Inf. dan Tek. Inform.*, vol. 7, no. 1, pp. 110–119, 2024, doi: 10.57093/jisti.v7i1.195.

[7] M. Iqbal *et al.*, "Implementasi Pfsense-Snort Pada Sistem Pencegahan Intrusi," *J. Inform. Softw. dan …*, vol. 4, no. 2, pp. 1–5, 2023.

[8] F. Tanang Anugrah, S. Ikhwan, and J. Gusti A.G, "Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection," *Techné J. Ilm. Elektrotek.*, vol. 21, no. 2, pp. 199–210, 2022, doi: 10.31358/techne.v21i2.320.

[9] D. Santoso, A. Noertjahyana, and J. Andjarwirawan, "Implementasi dan Analisa Snort dan Suricata Sebagai IDS dan IPS Untuk Mencegah Serangan DOS dan DDOS," *J. Infra*, vol. 10, no. 1, pp. 1–6, 2022.

[10] H. Suhendi and W. D. Cahyo, "Perancangan dan Implementasi Keamanan Jaringan Menggunakan Snort sebagai Intrusion Prevention System (IPS) pada Jaringan Internet STEI ITB," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 3, no. 2, pp. 60–68, 2021, [Online]. Available: https://naratif.sttbandung.ac.id/index.php/naratif/article/view/137

[11] W. W. Widiyanto, "SIMRS Network Security Simulation Using Snort IDS and IPS Methods," *Indones. Heal. Inf. Manag. J.*, vol. 10, no. 1, pp. 10–17, 2022, doi: 10.47007/inohim.v10i1.396.

[12] I. Setiawan *et al.*, "Desain Kontrol Keamanan Pada Content Management System Wordpress Berdasar Aspek Aplikasi Dengan Panduan OWASP," *J. Tek. Politek. Negeri Sriwij.*, vol. 19, no. 1, pp. 25–35, 2024.

[13] I. M. Razzanda and M. Koprawi, "Implementasi IDS dan IPS terhadap Serangan TCP Port Scanning dan ICMP Flooding," *Indones. J. Comput. Sci.*, vol. 13, no. 4, pp. 6549–6562, 2024, doi: https://doi.org/10.33022/ijcs.v13i4.4212.

[14] H. Awal, "Implementasi Intrusion Detection Prevention System Sebagai Sistem Keamanan Jaringan Komputer Kejaksaan Negeri Pariaman Menggunkan Snort Dan Iptables Berbasis Linux," *J. Sains Inform. Terap.*, vol. 2, no. 1, pp. 38–44, 2023, doi: 10.62357/jsit.v2i1.184.

[15] Prasetyo Taufan, "Pengamanan Jaringan Komputer Dengan Intrusion PreventionSystem (IPS) Berbasis Sms Gateway," *Teknologipintar.org*, vol. 2, no. 6, pp. 1–13, 2022.