



## Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force Menggunakan Intrusion Prevention System pada Mikrotik

| <u>INFO PENULIS</u>   | <u>INFO ARTIKEL</u>  |
|---|--|
| Ansharullah Patiroi Usman<br><a href="mailto:ancharullah@student.unismuh.ac.id">ancharullah@student.unismuh.ac.id</a><br><br>Rizki Yusliana Bakti<br>Universitas Muhammadiyah Makassar<br><br>Muhyiddin Am Hayat<br>Universitas Muhammadiyah Makassar | ISSN: 3026-3603<br>Vol. 2, No. 1 April 2024<br><a href="http://jurnal.ardenjaya.com/index.php/ajst">http://jurnal.ardenjaya.com/index.php/ajst</a> |

© 2024 Arden Jaya Publisher All rights reserved

### *Saran Penulisan Referensi:*

Usman, A. P., Bakti, R. Y., & Hayat, M. A. (2024). Optimalisasi Sistem Keamanan SSH dari Serangan Brute Force Menggunakan Intrusion Prevention System pada Mikrotik. *Arus Jurnal Sains dan Teknologi*, 2 (1), 116-122.

### **Abstrak**

Dalam era digital yang semakin berkembang, keamanan informasi dan jaringan menjadi hal yang sangat penting. Salah satunya komponen kunci dalam infrastruktur jaringan adalah protokol *secure shell* (SSH), yang digunakan untuk mengamankan komunikasi dan akses jarak jauh ke sistem. Meskipun SSH dirancang dengan lapisan yang sangat kuat, serangan *Brute force* tetap menjadi ancaman yang signifikan. Tujuan dari penelitian ini untuk membangun sistem keamanan dari serangan *Brute Force* menggunakan metode *Intrusion Prevention System*. Tujuan utama dari perencanaan sistem ini adalah untuk mengurangi risiko serangan brute force terhadap layanan SSH. Dengan merancang langkah-langkah keamanan yang efektif, seperti pembatasan IP, sistem akan dapat mendeteksi dan mencegah percobaan masuk yang mencurigakan.

Kata kunci: Sistem Keamanan, SSH, *Brute Force*, *Intrusion Prevention System*.

### Abstract

In the increasingly developing digital era, information and network security has become very important. One of the key components in the network infrastructure is the secure shell (SSH) protocol, which is used to secure communications and remote access to the system. Even though SSH is designed with very strong layers, Brute force attacks remain a significant threat. The aim of this research is to build a security system against Brute Force attacks using the Intrusion Prevention System method. The main goal of planning this system is to reduce the risk of brute force attacks against the SSH service. By designing effective security measures, such as IP restrictions, the system will be able to detect and prevent suspicious login attempts.

Keywords: Security system, SSH, Brute Force, Intrusion Prevention System.

### A. Pendahuluan

Dalam era digital yang semakin berkembang, keamanan informasi dan jaringan menjadi hal yang sangat penting. Salah satunya komponen kunci dalam infrastruktur jaringan adalah protokol *secure shell* (SSH), yang digunakan untuk mengamankan komunikasi dan akses jarak jauh ke sistem. Meskipun SSH dirancang dengan lapisan yang sangat kuat, serangan *Brute force* tetap menjadi ancaman yang signifikan.

Serang *Brute Force* pada SSH adalah teknik serangan yang dilakukan dengan mencoba berbagai kombinasi kata sandi secara berulang-ulang hingga sandi yang benar ditemukan. Keberhasilan serangan ini dapat membuka celah keamanan yang mengakibatkan akses yang tidak sah ke sistem, pencurian data, dan bahkan menghancurkan infrastruktur jaringan. Abdussyakur, Yayank Muhammad, Ahmad Zafrullah Mardiansyah, and Andy Hidayat Jatmika. (2021)

Mikrotik, sebagai penyedia solusi jaringan populer, memiliki perangkat keras dan perangkat lunak yang digunakan secara luas dalam berbagai lingkungan. Untuk menghadapi ancaman serangan brute force, pendekatan pencegahan yang efektif perlu diimplementasikan, salah satu solusi yang mungkin menggunakan *intrusion prevention system* (IPS), sebuah teknologi yang dapat mendeteksi dan mencegah serangan siber secara real-time.

Namun, implementasi Intrusion Prevention System untuk mencegah serangan brute force pada perangkat mikrotik memerlukan evaluasi dan optimalisasi yang sangat cermat. Dalam konteks ini, penelitian ini bertujuan untuk menerapkan metode optimalisasi sistem keamanan SSH menggunakan perangkat Mikrotik guna melindungi infrastruktur jaringan dari serangan brute force.

Melalui penelitian ini, diharapkan dapat ditemukan solusi yang efektif dan efisien memberikan kontribusi dalam keamanan sistem jaringan secara keseluruhan.

Protokol *Secure Shell* (SSH) adalah protokol kriptografi yang digunakan untuk mengamankan komunikasi jaringan dan memberikan akses aman ke perangkat jarak jauh. SSH diciptakan sebagai solusi pengganti protokol *Telnet* yang tidak aman, yang mentransmisikan data dalam bentuk teks biasa tanpa enkripsi, sehingga rentan terhadap penyadapan. Tujuan utama dari SSH adalah memberikan akses jarak jauh yang aman ke perangkat atau server melalui jaringan yang tidak aman, seperti Internet. Ini memungkinkan pengguna untuk mengontrol dan mengelola perangkat tanpa harus berada di lokasi fisik perangkat. Salah satu fitur utama SSH adalah enkripsi. Data yang dikirim melalui koneksi SSH dienkripsi sebelum dikirimkan melalui jaringan. Ini berarti bahwa data sensitif seperti kata sandi, perintah, dan informasi lainnya tidak dapat dibaca oleh pihak yang tidak berwenang yang mungkin mencoba menyadap lalu lintas jaringan. Ernawati, Rosalia, Ikhwan Ruslianto, and Syamsul Bahri. (2022).

Serangan *Brute Force* pada *Secure Shell* (SSH) adalah upaya untuk mendapatkan akses tidak sah ke sistem yang dilindungi oleh protokol SSH dengan mencoba kombinasi berbagai kata sandi secara berulang hingga menemukan yang benar. Ini adalah serangan yang umum dilakukan oleh penyerang untuk mengambil alih akun SSH yang lemah atau menggunakan kata

sandi yang mudah ditebak. Serangan Brute Force pada SSH adalah upaya penyerang untuk mendapatkan akses ilegal ke sistem yang menggunakan protokol SSH. Penyerang mencoba banyak kombinasi kata sandi secara berurutan sampai menemukan yang benar. Tujuannya adalah untuk mendapatkan akses ke sistem dengan hak akses dari akun yang berhasil diakses. Rahmadi, Kukuh. (2020).

*Intrusion Prevention System* adalah teknologi keamanan yang dirancang untuk melindungi jaringan dan sistem komputer dari serangan siber. *Intrusion Prevention System* mendeteksi aktivitas yang mencurigakan atau melanggar kebijakan keamanan, lalu mengambil tindakan untuk menghentikan serangan tersebut. Iqbal, Muhammad, Arini- Arini, and Hendra Bayu Suseno. 2020.

Penerapan keamanan pada perangkat MikroTik adalah suatu upaya yang penting dan strategis dalam menghadapi ancaman siber yang semakin kompleks. Perangkat MikroTik sering digunakan untuk mengelola jaringan, dan melindungi perangkat ini dari akses tidak sah dan serangan adalah suatu keharusan. Langkah pertama dalam penerapan keamanan adalah mengubah kata sandi default yang disediakan oleh perangkat. Kata sandi default sering kali diketahui oleh para penyerang, dan mengubahnya menjadi kata sandi yang kuat dan unik dapat mengurangi risiko akses yang tidak sah. Ismanto, and Aristejo. (2021).

## B. Metodologi

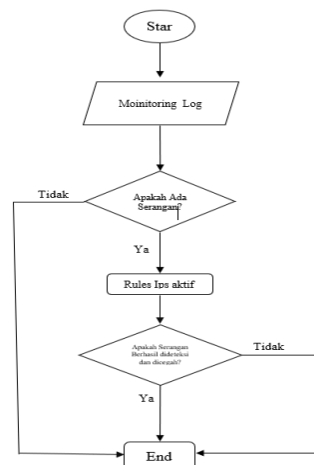
### Perancangan Sistem

Dalam proses pembangunan sistem komputerisasi, salah satu komponen, atau tahapan, adalah perancangan sistem. Untuk pengembangan sistem, biasanya lebih lama dari pemecahan masalah.

Tujuan utama dari perencanaan sistem ini adalah untuk mengurangi risiko serangan brute force terhadap layanan SSH. Dengan merancang langkah-langkah keamanan yang efektif, seperti pembatasan IP, sistem akan dapat mendeteksi dan mencegah percobaan masuk yang mencurigakan sebagai berikut :

#### 2.1.1 Flowchart System

Untuk mengetahui serangan brute force, maka peneliti membuat perancangan sistem dengan menggunakan *Flowchart* seperti gambar dibawah ini.

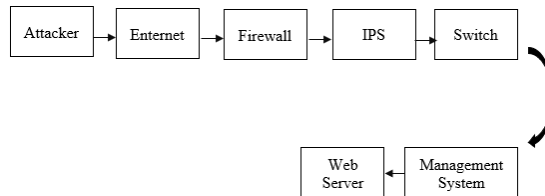


Gambar 1. Flowchart System

Pada flowchart di atas, adapun hal pertama yang harus dilakukan dalam Mendeteksi dan mencegah serangan, lalu hasil Mencegah sistem serangan ini Berbasis *Intrusion Prevention System* pada Mikrotik, kemudian IPS mendeteksi adanya serangan dan melakukan pencegahan dan Pemblokiran pada mikortik.

### Perancangan Blok Intrusion Prevention System

Pada implemetasi jaringan dibawah ini terdapat 2 PC, PC 1 berfungsi sebagai *attacker* dengan system operasi windows 10 ultimate. PC 2 berfungsi sebagai server dengan system operasi Linux ultimate. Terdapat *Firewal* SSH Port 22, *Intrusion Prevention System* untuk pemberitahuan serangan yang terjadi.



Gambar 2. Perancangan Intrusion Prevention System

Dari implementasi diatas dapat dilihat bahwa attacker akan mencoba menyerang ip server yang telah disediakan sebelumnya dengan memasukkan username dan password yang tidak diketahui oleh attacker kemudian server akan merespon serangan yang terjadi dan menyampaikan informasi ke *Intrusion Prevention system*. akan memungkinkan administrator untuk segera merespons ketika terjadi serangan. Sehingga Intrusion system dapat mencegah adanya serangan yang masuk melalui mikrotik. Perancangan sistem pencegahan intrusi (Intrusion Prevention System, IPS) adalah proses merancang sistem keamanan yang bertujuan untuk mendeteksi, mencegah, dan merespons aktivitas yang mencurigakan atau serangan yang terjadi di dalam jaringan atau sistem komputer.

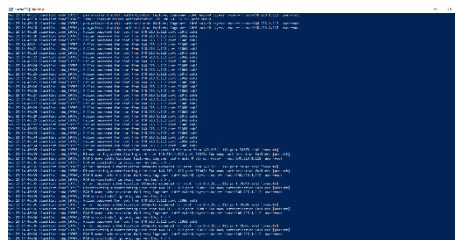
### Pengujian Sistem

Dari implementasi diatas dapat dilihat bahwa attacker akan mencoba menyerang ip server yang telah disediakan sebelumnya dengan memasukkan username dan password yang tidak diketahui oleh attacker kemudian server akan merespon serangan yang terjadi dan menyampaikan informasi ke *Intrusion Prevention system*. akan memungkinkan administrator untuk segera merespons ketika terjadi serangan. Sehingga Intrusion system dapat mencegah adanya serangan yang masuk melalui mikrotik. Perancangan sistem pencegahan intrusi (Intrusion Prevention System, IPS) adalah proses merancang sistem keamanan yang bertujuan untuk mendeteksi, mencegah, dan merespons aktivitas yang mencurigakan atau serangan yang terjadi di dalam jaringan atau sistem komputer.

## C. Hasil dan Pembahasan

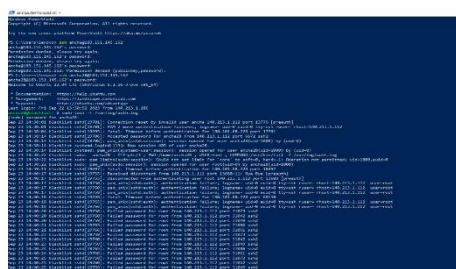
### Monitoring Log Server

Hasil penelitian dan pembahasan pada skripsi ini Selama proses implementasi dan pengujian, sejumlah serangan brute force SSH telah disimulasikan pada layanan SSH yang dijalankan pada perangkat MikroTik. untuk melihat log serangan ketikan perintah “`sudo tail -f var/log/auth.log`”.



Gambar 3. Log Server Linux

File log adalah catatan sistem yang mendokumentasikan berbagai kejadian yang terjadi dalam sistem operasi. Ini mencakup aktivitas pengguna, perubahan konfigurasi, percobaan login, dan kejadian lainnya. Contoh Setiap kali pengguna mencoba masuk (baik berhasil atau gagal), informasi tentang percobaan tersebut dicatat dalam file log.



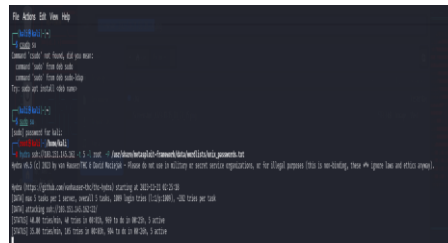
Gambar 4. Monitoring IP Address Login Server

Berfungsi sebagai alat pengawasan keamanan dengan mencatat aktivitas yang mencurigakan atau serangan potensial ke sistem server. Jika terdapat serangkaian percobaan login yang gagal dari alamat IP tertentu, hal ini akan tercatat dalam file log.

Analisis dan *Troubleshooting* File log menjadi sumber informasi vital saat mencari tahu penyebab kegagalan sistem, mencari tahu masalah kinerja, atau mendiagnosis insiden yang terjadi. Ketika sistem mengalami masalah, penggunaan file log dapat membantu mengidentifikasi perubahan atau kejadian yang menyebabkannya. Pentingnya File Log Keamanan Sistem File log autentikasi adalah instrumen kunci dalam mendeteksi serangan, percobaan akses yang tidak sah, atau aktivitas mencurigakan lainnya. Contoh Merekam setiap percobaan login yang gagal dapat membantu mengidentifikasi pola serangan brute force. Kepatuhan dan Audit Dalam bisnis dan lingkungan yang diatur, file log penting untuk memenuhi kepatuhan regulasi dan untuk tujuan audit. Pemeliharaan file log yang tepat diperlukan untuk memenuhi standar keamanan tertentu. Forensik dan Investigasi.

### Pengujian Serangan Brute Force

Melakukan uji coba dilakukan penyerangan pada server dengan memasukan kata perintah `"hydra ssh://103.151.145.162 -t 5 -l root -P /usr/share/metasploitframework/data/wordlists/unix_passwords.txt"` dimana bertujuan untuk menjalankan *dictionary file* yang sudah disiapkan menuju IP Server target tujuan. Dari penyerangan yang dilakukan telah didapatkan hasil sebagai berikut:



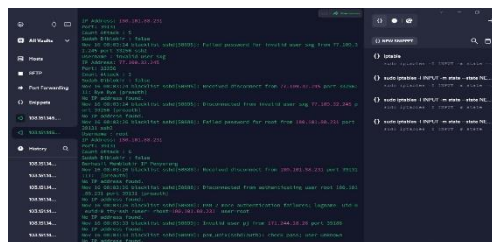
```

root@kali:~# hydra ssh://103.151.145.162 -t 5 -l root -P /usr/share/metasploitframework/data/wordlists/unix_passwords.txt
Hydra (https://bitbucket.org/vanhaacke/hydra) starting at 2025-12-02 07:33
[INFO] max 1 conn per 1 server, max(1) 1 conn, 5000 reqs from (103.151.145.162) [500 reqs per sec]
[INFO] attacking ssh://103.151.145.162:22
[INFO] 14 of 1000000, 4700 per 10000, 99.99% in 1000000, 1.47 sec
[INFO] 14 of 1000000, 4700 per 10000, 99.99% in 1000000, 1.47 sec
[INFO] 14 of 1000000, 4700 per 10000, 99.99% in 1000000, 1.47 sec
  
```

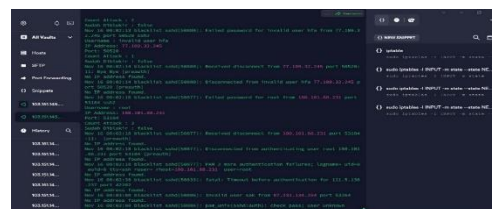
Gambar 5. Uji Coba Serangan Menggunakan Kali Linux

### Pengujian Sistem Intrusion Prevention System Di Server

Serangan berikut ini dilakukan setelah menerapkan sistem *IPS* pada *Server linux*. Dalam penelitian ini dilakukan uji coba penyerangan yaitu serangan *bruteforce*, berikut adalah hasil uji coba dalam penelitian ini :



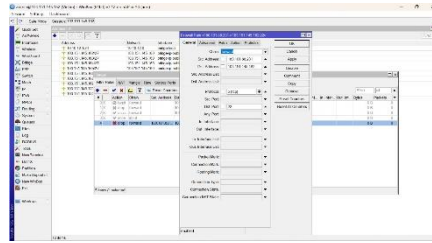
Gambar 7. Pengujian Setelah Menerapkan IPS pada Server



Gambar 8. Intrusion Prevention System Mendeteksi dan Memblokir Serangan

Pencatatan Percobaan Gagal Setiap alamat IP yang terlibat dalam percobaan login yang gagal dicatat dalam objek `currentAttacker`. Objek ini menggunakan alamat IP sebagai kunci dan menyimpan informasi terkait percobaan login yang gagal. Struktur data ini memungkinkan program untuk melacak jumlah percobaan login yang gagal untuk setiap alamat IP yang mencoba masuk.

## Hasil Pengujian Sistem



Gambar 9. Tampilan *address List* Pada *Firewall* Yangg Sudah Di Blokir Pada Mikrotik

Di dalam menu 'Address List', Anda akan melihat daftar alamat yang telah diblokir. Informasi yang ditampilkan biasanya mencakup nama alamat list, alamat IP yang diblokir. Adapun IP yang berhasil dideteksi Oleh sistem Intrusion prevention system.

Berikut IP yang dikenal sebagai sumber potensial serangan. Biasanya, daftar ini diperbarui secara teratur dan berisi alamat IP yang telah terlibat dalam aktivitas jahat sebelumnya.

Tabel 1. Hasil Pengujian Sistem Intrusion Prevention System

| No | IP Sumber       | IP Target       | Port | Jai  | Berhasil Diblokiir | dideteksi dan |
|----|-----------------|-----------------|------|------|--------------------|---------------|
| 1  | 180.101.88.231  | 103.151.145.162 | 22   | sshd | Terblokir          |               |
| 2  | 77.109.32.245   | 103.151.145.162 | 22   | sshd | Terblokir          |               |
| 3  | 192.241.139.149 | 103.151.145.162 | 22   | sshd | Terblokir          |               |
| 4  | 87.231.134.254  | 103.151.145.162 | 22   | sshd | Terblokir          |               |
| 5  | 101.43.6.203    | 103.151.145.162 | 22   | sshd | Terblokir          |               |
| 6  | 171.244.28.26   | 103.151.145.162 | 22   | sshd | Terblokir          |               |

Hasil dari pengujian ini menunjukkan bahwa IPS berhasil mendeteksi serangan dan mengambil tindakan yang sesuai sesuai dengan konfigurasi yang telah ditentukan. Hasil Penelitian menunjukkan bahwa penggunaan Intrusion Prevention System (IPS) pada perangkat MikroTik efektif dalam melindungi layanan SSH dari serangan brute force. Kemampuan IPS untuk mendeteksi serangan dan merespon dengan cepat telah meningkatkan keamanan SSH secara signifikan.

## D. Kesimpulan

Berdasarkan hasil penelitian dan pembahasan yang telah diuraikan dalam penelitian yang Berjudul Simulasi Implementasi *Intrusion Prevention system* Pada Router Mikrotik maka dapat disimpulkan sebagai berikut :

1. Serangan atau penyusupan dapat dicegah dengan menerapkan *Intusion Prevention System(IPS)*.
2. SerErnawati, Rosalia, Ikhwan Ruslianto, and Syamsul Bahri. (2022).angan terdeteksi tergantung pada pola serangan yang ada didalam *ruleIPS* tersebut. Untuk itu pengelolaan *filter rulesp* ada perangkat *IPS* harus secara rutin melakukan pengembangan *rules*.
3. Serangan yang dilakukan dengan software Hydra dalam bentuk *bruteforce* sudah bisa dicegah secara maksimal.
4. Serangan yang dilakukan dengan Hydra pada Kalilinux *windows* 10 dalam bentuk *port scanning* masih belum bisa dicegah secara maksimal karena *IPS* masih membutuhkan
5. beberapa kali serangan untuk bisa mendeteksi serangan dari *ip* yang sama.
6. *Log Server* bekerja dengan maksimal untuk mendeteksi serangan yang terjadi.

## E. Referensi

- Abdussyakur, Y. M., Mardiansyah, A. Z., & Jatmika, A. H. (2021). Optimasi Port Knocking dan Honeypot Menggunakan IPTables Sebagai Keamanan Jaringan pada Server. *Jurnal Teknologi Informasi, Komputer, dan Aplikasinya (JTIKA)*, 3(2), 35-45.
- Arifwidodo, B., Syuhada, Y., & Ikhwan, S. (2021). Analisis Kinerja Mikrotik Terhadap Serangan Brute Force Dan DDoS. *Techno. Com*, 20(3), 392-399.
- Ernawati, R., Ruslianto, I., & Bahri, S. (2022). Implementasi Metode Port Knocking Pada Sistem Keamanan Server Ubuntu Virtual Berbasis Web Monitoring. *Coding Jurnal Komputer dan*

*Aplikasi*, 10(01), 158-169.

- Fachri, F. (2023). Optimasi Keamanan Web Server Terhadap Serangan Brute-Force Menggunakan Penetration Testing. *Jurnal Teknologi Informasi dan Ilmu Komputer*, 10(1), 51-58.
- Iqbal, M., & Suseno, H. B. (2020). Analisa Dan Simulasi Keamanan Jaringan Ubuntu Server Dengan Port Knocking, Honeypot, Iptables, Icmp. *Cyber Security dan Forensik Digital*, 3(1), 27-32.
- Ismanto, I., & Aristejo, A. (2021). Optimalisasi Keamanan Jaringan Menggunakan Metode Port Knocking pada LAZIS Wahdah Jakarta. *Jurnal Teknik Informatika*, 7(1), 40-48..
- Machdi, A. R., Waryani, & Sugeng. (2021). Analisa Dan Implementasi Sistem Kemananan Jaringan Intrusion Detection System (IDS) Berbasis Mikrotik. *JET Jurnal Elektro Teknik* 1(1):1-6.
- Nuryadi, N., & Nainggolan, E. C. (2021). Implementasi Intrusion Detection System Pada Local Area Network (Studi Kasus: Yayasan Pendidikan Tanah Tingal Tangerang). *SITEKIN: Jurnal Sains, Teknologi dan Industri*, 19(1), 1-8.
- Rahmadi, K. (2020). "Program Studi Teknik Informatika Jurusan Teknik Informatika Dan Komputer Politeknik Negeri Jakarta 2020." 1-151.
- Rahmatillah, A., Firdaus, A., & Laila, E. (2021). "Implementasi Intrusion Prevention System (IPS) Pada Keamanan Jaringan Dengan Notifikasi Berbasis Telegram Di Jurusan Teknik Komputer." *Jurnal Laporan Akhir Teknik Komputer*, 1(1):10-17.