# IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN *TOOLS INTRUSSION PREVENTION SYSTEM* (IPS) DENGAN NOTIFIKASI TELEGRAM PADA PT. AKSES SATU NUSANTARA

**Reza Handono** [1]
Franciscus Asisi Ricky Bayu Styanto, S.Kom., M.Kom [2]
Program Studi Ilmu Komputer,Fakultas Teknologi Informasi, Universitas Respati Indonesia, Jakarta, Jl. Bambu Apus 1 No.3, Bambu Apus, Kec. Cipayung, Kota Jakarta Timur, DKI Jakarta 13890
E-mail : rezahandono4@gmail.com, ricky@urindo.ac.id

**Abstrak**

PT Akses Satu Nusantara, sebuah perusahaan penyedia layanan internet (ISP), menghadapi risiko keamanan data pada komputer-komputernya yang terhubung ke jaringan internet. Dalam usaha mengatasi permasalahan tersebut, penulis melakukan implementasi *Intrusion Prevention System* (IPS). Hasil penelitian menunjukkan bahwa IPS efektif dalam mencegah dan mendeteksi serangan, terutama serangan virus yang dapat merugikan server. Uji coba serangan berhasil ditanggulangi dengan IPS yang secara otomatis memutus koneksi dan menolak paket dari penyerang. Sistem keamanan jaringan yang dibangun dengan IPS terbukti dapat berfungsi dengan baik, memberikan perlindungan yang diperlukan terhadap data yang disimpan oleh PT Akses Satu Nusantara.

Kata kunci : *Keamanan Jaringan, Intrusion Prevention SystemKATA*.

**Abstract**

*PT Akses Satu Nusantara, an internet service provider (ISP) company, faces data security risks on its computers connected to the internet network. In an effort to overcome these problems, the author implemented an Intrusion Prevention System (IPS). The results showed that IPS is effective in preventing and detecting attacks, especially virus attacks that can harm servers. The test attack was successfully remediated with IPS which automatically disconnected and rejected packets from the attacker. Network security systems built with IPS are proven to function properly, providing the necessary protection to data stored by PT Akses Satu Nusantara.*

*Keywords: Network Security, Intrusion Prevention SystemKATA.*

## PENDAHULUAN

Perkembangan teknologi informasi, khususnya dalam jaringan, mengemuka sebagai aspek signifikan. Jaringan internet telah menjadi keberadaan umum di berbagai tempat seperti kantor, sekolah, dan lainnya. Keamanan jaringan komputer menjadi hal krusial untuk melindungi integritas dan validitas data, serta menjamin layanan yang aman bagi pengguna. Sistem keamanan jaringan diperlukan agar dapat mencegah dan menanggulangi serangan penyusup, menjaga agar sistem jaringan tidak terganggu atau rusak akibat virus atau serangan lainnya.

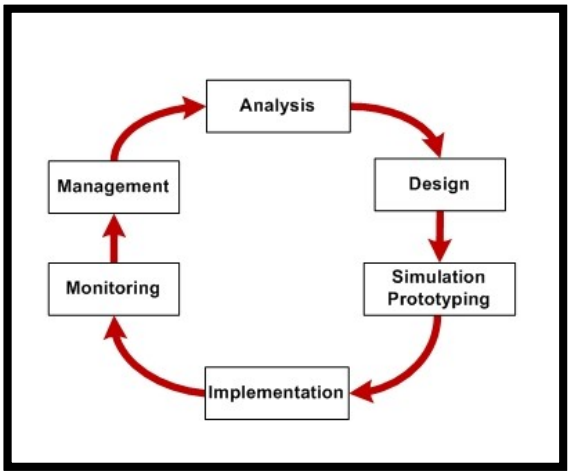
*Intrusion Prevention System* (IPS) unggul dalam pemantauan khusus di suatu host dengan kelebihan menindaklanjuti secara langsung tindakan mencurigakan. Berbeda dengan *Intrusion Detection System* (IDS), yang hanya memantau aktivitas mencurigakan di dalam jaringan tanpa kemampuan langsung mengatasi kejadian tersebut. IPS memberikan keamanan lebih proaktif dan responsif terhadap potensi ancaman daripada IDS.

Sistem keamanan komputer mendapat perhatian utama dalam beberapa tahun terakhir karena tingginya ancaman dan serangan dari internet atau dalam jaringan. Uji coba login seperti *bruteforce* adalah contoh serangan yang memerlukan keamanan jaringan komputer sebagai kunci utama untuk menjaga kualitas dan kemampuan layanan.

PT Akses Satu Nusantara, sebuah ISP dengan banyak komputer terhubung ke internet, sering mengalami kerusakan, kehilangan, atau serangan tidak bertanggung jawab, khususnya melalui *bruteforce* ke perangkat mikrotik. Kondisi ini terjadi 3-4 kali seminggu, mengancam keamanan data yang penting untuk kegiatan pekerjaan perusahaan. Untuk mengatasi masalah ini, diperlukan sistem keamanan jaringan yang mampu melindungi data, memastikan kelancaran operasional, dan menjaga reputasi PT Akses Satu Nusantara sebagai perusahaan yang mampu bersaing di bidangnya.

## METODE

Network Development Life Cycle (NDLC) merancang infrastruktur jaringan dengan fokus pada pemantauan dan analisis kinerja. Metode ini menerapkan prinsip perbaikan berkelanjutan untuk meningkatkan efisiensi jaringan.




Gambar 1. Metode NDLC

### 1. Analisis

Tahap analisis sebagai langkah awal melibatkan evaluasi kebutuhan, permasalahan, keinginan pengguna, dan topologi jaringan saat ini. Metode yang digunakan mencakup wawancara dengan pihak terkait, survei langsung ke PT Akses Satu Nusantara, membaca manual atau blueprint, serta menganalisis data teknis NOC untuk langkah berikutnya.

### 2. Desain

Tahap perancangan bertujuan menetapkan spesifikasi sistem dari hasil analisis, mencakup rancangan topologi jaringan sebagai representasi sistem sebenarnya. Desain melibatkan pembuatan jaringan *virtual private network* untuk aman menghubungkan kantor pusat dan cabang.

### 3. Simulasi

Tahap berikutnya adalah pembuatan prototipe manajemen sebagai simulasi implementasi sistem jaringan. Ini memungkinkan penulis mendapatkan gambaran komprehensif mengenai proses komunikasi, keterhubungan, dan mekanisme kerja seluruh elemen sistem jaringan yang akan dibangun.

### 4. Implementasi

Tahap ini memakan waktu sedikit lama. Dalam melakukan implementasi, penulis telah menerapkan semua perencanaan dan rancangan sebelumnya. Pada tahap ini akan terlihat bagaimana pengembangan yang akan dibangun akan memberikan pengaruh terhadap sistem yang ada.

### 5. Monitoring

Implementasi jaringan memerlukan tahap monitoring menggunakan tools bawaan perangkat atau sistem operasi. Pengujian dilakukan untuk memastikan kecocokan VPN dengan kebutuhan serta menjamin kinerja optimal jaringan yang dibangun.

**6. Management**

Tahap *Management Network Development Life Cycle* melibatkan perawatan, pemeliharaan, dan pengelolaan sistem jaringan untuk menjamin efektivitas interkoneksi. Fokusnya adalah keamanan dan kenyamanan dengan menentukan metode yang sesuai untuk sistem keamanan perusahaan.

## HASIL DAN PEMBAHASAN

Gambaran umum Implementasi Sistem Keamanan Jaringan Menggunakan *Tools Intrusion Prevention System* (IPS) dengan notifikasi Telegram Pada PT. Akses Satu Nusantara adalah sebagai berikut:

### a. Konfigurasi sistem jaringan

konfigurasi sistem jaringan adalah menjelaskan tentang penamaan komponen dan objek jaringan yang akan dibuat, terdiri dari topologi jaringan, spesifikasi teknis hardware dan spesifikasi teknis software yang digunakan.

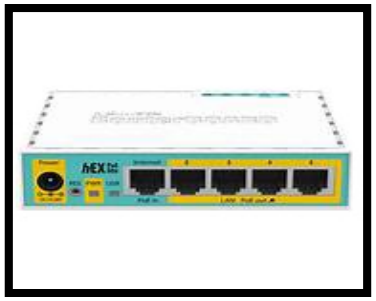
**1. Spesifikasi teknis hardware**

Topologi jaringan yang diusulkan adalah menyediakan sebuah perangkat router mikrotik yang secara free (bebas) untuk diserang oleh attackers, yang dimana attackers kali ini dicontohnya menggunakan tipe serangan bruteforce.

**2. Spesifikasi teknis hardware**

**1. Router mikrotik**

Penulis menggunakan router mikrotik tipe RB951Ui-2nD dalam melakukan implementasi, karena pada saat ini router yang dipakai untuk mengelola jaringan di kantor PT.Akses Satu Nusantara menggunakan router dengan tipe tersebut.

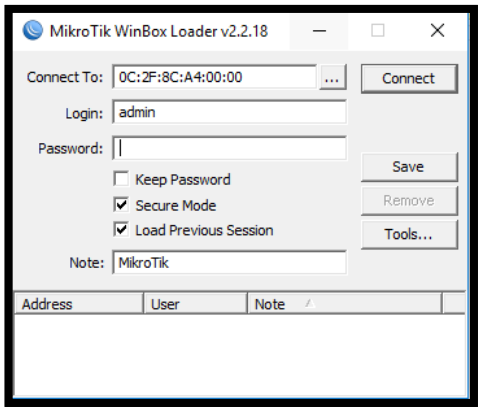


Gambar 2. Mikrotik RB951Ui-2nD

**3. Spesifikasi teknis *software***

**1. Winbox**

Winbox merupakan aplikasi default dari mikrotik untuk melakukan konfigurasi maupun administrasi perangkat mikrotik. Disini penulis menggunakan winbox versi 3.18. Berikut tampilan dari winbox 2.2.18.



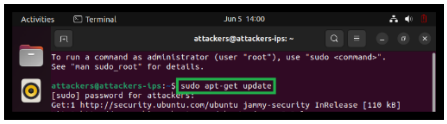

Gambar 3. Halaman login winbox

### b. Pengujian jaringan

**1. Installasi paket ncrack pada Ubuntu**

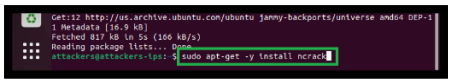
Pada pengujian kali ini, dibutuhkan packet di Ubuntu yang akan digunakan untuk melakukan bruteforce nantinya kepada router mikrotik.

a. Masukan perintah sudo apt-get update.




Gambar 4. Mengupdate ubuntu

b. Masukan perintah sudo apt-get -y install ncrack.

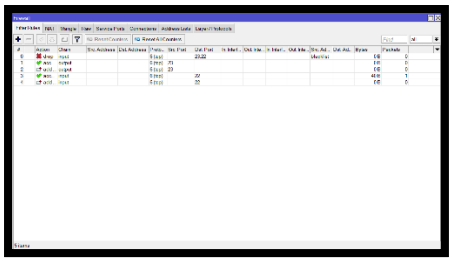



Gambar 5. Menginstall ncrack.

**2. Uji coba bruteforce dari Ubuntu ke Mikrotik**

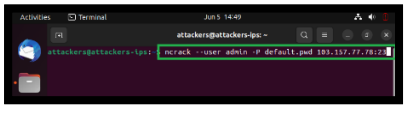
Berikut ini adalah tahap-tahapan untuk melakukan uji coba bruteforce attacks ke mikrotik yang akan menjadi targetnya.

a. Tampilan awal pada mikrotik sebelum diserang oleh bruteforce.



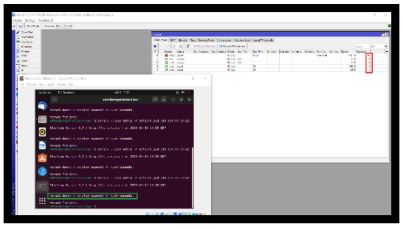
Gambar 6. Tampilan awal mikrotik

b. Client ubuntu server melakukan serangan bruteforce attacks. Selanjutnya untuk melihat apakah hasil konfigurasi ini berhasil, disini penulis langsung melakukan bruteforce dengan ubuntu yang menggunakan perintah ncrack –user admin -P default.pwd 103.157.77.78:22.



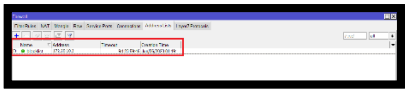

Gambar 7. Melakukan bruteforce ke mikrotik

c. Setelah bruteforce diluncurkan, kita bisa memantau Packets kembali, disana terdapat beberapa packets yang sudah terkirimkan oleh user ubuntu yang telah melakukan bruteforce attacks tadi, sehingga konfigurasi dari Filter Rules yang dibuat dari awal tadi, memproses perannya masing-masing.



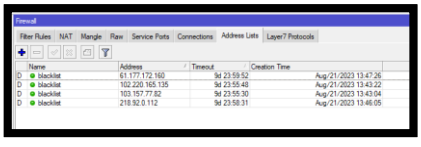
Gambar 8. Bruteforce berhasil diblocking

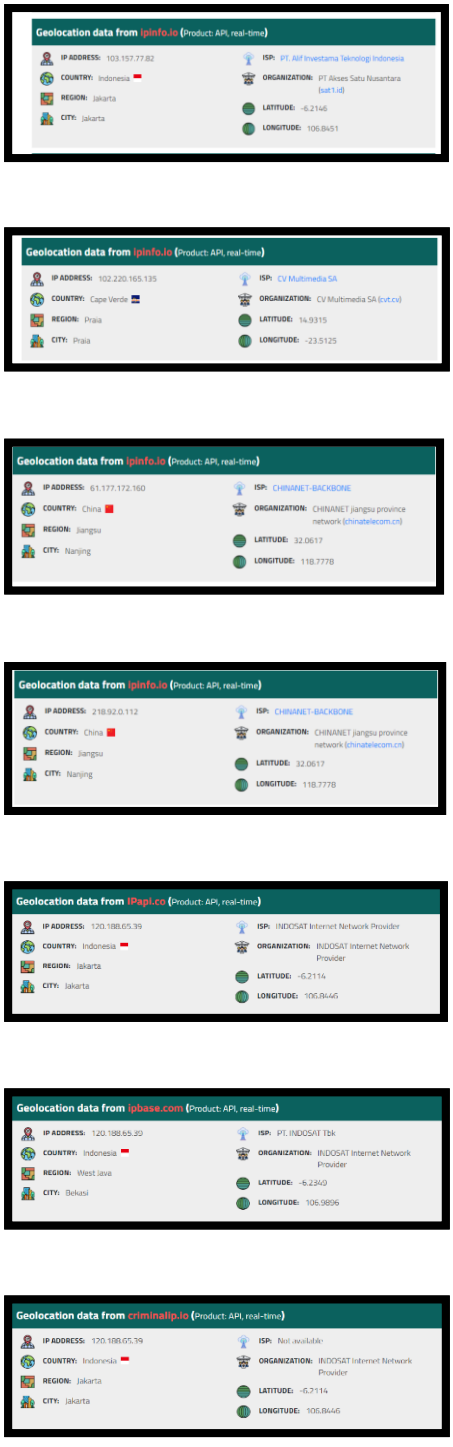
d. Pada menu Address List tadi yang sering penulis katakana sebagai blacklist, adalah tempat dimana user yang melakukan pengiriman file virus berupa bruteforce maupun trojan dll, akan langsung masuk kedalam menu address list ini yang secara otomatis akan terblock/terblacklist selama 10d sesuai dengan yang telah ditetapkan penulis pada saat mengonfigurasikan intrusion prevention system dari awal tadi.



Gambar 9. Hasil Blacklist ip mencurigakan

e. Berikut adalah IP yang terdaftar pada PT Akses Satu Nusantara yang dimana, selain IP yang dilampirkan merupakan IP dari pihak luar, yang berusaha masuk kedalam sistem mikrotik



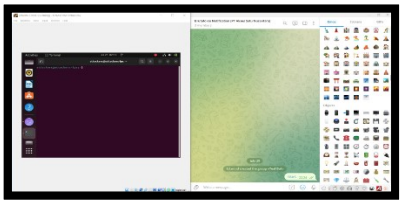



Gambar 10. IP pada PT Akses Satu Nusantara

### 3. Uji coba bot notifikasi di telegram terhadap serangan bruteforce

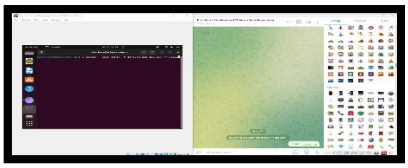
Berikut ini adalah tahap-tahapan untuk melakukan uji coba bot yang akan memberikan notifikasi apabila terjadi serangan bruteforce terhadap mikrotik:

a. Simulasi penyerangan kepada mikrotik dengan menggunakan salah satu software hacker yaitu ncrack pada port ssh 22.



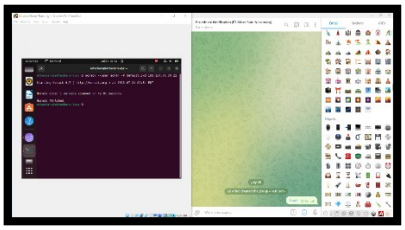
Gambar 11. Membuka terminal ubuntu

b. Selanjutnya mengetikan perintah ncrack --user admin -P default.pwd 103.157.77.78:22 untuk memasuki port 22 ssh.



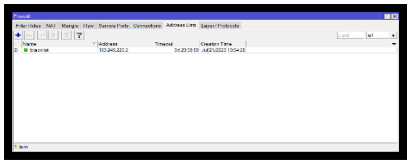
Gambar 12. Tampilan script ncrack

c. Bruteforce adalah metode hacking dengan memasukan username dan password secara random dengan struktur logic yang kompleks sehingga segala kemungkinan password dan username akan bisa ditebak.



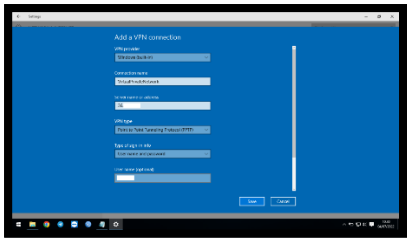
Gambar 13. Melakukan bruteforce

d. Pada menu Addresslist blacklist terdeteksi IP IP yang telah menyerang mikrotik yang tentu IP IP ini akan terblacklist oleh mikrotik, sehingga akan terjadi downtime selama 10hari untuk IP tersebut agar dapat melakukan aksinya kembali.



Gambar 14. Pelaku bruteforce terblockir

e. Kemudian pada group telegram juga sudah muncul notifikasi terhadap serangan yang terjadi, dengan detail alamat IP, mac address serta waktu dilakukan aksi tersebut, dengan demikian dapat disimpulkan jaringan mikrotik sudah aman dari serangan hacking dengan memunculkan notifikasi dari aksi serangan pihak luar.



Gambar 15. Notifikasi via telegram

## SIMPULAN

Penelitian dan uji coba sistem keamanan jaringan di PT Akses Satu Nusantara menunjukkan keberhasilan konfigurasi *intrusion prevention system* (IPS) setelah diimplementasikan. IPS mampu secara efektif mendeteksi dan mencegah berbagai jenis serangan, seperti serangan *Bruteforce FTP, Packet Sniffing, Smurt Attack, dan Denial of Service*. Sistem ini juga berhasil mengintegrasikan notifikasi Telegram, memberikan respons yang cepat terhadap potensi ancaman keamanan. Dengan adanya IPS, perusahaan dapat merespons serangan secara proaktif dan mengurangi dampak serangan terhadap jaringan mereka.

Pentingnya penggunaan *intrusion prevention system* (IPS) dalam penelitian ini terbukti dari kemampuannya untuk dengan mudah mengamankan port-port yang menjadi target serangan. IPS tidak hanya mendeteksi serangan, tetapi juga mencegahnya, meningkatkan lapisan perlindungan jaringan. Hasil penelitian memberikan gambaran bahwa IPS dapat memberikan perlindungan yang efektif terhadap ancaman keamanan jaringan, mengurangi risiko dan kerugian yang dapat ditimbulkan oleh serangan siber. Dengan demikian, implementasi IPS menjadi suatu langkah yang strategis dalam memastikan keamanan dan keberlanjutan operasional jaringan perusahaan seperti PT Akses Satu Nusantara.

Dalam kesimpulannya, rancangan sistem jaringan yang telah dibuat ini dapat membantu PT Akses Satu Nusantara memiliki sistem jaringan yang lebih aman, efisien, dan handal untuk menjalankan kegiatan bisnis mereka dengan lebih baik.

## DAFTAR PUSTAKA


A. Hidayat and I. P. Saputra, 2018, Analisa Dan Problem Solving Keamanan Router Mikrotik Rb750ra Dan Rb750gr3 Dengan Metode Penetration Testing ( Studi Kasus : Warnet Aulia . Net , Tanjung Harapan Lampung Timur ),” vol. 1, no. 2, pp. 118–124.

Hamdi Agustin. 2018. Sistem Informasi Manajemen Menurut Prespektif Islam. Vol. 1. No.1. Universitas Islam Riau. Riau.

Ikhwan Ar-Razy, Rinta Kridalukmana, Eko Didik Widianto. 2016. Implementasi Cloud Storage yang High¬-Availability. Vol.4. No.2. Program Studi Sistem Komputer. Fakultas Teknik. Universitas Diponegoro.

Mulyani, Sri. 2016. Metode Analisis dan Perancangan Sistem. Jilid-2. Abdi Sistematika. Jakarta.

Y. Mulyanto, H. Herfandi, and R. Candra Kirana, 2022, Analisis Keamanan Wireless Local Area Network (Wlan) Terhadap Serangan Brute Force Dengan Metode Penetration Testing (Studi Kasus:Rs H.Lmanambai Abdulkadir), J. Inform. Teknol. dan Sains, vol. 4, no. 1, pp. 26–35, 2022, doi: 10.51401/jinteks.v4i1.1528.

Pernama 2016 Jurnal Teknik Sistem Informasi Dan Bisnis. Pendekatan Kesamaan Semantik Dan Struktur Dalam Kasus Penggunaan Untuk Mendapatkan Kembali Spesifikasi Kebutuhan Perangkat Lunak.

Septiani 2016 Jurnal Edukasi Dan Penelitian Informatika. Investigasi Serangan Malware Njrat Pada PC.

Rijalludin, 2022, Analisis Keamanan Firewall Pada Login Router Mikrotik Dengan Metode Penetration Testing. SMK NEGERI 3 SUMBAWA. Sumbawa.
D. Lagercrantz, 2019, The Girl in The Spider's Web. Qanita. Bandung.

Angga Setyadi. 2017. Implementasi Modul Network MITM Pada Websploit sebagai Monitoring Aktifitas Penggunaan dalam Mengakses Internet. Program Studi Teknik Informatika. Universitas Komputer Indonesia. Bandung, Jawa Barat.

Asika Putri, Fatoni, Imam Solikin. 2017. Analisa Kinerja Koneksi Jaringan Komputer Pada SMK Teknologi Bistek Palembang. Universitas Bina Darma. Palembang.
Winarno, Edy, Zaki, Ali 2013. Membangun Jaringan Komputer di Windows Xp Hingga Windows 8. Jakarta.

Monarfa 2016 Jurnal Teknik Elektro. Analisa dan Implementasi Network Intrusion Prevention System Di Jaringan Universitas Sam Ratunglangi. Ratulangi.

H. D. Sabdho and M. Ulfa, 2018, Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor Pt. Mora Telematika Indonesia Regional Palembang," pp. 15-24, [Online]. Available:https://conference.binadarma.ac.id/index.php/semhavok/article/view/5/4.