Jurnal Teknik Ilmu dan Aplikasi
ISSN: 2460-5549 | E-ISSN: 2797-0272

PEMANFAATAN API CLIENT BERBASIS PYTHON UNTUK KONFIGURASI IPS PADA ROUTER MIKROTIK

Rinanza Zulmy Alhamri[1)], Kunti Eliyen[2)] , Agustono Heriadi[3)]
Politeknik Negeri Malang
Jl. Sokarno Hatta No 1 Kota Malang
[1)]*rinanza.z.alhamri@polinema.ac.id*
[2)]*kunti.eliyen@polinema.ac.id*
[3)]*agustono.heriadi@polinema.ac.id*

Abstrak

Penelitian ini bertujuan untuk bagaimana mengendalikan RouterOS MikroTik sebagai sebuah konfigurasi IPS menggunakanAPI Client berbasis Python. Apakah perintah-perintah jaringan untuk konfigurasi IPS melalui API berbasis Python dapat memiliki kinerja sebaik ketika mengkonfigurasi router MikroTik secara langsung malaui SSH, WinBox, atau bahkan WebFig. Dalam penelitian ini API yang digunakan berbasis Python, secara lebih spesifik lingkungan Python 3. Terdapat tiga fokus serangan meliputi Port Scan, Brute Force, dan serangan Denial of Service (DoS). Manfaat yang diperoleh pada hasil penelitian ini adalah sebagai awal dari penelitian selanjutnya dimana apabila pengendalian API Client berhasil dan kinerja baik maka bisa dikembangkan menjadi aplikasi kendali jaringan yang otonom dimana dengan memanfaatkan teknologi IoT dapat mengakses router MikroTik sebagai IPS kapanpun dan dimanapun. Metode penelitian meliputi Studi Literatur, Persiapan Test Bed, Implementasi, dan Pengujian. Hasilnya telah berhasil dimanfaatkan API Client berbasis Python untuk menerapkan konfigurasi IPS pada router MikroTik dalam bertahan dari serangan Port Scan, Brute Force, dan DoS. Secara fungsional, konfigurasi berhasi diterapkan pada router MikroTik. Sedangkan secara kinerja, router MikroTik mampu bertahan dari skenario serangan. Parameter penting pada konfigurasi IPS untuk Port Scan adalah PSD, Brute Force SSH adalah jumlah filter SSH, Brute Force FTP adalah Destination Limit, dan serangan DoS adalah pengaktifan TCP SynCookies serta penggunaan Firewall Raw.

Kata Kunci: MikroTik, IPS, API, Python

1. PENDAHULUAN

Intrusion Prevention System (IPS) merupakan perangkat pada jaringan yang dikonfigurasi untuk mampu menolak koneksi yang telah dideteksi sebagai serangan. Berbeda dengan Intrusion Detection System (IDS) dimana hanya melakukan deteksi dini terhadap koneksi-koneksi yang mencurigakan tanpa adanya aktivitas konkrit dalam menolak koneksi serangan tersebut, IPS berperan secara langsung untuk menolak koneksi yang telah dideteksi sebagai serangan. IPS merupakan perangkat yang dikonfigurasi untuk mencegah suatu serangan jaringan dengan menolak paket data yang memiliki perilaku anomali serta memberikan peringatan apabila aksi penolakan telah dilakukan [1]. Peringatan dari aksi IPS ini biasanya didokumentasikan pada log sistem.

Router MikroTik dimana menggunakan sistem operasi RouterOS dapat dikonfigurasi sebagai IPS. Dengan melakukan konfigurasi pada aturan-aturan Firewall, router MikroTik dapat berperan sebagai IPS dimana melindungi koneksi sub jaringan yang berada di bawah. Telah banyak penelitian terdahulu yang membahas router MikroTik sebagai IPS seperti blokade koneksi yang dideteksi sebagai aksi Port Scan dan Brute Force, baik Brute Force melalui SSH maupun FTP [2][3]. Router MikroTik sebagai IPS juga mampu menolak koneksi yang terdeteksi sebagai serangan Denial of Service (DoS) baik jenis SYN Flood ataupun Ping Flood [4][5].

Secara umum konfigurasi router MikroTik sebagai IPS dilakukan secara langsung melalui aplikasi WinBox port 8291 pada PC sebagai host client dimana satu jaringan dengan router. Apabila administrator berada di luar jaringan router, akses router bisa dilakukan secara remote melalui koneksi VPN dengan menggunakan aplikasi SSH port 22. Bahkan untuk mendukung kemudahan administrator router, pada RouterOS MikroTik disediakan koneksi melalui Application Programming Interface (API) port 8728 sehingga memungkinkan pengguna sebagai client bisa mengakses router dengan aplikasi buatan sendiri (custom). Telah banyak disediakan API dengan berbagai bahasa pemrograman yang berbeda seperti PHP, Java, Delphi, C#, ataupun Python.

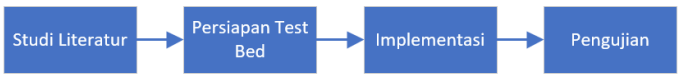
Hal ini menjadi menarik karena dengan tersedianya akses melalui API, pengguna atau client pada router MikroTik dimungkinkan untuk membangun aplikasi yang sesuai dengan kebutuhan. Aplikasi yang dikembangkan bervariasi bisa berbasis web, desktop, atau bahkan berbasis mobile. Tidak hanya itu saja, dengan adanya API membuat akses kendali router MikroTik dimungkinkan bisa dilakukan secara remote memanfaatkan teknologi Internet of Thing (IoT). IoT memungkinkan aplikasi atau sistem dapat melakukan kendali dari jarak jauh melalui internet sehingga tujuan konfigurasi

kemanan pada router bisa dilakukan [6]. Menggunakan konsep IoT, telah banyak penelitian yang mengembangkan aplikasi untuk kebutuhan keamanan jaringan seperti aplikasi Android untuk mengelola bandwidth dan traffic jaringan [7][8], bahkan untuk mengelola jaringan berbasis Software Defined Network [9].

Menjadi fokus pada penelitian ini adalah bagaimana API Client berbasis Python dapat mengendalikan RouterOS MikroTik sebagai sebuah konfigurasi IPS. Apakah perintah-perintah jaringan untuk konfigurasi IPS melalui API berbasis Python dapat memiliki kinerja sebaik ketika mengkonfigurasi router MikroTik secara langsung malaui SSH, WinBox, atau bahkan WebFig port 80. Hal ini perlu dikaji secara detail dikarenakan keberhasilan akses konfigurasi IPS melalui API dapat dikembangkan menjadi aplikasi berbasis IoT untuk tahap penelitian selanjutnya. Dalam penelitian ini API yang digunakan berbasis Python, secara lebih spesifik lingkungan Python 3. Terdapat tiga fokus serangan meliputi Port Scan, Brute Force, dan serangan Denial of Service (DoS) sebagai pengujian keberhasilan konfigurasi. Tujuan dari penelitian ini adalah untuk mengendalikan router MikroTik sebagai IPS melalui API Client berbasis Python serta mengetahui kinerja dari konfigurasi IPS tersebut. Manfaat yang diperoleh pada hasil penelitian ini adalah sebagai awal dari penelitian selanjutnya dimana apabila pengendalian API Client berhasil dan kinerja baik maka bisa dikembangkan menjadi aplikasi kendali jaringan yang otonom dimana dengan memanfaatkan teknologi IoT dapat mengakses router MikroTik sebagai IPS kapanpun dan dimanapun.

2. KAJIAN PUSTAKA

Terdapat empat tahapan dalam melakukan penelitian meliputi Studi Literatur, Persiapan, Implementasi, dan Pengujian seperti pada Gambar 1.



Gambar 1. Metode Penelitian

Detail penjelasan setiap tahapan adalah sebagai berikut.

2.1. Studi Literatur

Pada tahapan Studi Literatur dilakukan analisis mengenai tiga fokus serangan pada penelitian ini meliputi Port Scan, Brute Force, dan DoS. Berdasarkan ketiga serangan tersebut diperoleh bagaimana langkah-langkah konfigurasi IPS pada router MikroTik dimana langkah-langkah konfigurasi berbeda-beda sesuai dengan jenis serangan masing-masing.

a. Port Scan

Serangan Port Scan merupakan serangan jenis pasif dimana merupakan metode untuk memeriksa port layanan berapa saja yang terbuka pada suatu server (target)**.** Langkah konfigurasi IPS untuk menolak koneksi Port Scan pada router MikroTik dilakukan pada fitur Port Scan Detection (PSD). PSD mampu mendeteksi koneksi yang melakukan scan port melalui TCP atau UDP dengan parameter Weight Threshold – total bobot paket datang yang memiliki port tujuan berbeda-beda namun dari sumber koneksi yang sama, Delay Threshold – penundaan paket datang yang memiliki port tujuan berbeda-beda namun dari sumber koneksi yang sama, Low Port Weight – bobot paket datang yang memiliki port tujuan privileged (1-1024), dan High Port Weight – bobot paket datang yang memiliki port tujuan non-privileged. Langkah-langkahnya adalah sebagai berikut [10].

1) Buat aturan pada Firewall untuk drop alamat IP yang telah terdeteksi sebagai Port Scan dengan menentukan Chain Input, Protocol TCP, label yang diambil Source Address List adalah PortScan, Action Drop.
2) Buat aturan Firewall untuk filter koneksi Port Scan yang masuk dengan Chain Input, Protocol TCP, Action Add Src To Address List, Label Address List adalah PortScan, Time Out misal 3 hari.
3) Pada aturan Firewall sebelumnya tentukan Port Scan Detection dengan menentukan nilai Weight Threshold 21, Delay Threshold 3 detik, Low Port Weight 3, dan High Port Weight 1.

b. Brute Force

Brute force merupakan metode serangan aktif yang memaksa masuk suatu hak akses dengan menebak info login, kunci enkripsi, atau mencoba mencari halaman atau data yang tersembunyi dari target secara otomatis dan terus menerus**.** Serangan Brute Force umumnya ada dua jenis meliputi FTP dan SSH. Untuk Brute Force jenis SSH maka konfigurasi IPS-nya berawal dari ide untuk memeriksa koneksi datang dengan paket status New menuju port SSH 22 apakah lebih dari 3 kali dalam interval waktu tertentu, jika benar maka akan dideteksi sebagai Brute Force SSH. Langkah-langkahnya adalah sebagai [11][12].

1) Buat aturan Firewall untuk drop alamat IP yang dideteksi sebagai Brute Force SSH dengan menentukan Chain Input, Protocol TCP, Destination Port 22, Label yang diambil dari Source Address List adalah BruteForceSSH, Action Drop.
2) Buat aturan Firewall untuk filter koneksi SSH ke-4 dengan Chain Input, Protocol TCP, Destination Port 22, Connection State New, Label yang diambil dari Source Address List adalah SSH3, Action Add Src To Address List, Label Address List adalah BruteForceSSH, Time Out 3 hari.

3) Buat aturan Firewall untuk filter koneksi SSH ke-3 dengan Chain Input, Protocol TCP, Destination Port 22, Connection State New, Label yang diambil dari Source Address List adalah SSH2, Action Add Src To Address List, Label Address List adalah SSH3, Time Out 3 hari.
4) Buat aturan Firewall untuk filter koneksi SSH ke-2 dengan Chain Input, Protocol TCP, Destination Port 22, Connection State New, Label yang diambil dari Source Address List adalah SSH1, Action Add Src To Address List, Label Address List adalah SSH2, Time Out 3 hari.
5) Buat aturan Firewall untuk filter koneksi SSH ke-1 dengan Chain Input, Protocol TCP, Destination Port 22, Connection State New, Action Add Src To Address List, Label Address List adalah SSH1, Time Out 3 hari.

Sedangkan konfigurasi penanganan Brute Force FTP adalah dengan melakukan konfigurasi fitur Dst Limit pada koneksi (connection limit). Koneksi akan dideteks sebagai Brute Force FTP, apabila terdapat kegagalan login melebihi batas tertentu. Hal tersebut bisa dilakukan dengan memangfaatkan fitur Dst. Limit dimana mencocokkan paket apakah melebihi nilai batas tertentu. Setiap aliran koneksi diberikan batas jumlah paket gagal loging per interval waktu. Jika melebihi maka koneksi tersebut dideteksi sebagai Brute Force FTP. Parameter nilai batas berdasarkan Rate – jumlah paket per interval waktu, Burst – jumlah paket di awal koneksi yang tidak dihitung, Expire – durasi waktu yang disediakan untuk pemeriksaan koneksi. Langkah-langkahnya adalah sebagai berikut.

1) Buat aturan Firewall untuk drop alamat IP yang dideteksi sebagai Brute Force FTP dengan menentukan Chain Input, Protocol TCP, Dst Port Port 21, Label yang diambil dari Source Address List adalah BruteForceFTP, Action Drop.
2) Buat aturan Firewall untuk filter koneksi FTP keluar dengan Chain Outtput, Protocol TCP, Src Port 21, Content 530 Login incorrect, Action Accept.
3) Pada aturan Firewall sebelumnya tentukan Dst Limit berupa Rate 1 per detik, Burst 4, Expire 60 detik.
4) Buat aturan Firewall untuk filter koneksi FTP keluar dengan Chain Output, Protocol TCP, Src Port 21 Content 530 Login incorrect, Action Add Dst To Address List, Label Address List adalah BruteForceFTP, Time Out misal 3 hari.

c. DoS

Denial-of-Service Attack merupakan serangan yang menyebabkan layanan suatu sistem lumpuh. Layanan sistem lumpuh mengakibatkan penolakan penggunaan layanan, fungsionalitas layanan menurun, bahkan pengguna tidak bisa akses sistem. Cara dalam menolak serangan DoS mirip dengan Brute Force dimana mendeteksi koneksi, apabila koneksi memiliki paket berjumlah melebihi batas dalam interval waktu yang ditentukan, maka bisa dideteksi sebagai DoS. Untuk itu digunakan fitur Dst Limit dalam mendeteksi DoS. Selain itu serangan DoS menyebabkan CPU router lumpuh, sehingga perlu penanganan tersendiri agar serangan CPU tidak membebani CPU. Dimanfaatkan cookies paket SYN dan Firewall Raw agar koneksi yang dideteksi sebagai serangan DoS berada pada kondisi pre-routing sehingga tidak membebani CPU. Pada penelitian ini dipilih DoS jenis SYN Flood dengan langkah penanganan sebagai berikut [13].

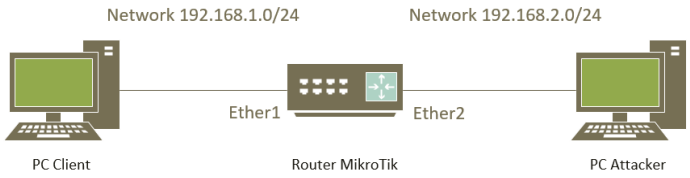
1) Pastikan TCP Syncookies bernilai Yes.
2) Buat aturan Firewall Raw untuk drop alamat IP yang dideteksi sebagai serangan DoS dengan menentukan Chain Prerouting, Protocol TCP, Label yang diambil dari Source Address List adalah DoS, Action Drop.
3) Buat aturan Firewall Raw untuk filter koneksi kondisi prerouting DoS dengan Chain Prerouting, Protocol TCP, Action Add Src To Address List, Label Address List adalah DoS, Time Out misal 3 hari
4) Pada aturan Firewall sebelumnya tentukan Dst Limit berupa Rate 1 per detik, Burst 5, Expire 60 detik.

2.2. Persiapan Test Bed

Test Bed perlu dipersiapkan untuk memungkinan skenario pengujian yang direncanakan bisa dilaksanakan. Berikut ini penjelasan sub tahapan dalam menyediakan test bed sesuai kebutuhan penelitian.

a. Topologi

Dipersiapkan topologi jaringan secara sederhana namun relevan untuk memungkinkan MikroTik API Client berbasis Python bisa diterapkan pada kondisi relevan. Jaringan terdiri dari tiga perangkat yaitu PC Client, Router MikroTik, dan PC Attacker seperti pada Gambar 2.



Gambar 2. Topologi Jaringan pada Test Bed

PC Client berperan untuk mengendalikan Router MikroTik sebagai IPS dimana terpasang API Client berbasis Python melalui interface Ether1 pada jaringan 192.168.1.0/24. Sedangkan PC Attacker berperan untuk menyerang router MikroTik melalui interface Ether2 pada jaringan 192.168.2.0/24. Serangan meliputi Port Scan, Brute Force SSH dan FTP, serta DoS SYN Flood. Router MikroTik berperan sebagai perangkat jaringan IPS yang akan bertahan dari serangan PC Attacker.

b. Hardware

Berikut ini spesifikasi hardware yang digunakan dalam test bed.

1) Spesifikasi minimal PC Client dan PC Penyerang: CPU Intel Dual Core 2.1 GHz, RAM 8GB DDR3, SSD 150GB, Gigabit Ethernet LAN
2) Router MikroTik: Jenis RB951Ui-2HnD license level 4, CPU AR9344 600MHz, NAND 128 MB, RAM 128 MB, Gigabit Ethernet LAN

c. Software

Berikut ini spesifikasi software yang digunakan dalam test bed untuk setiap perangkat keras.

1) PC Client: SO Debian 11 x64, Python3, WinBox x64
2) Router MikroTik: RouterOS versi 6.2
3) PC Attacker: Kali Linux 2022, NMap, Hydra, dan HPing3

2.3. Implementasi

MikroTik API Client berbasis Python telah disediakan terutama pada lingkungan pemrograman Python 3 yang dapat dilihat di https://wiki.mikrotik.com/wiki/Manual:API_Python3. Implementasi kendali router MikroTik sebagai IPS dilakukan pada PC bersistem operasi Debian 11 dengan menggunakan Python3. Berdasarkan test bed yang dirancang PC Client memiliki alamat IP 192.168.1.2/24, router MikroTik memiliki alamat IP 192.168.1.1/24 pada port Ether1 dan 192.168.2.1/24 pada port Ether2, sedangkan PC Attacker memiliki alamat IP 192.168.2.3/24. Langkah-langkah implementasi secara umum adalah sebagai berikut adalah sebagai berikut.

1) Simpan file Python Mikrotik API Client berformat .py. pada PC Client.
2) Eksekusi file Python Mikrotik API Client dan akan terbuka koneksi ke router MikroTik via API port 8728 dengan IP router 192.168.1.1, username admin, password kosong.

```
# ./mikrotikapi.py 192.168.1.1 admin ''
```

3) Masukkan perintah konfigurasi IPS berbasis API untuk serangan Port Scan, Brute Force, dan DoS dari PC Client.
4) Memastikan konfigurasi IPS berhasil di router MikroTik melalui WinBox dari PC Client.
5) Dilanjutkan Tahap Pengujian dengan melakukan skenario serangan melalui PC Attacker.

Berikut ini adalah perintah-perintah melalui API berbasis Python untuk konfigurasi IPS.

a. Perintah API untuk Port Scan

Perintah API untuk drop alamat IP yang telah terdeteksi sebagai Port Scan adalah seperti berkut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=src-address-list=PortScan
=action=drop
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =src-address-list=PortScan
<<< =action=drop
<<<
>>> !done
>>> =ret=*5
```

Gambar 3. Output Perintah API Drop Port Scan

Perintah API filter koneksi Port Scan dan menentukan Port Scan Detection adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=psd=21,3s,3,1
=action=add-src-to-address-list
=address-list=PortScan
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =address-list=PortScan
<<< =psd=21,3s,3,1
<<< =action=add-src-to-address-list
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*6
```

Gambar 4. Output Perintah API Filter Port Scan

b. Perintah API untuk Brute Force

- SSH

Perintah API untuk drop alamat IP yang dideteksi sebagai Brute Force SSH adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=22
=connection-state=new
=src-address-list=BruteForceSSH
=action=drop
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=22
<<< =connection-state=new
<<< =src-address-list=BruteForceSSH
<<< =action=drop
<<<
>>> !done
>>> =ret=*7
```

Gambar 5. Output Perintah API Drop Brute Force SSH

Perintah API untuk filter koneksi SSH ke-4 adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=22
=connection-state=new
=src-address-list=SSH3
=action=add-src-to-address-list
=address-list=BruteForceSSH
```

```
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=22
<<< =connection-state=new
<<< =src-address-list=SSH3
<<< =action=add-src-to-address-list
<<< =address-list=BruteForceSSH
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*8
```

Gambar 6. Output Perintah API Filter SSH ke-4

Perintah API untuk filter koneksi SSH ke-3 adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=22
=connection-state=new
=src-address-list=SSH2
=action=add-src-to-address-list
=address-list=SSH3
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=22
<<< =connection-state=new
<<< =src-address-list=SSH2
<<< =action=add-src-to-address-list
<<< =address-list=SSH3
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*9
```

Gambar 7. Output Perintah API Filter SSH ke-3

Perintah API untuk filter koneksi SSH ke-2 adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=22
=connection-state=new
=src-address-list=SSH1
=action=add-src-to-address-list
=address-list=SSH2
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=22
<<< =connection-state=new
<<< =src-address-list=SSH1
<<< =action=add-src-to-address-list
<<< =address-list=SSH2
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*B
```

Gambar 8. Output Perintah API Filter SSH ke-2

Perintah API untuk filter koneksi SSH ke-1 adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=22
=connection-state=new
=action=add-src-to-address-list
=address-list=SSH1
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=22
<<< =connection-state=new
<<< =action=add-src-to-address-list
<<< =address-list=SSH1
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*C
```

Gambar 9. Output Perintah API Filter SSH ke-1

- FTP

Perintah API untuk drop alamat IP yang dideteksi sebagai Brute Force FTP adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=input
=protocol=tcp
=dst-port=21
=src-address-list=BruteForceFTP
=action=drop
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=input
<<< =protocol=tcp
<<< =dst-port=21
<<< =src-address-list=BruteForceFTP
<<< =action=drop
<<<
>>> !done
>>> =ret=*12
```

Gambar 10. Output Perintah API Drop Brute Force FTP

Perintah API filter koneksi FTP keluar dengan menentukan Dst Limit adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=output
=protocol=tcp
=src-port=21
=content=530 Login incorrect
=dst-limit=1/1s,4,dst-address/60s
=action=accept
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=output
<<< =protocol=tcp
<<< =src-port=21
<<< =content=530 Login incorrect
<<< =dst-limit=1/1s,4,dst-address/60s
<<< =action=accept
<<<
>>> !done
>>> =ret=*13
```

Gambar 11. Output Perintah API Filter FTP Dst Limit

Perintah API untuk filter koneksi FTP keluar adalah sebagai berikut.

```
/ip/firewall/filter/add
=chain=output
=protocol=tcp
=src-port=21
=content=530 Login incorrect
```

```
=action=add-dst-to=address-list
=address-list=BruteForceFTP
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/filter/add
<<< =chain=output
<<< =protocol=tcp
<<< =src-port=21
<<< =content=530 Login incorrect
<<< =action=add-dst-to-address-list
<<< =address-list=BruteForceFTP
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*14
```

Gambar 12. Output Perintah API Filter FTP Keluar

c. Perintah API untuk DoS

Perintah API untuk setting TCP Syncookies bernilai Yes adalah sebagai berikut.

```
/ip/settings/set
=tcp-syncookies=yes
```

Output

```
<<< /ip/settings/set
<<< =tcp-syncookies=yes
<<<
>>> !done
```

Gambar 13. Output Perintah API TCP Syncookies

Perintah API untuk drop alamat IP yang dideteksi sebagai serangan DoS adalah sebagai berikut.

```
/ip/firewall/filter/raw
=chain=prerouting
=protocol=tcp
=src-address-list=DoS
=action=drop
```

Output

```
<<< /ip/firewall/raw/add
<<< =chain=prerouting
<<< =protocol=tcp
<<< =src-address-list=DoS
<<< =action=drop
<<<
>>> !done
>>> =ret=*4
```

Gambar 14. Output Perintah API Drop DoS

Perintah API untuk filter koneksi kondisi prerouting serangan DoS adalah sebagai berikut.

```
/ip/firewall/raw/add
=chain=prerouting
=protocol=tcp
=dst-limit=1/1s,5,dst-address/60s
=action=add-src-to-address-list
=address-list=DoS
=address-list-timeout=3d
```

Output

```
<<< /ip/firewall/raw/add
<<< =chain=prerouting
<<< =protocol=tcp
<<< =dst-limit=1/1s,5,dst-address/60s
<<< =action=add-src-to-address-list
<<< =address-list=DoS
<<< =address-list-timeout=3d
<<<
>>> !done
>>> =ret=*5
```

Gambar 15. Output Perintah API Filter DoS

2.4. Pengujian

Pengujian dilakukan dengan dua tahap meliputi pengujian fungsional dan pengujian kinerja. Pengujian fungsional bertujuan untuk memastikan perintah yang dikirim melalui API Client berbasis Python bisa diaktifkan secara benar pada router MikroTik. Sedangkan pengujian kinerja bertujuan untuk menguji kemampuan konfigurasi IPS dengan cara melakukan skenario serangan.

a. Pengujian Fungsional

Dilakukan dengan validasi turan melalui aplikasi WinBox setiap konfigurasui yang diberikan kepada router MikroTik. Adapun yang perlu divalidasi pada pangujian fungsional dijelaskan pada Tabel 1.

TABEL 1. PENGUJIAN FUNGSIONAL

No	Perintah API	Hasil yang Diharapkan
1	Konfigurasi IPS menolak serangan Port Scan	Muncul daftar aturan Firewall Filter
2	Konfigurasi IPS menolak serangan Brute Force SSH	Muncul daftar aturan Firewall Filter
3	Konfigurasi IPS menolak serangan Brute Force FTP	Muncul daftar aturan Firewall Filter
4	Konfigurasi IPS menolak serangan DoS SYN Flood	- Muncul daftar aturan Firewall Raw - TCP Syncookies aktif

b. Pengujian Kinerja

Dilakukan dengan melakukan serangan langsung pada router MikroTik sebagai target berupa serangan Port Scan, Brut Force SSH dan FTP, serta DoS SYN Flood dari PC Attacker. Adapun skenario serangan yang dilakukan dijelaskan pada Tabel 2.

TABEL 2. PENGUJIAN KINERJA

No	Serangan	Aplikasi	Hasil yang Diharapkan
1	Port Scan	Nmap	- Port Scan timeout - Muncul alamat IP penyerang di Address List Firewall
2	Brute Force SSH	Hydra	- Brute Force timeout - Muncul alamat IP penyerang di Address List Firewall
3	Brute Force FTP	Hydra	- Brute Force timeout - Muncul alamat IP penyerang di Address List Firewall
4	DoS SYN Flood	Hping3	- DoS tidak membebani CPU - DoS timeout - Muncul alamat IP penyerang di Address List Firewall

3. HASIL

Berikut ini adalah penjelasan hasil dari tahap pengujian sesuai skenario yang ditentukan meliputi pengujian fungsional maupun pengujian kinerja.

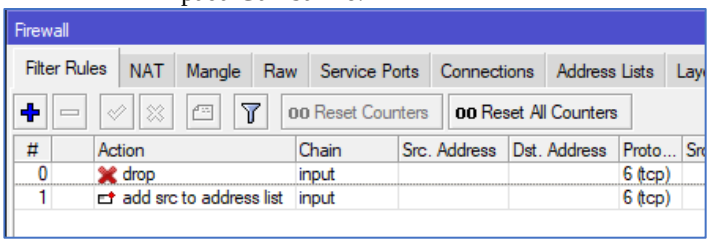
3.1. Hasil Pengujian Fungsional

Penjelasan hasil pengujian fungsional dijabarkan berdasarkan serangan sesuai Tabel 1.

a. Port Scan

Setelah perintah API konfigurasi IPS untuk menolak Port Scan diimplementasikan maka muncul aturan Firewall sebanyak 2 baris aturan

yang diwali dengan aturan tipe action Drop dan tipe action Add Src To Address List seperti pada Gambar 16.

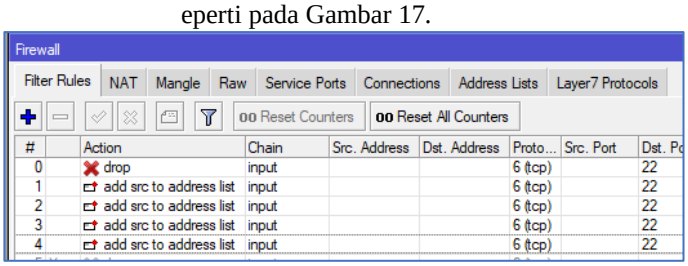


Gambr 16. Hasil Konfigurasi IPS Port Scan

b. Brute Force

- SSH

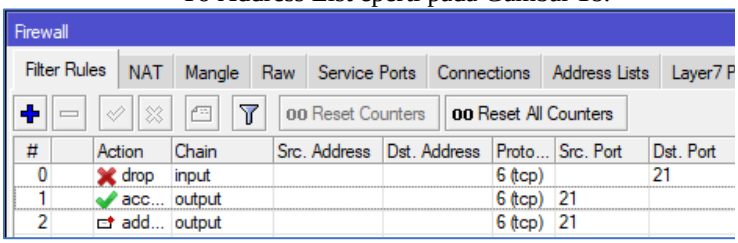
Setelah perintah API konfigurasi IPS untuk menolak Brute Force tipe SSH diimplementasikan maka muncul aturan Firewall sebanyak 5 baris aturan yang diawali dengan aturan tipe action Drop dan 4 baris aturan tipe action Add Src To Address List eperti pada Gambar 17.



Gambar 17. Hasil Konfigurasi IPS Brute Force SSH

- FTP

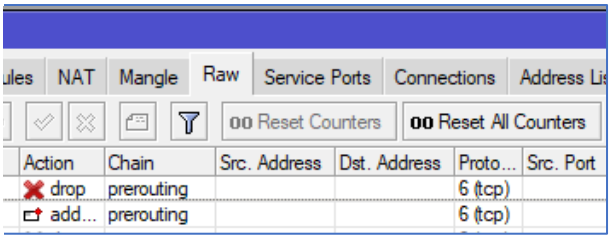
Setelah perintah API konfigurasi IPS untuk menolak Brute Force tipe FTP diimplementasikan maka muncul aturan Firewall sebanyak 3 baris aturan yang diawali dengan aturan tipe action Drop, aturan tipe action Accept, dan aturan tipe action Add Dst To Address List eperti pada Gambar 18.



Gambar 18. Hasil Konfigurasi IPS Brute Force FTP

c. DoS

Setelah perintah API konfigurasi IPS untuk menolak serangan DoS diimplementasikan maka muncul aturan Firewall Raw sebanyak 2 baris aturan yang diawali dengan aturan tipe action Drop dan aturan tipe action Add Src To Address List seperti pada Gambar 19.



Gambar 19. Hasil Konfigurasi IPS DoS

3.2. Hasil Pengujian Kinerja

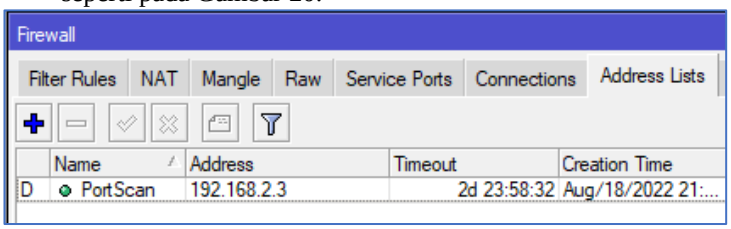
Berikut ini dijelaskan hasil pengujian kinerja berdasarkan Tabel 2.

a. Port Scan

Melalui PC Attacker, menggunakan aplikasi Nmap, serangan Port Scan dilakukan dengan perintah seperti berikut.

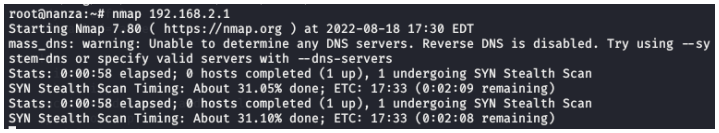
```
# nmap <IP Target>
```

IP Target adalah alamat IP router MikroTik yaitu 192.168.2.1. Kemudian pada Firewall Address List akan muncul alamat IP PC Attacker 192.168.2.3 dengan label PortScan seperti pada Gambar 20.



Gambar 20. Hasil Address List Port Scan

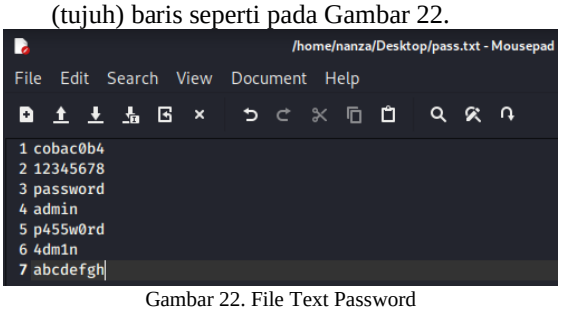
Pada PC Attacker, serangan Port Scan tidak berhasil seperti yang ditampilkan pada Gambar 21.



Gambar 21. Tampilan Serangan Port Scan

b. Brute Force

Untuk serangan Brute Force baik melalui SSH atau FTP, disediakan file berformat txt yang menyimpan karakter password berjumlah 7 (tujuh) baris seperti pada Gambar 22.



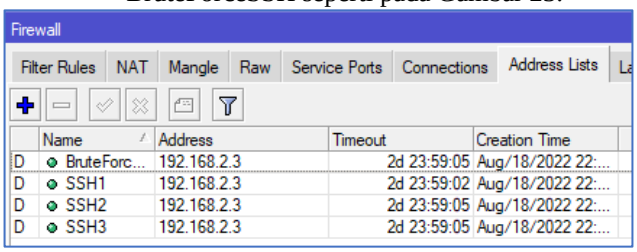
Gambar 22. File Text Password

- SSH

Melalui PC Attacker, menggunakan aplikasi Hydra, serangan Brute Force tipe SSH dilakukan dengan perintah seperti berikut.

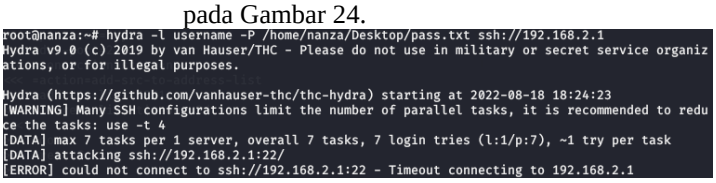
```
# hydra -l <username> -P <path dokumen list password> ssh://<IP Target>
```

Username diisi username target, path dokumen password adalah path direktori kumpulan password, sedangkan IP Target adalah alamat IP router MikroTik yaitu 192.168.2.1. Kemudian pada Firewall Address List akan muncul alamat IP PC Attacker 192.168.2.3 dengan label SSH1, SSH2, SSH3, dan BruteForceSSH seperti pada Gambar 23.



Gambar 23. Hasil Address List Brute Force SSH

Pada PC Attacker, serangan Brute Force tipe SSH tidak berhasil seperti yang ditampilkan pada Gambar 24.



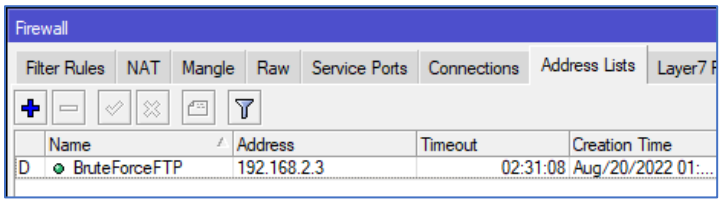
Gambar 24. Tampilan Serangan Brute Force SSH

- FTP

Melalui PC Attacker, menggunakan aplikasi Hydra, serangan Brute Force tipe FTP dilakukan dengan perintah seperti berikut.

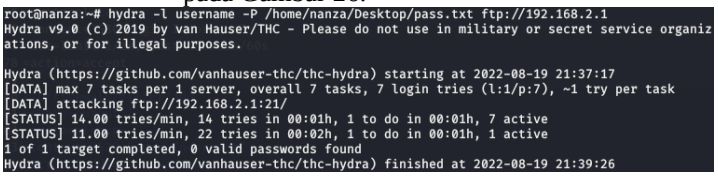
```
# hydra -l <username> -P <path dokumen list password> ftp://<IP Target>
```

Username diisi username target, path dokumen password adalah path direktori kumpulan password, sedangkan IP Target adalah alamat IP router MikroTik yaitu 192.168.2.1. Kemudian pada Firewall Address List akan muncul alamat IP PC Attacker 192.168.2.3 dengan label BruteForceFTP seperti pada Gambar 25.



Gambar 23. Hasil Address List Brute Force FTP

Pada PC Attacker, serangan Brute Force tipe FTP tidak berhasil seperti yang ditampilkan pada Gambar 26.



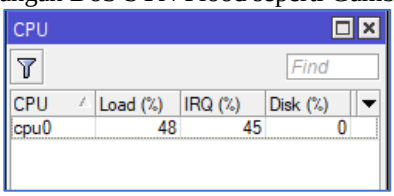
Gambar 26. Tampilan Serangan Brute Force FTP

c. DoS

Melalui PC Attacker, menggunakan aplikasi Hping3, serangan DoS dilakukan dengan perintah seperti berikut.

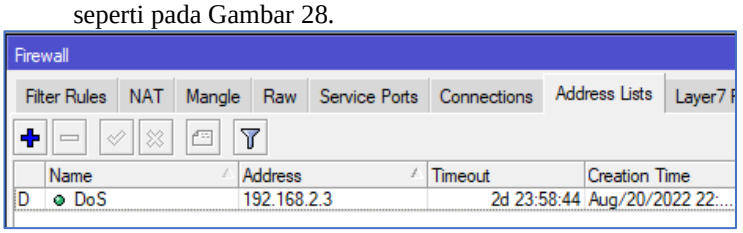
```
# hping3 -i u1 -S -p <port target> <ip target>
```

-S adalah perintah SYN Flood, Port Target adalah nomor port yang akan diserang, dan IP Target adalah alamat IP router MikroTik yaitu 192.168.2.1. Adanya pengaktifan Syn Cookies dan Prerouting, CPU tidak terbebani dengan serangan DoS SYN Flood seperti Gambar 27.



Gambar 27. Hasil Load CPU saat DoS

Load CPU bernilai antara 5% s/d 80% secara fluktuatif, tidak sampai 100%. Kemudian pada Firewall Address List akan muncul alamat IP PC Attacker 192.168.2.3 dengan label DoS seperti pada Gambar 28.



Gambar 28. Hasil Address List DoS

Pada PC Attacker, serangan DoS tidak berhasil seperti yang ditampilkan pada Gambar 29.

Gambar 29. Tampilan Serangan DoS

4. PEMBAHASAN

Pada pembahasan akan dijelaskan detail hasil pengujian serta temuan-temuan penting saat dilakukannya penelitian ini.

4.1. Pembahasan Hasil Pengujian

Pengujian berdasarkan Tabel 1 telah diperoleh hasil bahwa seluruh perintah API berbasis Python dari Client, berhasil diterima dengan baik oleh router MikroTik. Sehingga muncul rule-rule pada Firewall sebagai konfigurasi IPS baik untuk menolak serangan Port Scan, Brute Force, maupun DoS. Tabel 3 merupakan hasil pengujian fungsional yang telah dilakukan.

TABEL 3. HASIL PENGUJIAN FUNGSIONAL

No	Perintah API	Hasil yang Diharapkan	Status

1	Konfigurasi IPS menolak serangan Port Scan	Muncul daftar aturan Firewall Filter	Berhasil
2	Konfigurasi IPS menolak serangan Brute Force SSH	Muncul daftar aturan Firewall Filter	Berhasil
3	Konfigurasi IPS menolak serangan Brute Force FTP	Muncul daftar aturan Firewall Filter	Berhasil
4	Konfigurasi IPS menolak serangan DoS SYN Flood	- Muncul daftar aturan Firewall Raw - TCP Syncookies aktif	- Berhasil - Berhasil

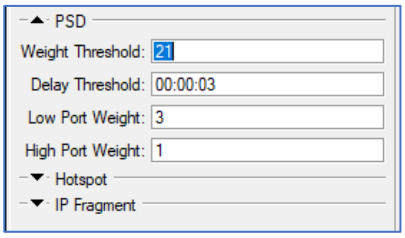
Sedangkan pengujian berdasarkan Tabel 2 telah diperolah hasil bahwa konfigurasi IPS yang ada dalam menolak serangan Port Scan, Brute Force, maupun DoS bisa dilakukan dengan baik. Sehingga PC Attacker tidak dapat melakukan aksinya secara baik karena adanya pengamanan IPS pada router MikroTik. Setiap aksi serangan, alamat IP PC Attacker berhasil dideteksi pada Address List. Tabel 4 merupakan hasil pengujian kinerja yang telah dilakukan.

TABEL 4. HASIL PENGUJIAN KINERJA

No	Serangan	Aplikasi	Hasil yang Diharapkan	Status
1	Port Scan	Nmap	- Port Scan timeout - Muncul alamat IP penyerang di Address List Firewall	- Berhasil - Berhasil
2	Brute Force SSH	Hydra	- Brute Force timeout - Muncul alamat IP penyerang di Address List Firewall	- Berhasil - Berhasil
3	Brute Force FTP	Hydra	- Brute Force timeout - Muncul alamat IP penyerang di Address List Firewall	- Berhasil - Berhasil
4	DoS SYN Flood	Hping3	- DoS tidak membebani CPU - DoS timeout - Muncul alamat IP penyerang di Address List Firewall	- Berhasil - Berhasil - Berhasil

4.2. Konfigurasi IPS untuk Port Scan

Konfigurasi penting untuk bertahan dari serangan Port Scan adalah Port Scan Detection atau PSD. PSD sendiri memiliki empat parameter meliputi Weight Threshold, Delay Threshold, Low Port Weight, dan High Port Weight. Pada penelitian ini, implementasi konfigurasi menggunakan Wight Threshold bernilai 21, Delay Threshold 3 detik, Low Port Weight 3, dan High Port Weight 1 seperti pada Gambar 30.



Gambar 30. Tampilan Konfigurasi Fitur PSD

Nilai Weight Threshold merupakan nilai ambang batas suatu koneksi yang datang dianggap koneksi serangan Port Scan atau tidak. Ketika paket datang, port tujuan dari paket dianalisa selama Delay Threshold, dalam hal ini selama 3 detik. Low Port Weight merupakan penilaian bobot untuk port rendah antara 0 – 1024 dimana bersifat privileged. Port-port rendah banyak digunakan sebagai port default untuk berbagai aplikasi jaringan yang penting seperti SSH, FTP, HTTP, dan sebagainya oleh host / server. Sehingga bobot Low Port Weight ini harus lebih besar dibanding High Port Weight yang artinya paket dengan tujuan port rendah memiliki prioritas perlindungan lebih daripada port tinggi. Dalam hal ini Low Port Weight bernilai 3 sedangkan High Port Weight bernilai 1. MikroTik menggunakan bobot seperti layaknya persentase ambang batas berapa kali dibolehkan hit pada port tujuan tertentu pada satuan waktu analisa.

Nilai pada Weight Threshold dipengaruhi nilai bobot Low Port Weight dan High Port Weight. Total perhitungan port yang dituju (hit) baik pada port rendah maupun port tinggi menghasilkan total bobot yang akan dibandingkan dengan Weight Threshold yang telah ditentukan seperti pada rumus 1.

$$\boldsymbol{Wt = (hLP \times LPW) + (hHP \times HPW)} \quad \textbf{(1)}$$

Keterangan:
Wt = total perhitungan bobot yang akan dibandingkan dengan threshold (Weight Threshold)
hLP = jumlah hit pada port pada port rendah dalam durasi waktu tertentu (Delay Threshold)
LPW = nilai bobot port rendah (Low Port Weight)
hHP = jumlah hit port tinggi dalam durasi waktu tertentu (Delay Threshold)
HPW = nilai bobot port tinggi (High Port Weight)

Dalam penelitian ini, apabila melebihi nilai 21 maka koneksi tersebut akan dideteksi sebagai Port Scan. Misalkan dengan nilai sesuai Gambar 30 dan rumus 1, dalam durasi waktu 3 detik misalkan suatu koneksi terdapat paket hit port rendah berjumlah 7 maka dikalikan bobot port rendah 3 hasilnya 21, ditambah paket hit port atas berjumlah 10 maka dikalikan bobot port tinggi 1 hasilnya 10, sehingga menghasilkan total 21 tambah 10 menjadi 31. Total bobot 31 tentunya melebihi Weight Threshold yang bernilai 21, sehingga koneksi tersebut akan dideteksi sebagai Port Scan. Tentunya semakin rendah nilai Weight Threshold berdampak pada syarat koneksi dengan hit port tujuan harus semakin sedikit.

4.3. Konfigurasi IPS untuk Brute Force

a. Brute Force SSH

Konfigurasi IPS untuk bertahan dari Brute Force SSH pada penelitian ini, terdapat filter SSH berjumlah 4 aturan. Artinya konfigurasi tersebut akan mendeteksi suatu koneksi adalah Brute Force SSH jika koneksi tersebut melakukan akses port SSH selama lebih dari 3 kali terlepas akses SSH tersebut gagal ataupun berhasil secara beruntun. Berdasarkan Gambar 22 bahwa jumlah baris password yang menjadi serangan Brute Force SSH berjumlah 7. Hal ini membuat skenario serangan Brute Force SSH yang dilakukan tidak berhasil,

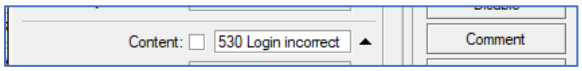
karena mencoba akses SSH lebih dari 3 kali, maka akan dideteksi sebagai Brute Force SSH. Dapat disimpulkan bahwa jumlah aturan filter SSH harus lebih kecil dibandingkan dengan jumlah percobaan Brute Force SSH seperti pada rumus 2.

$$NFr < NBfH \quad (2)$$

Keterangan:
NFr = jumlah aturan filter SSH
NBfH = jumlah percobaan Brute Force SSH
Hal ini membuat adanya kekurangan, apabila konfigurasi IPS Brute Force SSH memiliki jumlah filter SSH lebih besar dari jumlah percobaan Brute Force SSH maka deteksi tidak akan berhasil.

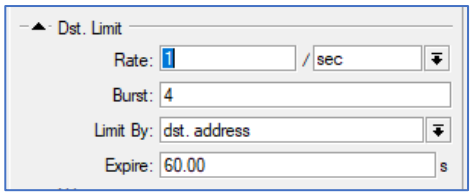
b. Brute Force FTP

Pada konfigurasi IPS untuk bertahan dari serangan Brute Force FTP, content dengan isi ”530 Login incorrect” menjadi penting seperti Gambar 31. Hal tersebut karena bagian content menjadi penanda koneksi bahwa koneksi tersebut gagal untuk login melalui port FTP. Seperti yang telah dijelaskan sebelumnya, ide pertahanan dari Brute Force FTP dilakukan dengan mendeteksi jumlah rate kegagalan login FTP, apabila melebihi rate atau nilai yang ditentukan maka akan dideteksi sebagai Brute Force FTP.



Gambar 31. Tampilan Content 530 Login Incorrect

Jumlah kegagalan login FTP bisa dideteksi melalui fitur Dst. Limit. Parameter Dst. Limit terdiri dari Rate, Burst, dan Expire. Pada penelitian ini, seperti pada Gambar 32, Dst. Limit untuk deteksi Brute Force FTP adalah Rate sebesar 1 paket per detik, Burst sejumlah 4 paket, dan Expire sebagai durasi analisis Dst. Limit bernilai 60 detik.



Gambar 32. Dst. Limit pada Brute Force FTP

Hal tersebut berarti, koneksi akses FTP yang datang akan dianalisis dalam waktu 60 detik, apakah rate paket yang ditentukan dalam interval waktu koneksi tersebut melebihi batas. Dalam penelitian ini, batasannya adalah hanya bisa 1 paket dalam interval satu detik (Rate) dan 4 paket pertama (Burst) tidak dihiraukan. Artinya adalah konfigurasi Dst. Limit membatasi kesalahan login FTP hanya 4 kali, melebihi itu maka akan dideteksi sebagai Brute Force FTP.

Sesuai Gambar 22, terdapat 7 kali percobaan akses FTP, sehingga skenario serangan Brute Force FTP akan dideteksi sebagai Brute Force FTP. Untuk itu, nilai Burst sangat penting untuk membatasi kegagalan login FTP secara beruntun dalam interval waktu tertentu. Sehingga nilai Burst harus lebih kecil dibandingkan dengan percobaan login FTP agar deteksi Brute Force FTP berhasil seperti pada rumus 3.

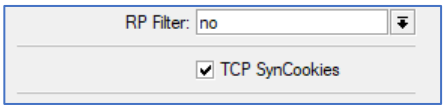
$$Nrb < NBfP \quad (2)$$

Keterangan:
Nrb = nilai Rate dan Burst
NBfP = jumlah percobaan Brute Force FTP

Seperti Brute Force SSH, konfigurasi Brute Force FTP tidak akan berhasil apabila konfigurasi IPS Brute Force FTP memiliki Rate dan Burst lebih besar dari jumlah percobaan Brute Force FTP.

4.4. Konfigurasi IPS untuk DoS

Dalam konfigurasi IPS untuk bertahan dri DoS pengaktifan TCP SynCookies sangat penting karena ebagai tempat untuk menyimpan paket SYN yang berlebih akibat serangan SYN Flooding. Sehingga CPU secara signifikan tidak terbebani akibat menghandle begitu banyaknya paket SYN. Pengaktifan TCP SynCookies seperti pada Gambar 33.



Gambar 33. Pengaktifan TCP SynCookies

Namun demikian tidak bisa dihindari bahwa dengan aktifnya SynCookies sebaiknya diimbangi dengan penambahan resource penyimpanan. Karena apabila terjadi benar SYN Flooding, akan membuat bertambahnya kebutuhan penyimpanan. Apabila penyimpanan untuk Syn Cookies ini juga ikut menipis, maka akan tetap membuat lumpuh router MikroTik.

5. KESIMPULAN

Telah berhasil dimanfaatkan API Client berbasis Python untuk menerapkan konfigurasi IPS pada router MikroTik dalam bertahan dari serangan Port Scan, Brute Force, dan DoS. Secara fungsional, konfigurasi berhasil diterapkan pada router MikroTik. Sedangkan secara kinerja, router MikroTik mampu bertahan dari skenario serangan. Parameter penting pada konfigurasi IPS untuk Port Scan adalah PSD, Brute Force SSH adalah jumlah filter SSH, Brute Force FTP adalah Dst. Limit, dan serangan DoS adalah pengaktifan TCP SynCookies.

6. Daftar Pustaka

[1] F. Wahyudi and L. T. Utomo, "Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang," *EDUMATIC*, vol. 5, no. 1, pp. 60-69, 2021.

[2] Y. Arta, A. Syukur and R. Kharisma, "Simulasi Implementasi Intrusion Prevention System (IPS) pada Router MikroTik," *IT Journal Research and Development*, vol. 3, no. 1, pp. 104-114, 2018.

[3] G. T. Irawan, M. Djaohar and M. F. Duskarnaen, "PERANCANGAN DAN IMPLEMENTASI SISTEM KEAMANAN JARINGAN MENGGUNAKAN FIREWALL DAN WEB PROXY BERBASIS MIKROTIK DI SMA NEGERI 1 KOTA SUKABUMI," *PINTER*, vol. 2, no. 1, pp. 27-32, 2018.

[4] B. Jaya, Y. Yunus and Sumijan, "Peningkatan Keamanan Router Mikrotik Terhadap Serangan Denial of Service (DoS)," *Juranal Sistim Informasi dan Teknologi*, vol. 2, no. 4, pp. 115-123, 2020.

[5] M. Fakhmi and L. M. Gultom, "eningkatan Keamanan Router Mikrotik Terhadap Serangan Syn Flood dengan Menggunakan Firewall Raw," Bengkalis, 2021.

[6] S. Kumar, P. Tiwari and M. Zymbler, "Internet of Things is a revolutionary approach for future technology enhancement: a review," *Journal of Big Data*, vol. 6, no. 111, pp. 1-21, 2019.

[7] M. Risaldi and A. Ayuningtyas, "SIMULASI PENGENDALIAN ROUTER MIKROTIK MENGGUNAKAN ANDROID," *COMPILER*, vol. 7, no. 1, pp. 46-53, 2018.

[8] Y. H. T. Assakur, M. S. Fahrudin and Ferdiansyah, "Implementasi API Mikrotik untuk Management Router Berbasis Android Studi Kasus PT Sigma Adi Perkasa," *Jurnal Sains dan Informatika*, vol. 6, no. 1, pp. 92-101, 2020.

[9] A. Imae, K. Mino , O. Koyama, K. Oyama, M. Yamaguchi, K. Ikeda and M. Yamada, "Router Control Function Using IoT Device Supported OpenFlow Switch in IP over AWG-STAR Network," Opto-Electronics and Communications Conference (OECC), 2020.

[10] A. D. Susilo, "IDS IMPLEMENTATION WITH MIKROTIK," MUM MikroTik, Hanoi, 2017.

[11] F. A. Zaky, "Prevention Login Bruteforce MikroTik," MUM MikroTik, Jakarta, 2016.

[12] T. Yuliswar, "How to Protecting your MikroTik Routers from Brute Force Attack," MUM MikroTik, Vientiane, 2017.

[13] A. Giordano and M. Ciantar, "Reducing The Impact of DoS Attacks with MikroTik RouterOS," MUM MikroTik, Prague, 2015.