JET Jurnal Elektro Teknik
Volume 1, No.1, Maret 2021, pp. 16-21

Analisa dan Implementasi Sistem Kemananan Jaringan Intrusion Detection System (IDS) Berbasis Mikrotik

[1]Agustini Rodiah Machdi, [2]Waryani, [3]Sugeng

[1,2]Program Studi Teknik Elektro, Universitas Pakuan,

[3]Program Studi Teknik Elektro, Univesitas Islam 45 Bekasi.

Email : agustini.rodiah@unpak.ac.id[1], waryani@unpak.ac.id[2], sugeng_pratama@yahoo.co.id[3]

Abstrak

Jurnal ini membahas mengenai analisa dari suatu system Intrusion Detection System (IDS) Berbasis Mikrotik untuk mendeteksi serangan DoS (Denial of Service) yang biasanya sering terjadi . Sistem ini digunakan untuk mendeteksi perilaku traffic dan mencocokannya dengan parameter-parameter yang telah dibuat untuk setiap jenis serangan. Analisa yang dilakukan adalah dengan mengkaji keakuratan pendeteksian system IDS, Analisa difokuskan pada enam jenis serangan DoS yaitu SYN flood, UDP flood, ICMP flood, Smurf, port scan, dan host scan. Hasil menunjukkan system ini dapat secara akurat mengidentifikasi semua traffic dan semua host yang terkait dengan aktivitas serangan.

Kata Kunci : Intrusion Detection System (IDS), Mikrotik, Denial of Service, DoS, DDoS

Abstract

This journal discusses the analysis of a Mikrotik-Based Intrusion Detection System (IDS) to detect DoS (Denial of Service) attacks that usually occur frequently. This system is used to detect traffic behavior and match it with the parameters that have been created for each type of attack. The analysis carried out is to examine the accuracy of the detection of the IDS system. The analysis focuses on six types of DoS attacks, namely SYN flood, UDP flood, ICMP flood, Smurf, port scan, and host scan. The results show this system can accurately identify all traffic and all hosts associated with attack activity.

Keywords : Intrusion Detection System (IDS), Mikrotik, Denial of Service, DoS, DDoS

1. Pendahuluan

Dengan semakin berkembangnya teknologi berbasis IP dan Internet, dimana akses ke dalam suatu system jaringan yang terhubung ke dalam internet semakin mudah, salah satu aspek yang menjadi perhatian adalah aspek keamanan. Seberapa amankah system jaringan yang ada dan terhubung ke dalam intenet ini.

Sistem yang terbuka di internet memungkinkan untuk diakses ataupun disusupi oleh orang-orang yang tidak bertanggung jawab, ataupun serangan yang mengganggu system sehingga menjadi tidak berfungsi.

Karena itu dibutuhkan suatu system keamanan jaringan yang mampu mendeteksi serangan maupun gangguan-gangguan kemanan tersebut.

Salah satu serangan yang paling sering terjadi adalah penyusupan ke dalam system jaringan atau biasa dikenal dengan network intrusion

Kemanan jaringan saat ini dapat berupa perangkat jaringan seperti Router, Firewall, Proxy Server, Demiliterized Zone (DMZ), Honeynet, Intrusion Prevention System (IPS) dan Intrusion Detection System (IDS)

Penelitian kali ini akan menganalisa dan menginplementasikan Intrusion Detection System (IDS) berbasis Router Mikrotik sebagai salah satu upaya mengamankan system jaringan dari serangan dan gangguan intrusi.

2. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan sebuah sistem yang digunakan sebagai pendeteksi aktivitas yang mencurigakan dalam sebuah system atau jaringan.

Intrusion tersebut dapat berupa :

1. Ping flood
2. Port scan
3. Serangan DoS/DDoS
4. Akses yang tidak dikenal ke router

A. Ping Flood

Ping Flood atau "Banjir Ping" merupakan serangan Denial of Service sederhana yaitu metode penyerangan dengan cara membanjiri target dengan paket "echo request" (ping) ICMP. Ini merupakan serangan paling efektif karena dengan menggunakan opsi flood ping maka paket ICMP dikirimkan secepat mungkin tanpa harus menunggu balasan dari target, sehingga akhirnya target menjadi down.

B. Port Scan

Port Scan merupakan sebuah serangan awal yang digunakan untuk mencari informasi atau status dari protocol dan port yang terbuka (open) dari sebuah perangkat. Ketika informasi protocol/port sudah ditemukan maka 'Hacker' dapat memanfaatkan port tersebut untuk melakukan eksploitasi melalui protocol/port tersebut.

C. Serangan DoS/DDoS

Denial-of-service (DDoS) attack terdistribusi adalah bentuk serangan untuk membuat layanan online menjadi down atau tidak dapat diakses oleh pengguna. DDoS attack dilancarkan dari berbagai perangkat yang disusupi, sering kali didistribusikan secara global dalam apa yang disebut sebagai botnet. Tipe serangan ini berbeda dari serangan Denial-of-service (DoS) yang hanya menggunakan satu perangkat yang terhubung ke Internet (satu koneksi jaringan) untuk membanjiri target dengan traffic data berbahaya. Skema inilah yang menjadi pembeda dua definisi serangan Dos dan DDoS.

Frekuensi serangan DDoS terus meningkat selama beberapa tahun terakhir, dan Q4 tahun 2020 mengalami peningkatan sekitar 10% selama tahun 2019.

D. Akses yang tidak dikenal ke router

Upaya jahat yang dilakukan dengan cara memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa izin atau tanpa sepengetahuan dari pemilik sistem jaringan. Biasanya pelaku (hacker) melakukan hal ini dengan tujuan sabotase ataupun mencuri informasi penting dan rahasia.

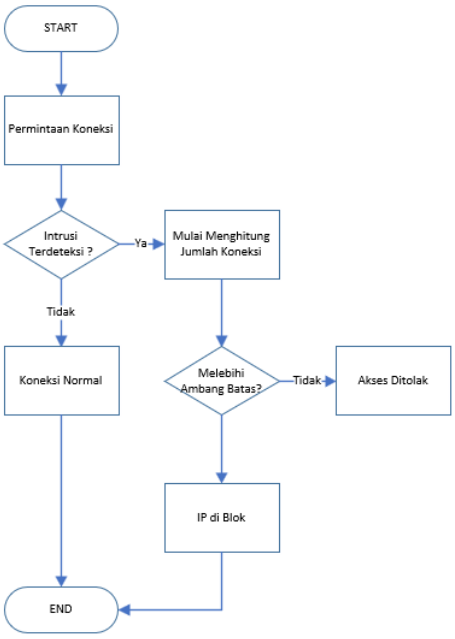
Dalam melakukan serangan terhadap jaringan terdapat beberapa tahapan yang harus dilakukan oleh penyerang, yaitu :

1. Planning
2. Information Gathering
3. Vulnerability Assessment
4. Exploiting

3. Implementasi IDS

Pada tahap information gathering. penyerang akan mencoba secara berulang-ulang untuk mengumpulkan informasi dari target sebanyak mungkin yang nantinya akan dipergunakan dalam menjalankan tahapan penyerangan selanjutnya. Saat proses pengumpulan informasi inilah penyerang akan mencari informasi port dan service apa yang terbuka.

Berikut ini merupakan gambar flowchart proses deteksi yang akan diimplementasikan



Gambar 1. Diagram alur sistematika implemetasi IDS

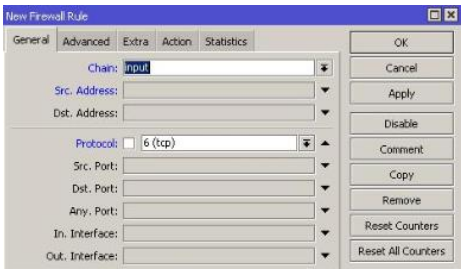
Penggunaan fitur firewall built in pada Mikrotik RouterOS yang didalamnya terdapat matcher Port Scan Detection fungsi bertujuan untuk mengenali adanya serangan port scanning dan melakukan pencegahan terhadap ancaman tersebut

Prinsip atau cara kerja nya adalah sebagai berikut :

1. Router akan melakukan monitoring setiap koneksi traffic yang masuk pada chain yang sudah dibuat.
2. Pada saat terdeteksi koneksi dari source address dan destination address yang sama dengan destination port yang berbeda dalam jangka waktu yang lebih kecil atau sama dengan delay threshold router maka akan menambahkan nilai sesuai kategori port yang diakses, apabila melakukan koneksi ke port yang rendah maka akan ditambahkan nilai yang ada di parameter low port weight dan apabila destination port pada port tinggi akan ditambahkan sesuai nilai yang ada pada parameter high port weight.
3. Saat Total nilai mencapai nilai Wight Threshold maka action pada rule tersebut akan dilakukan oleh router.

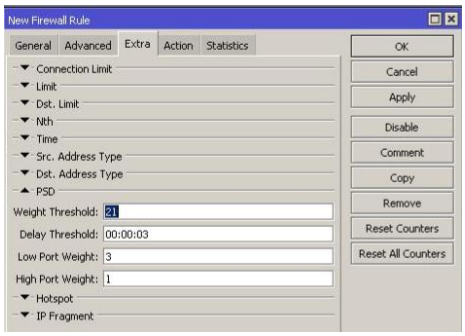
Berikut merupakan langkah untuk mengaktifkan IDS tersebut :

1. Pembuatan chain dan protocol, pada kasus ini chain yang digunakan adalah input karena tujuan nya adalah untuk melindungi dari ancaman port scanning pada router itu sendiri, sperrti yang terlihat pada gambar 2.



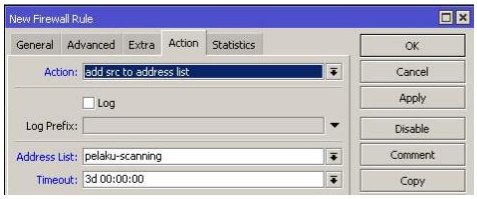
Gambar 2. Setting chain pada mikrotik

2. Setelah itu dilakukan aktivasi PSD dengan memasukan nilai parameter Weight Threshold, Low Port dan High Port, hal ini terlihat pada gambar 3



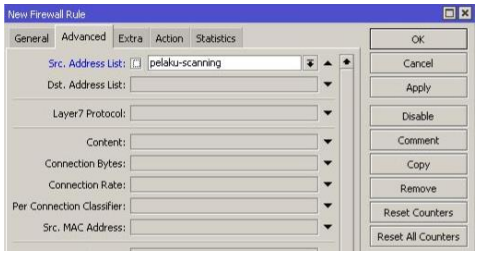
Gambar 3. Setting nilai threshold

3. Gambar 4 merupakan pembuatan address list agar router secara otomatis memasukan IP address yang dicurigai sebagai serangan pada system.



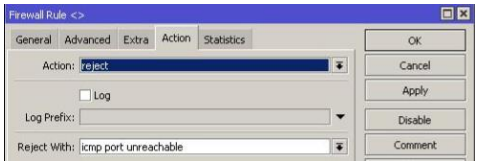
Gambar 4. Setting address list

4. Selanjutnya pembuatan rule agar router secara otomatis melakukan reject koneksi dan blok IP address secara otomatis, setting yang dilakukan terlihat pada gambar 5 berikut ini.



Gambar 5. Input ke address list otomatis untuk blok IP address

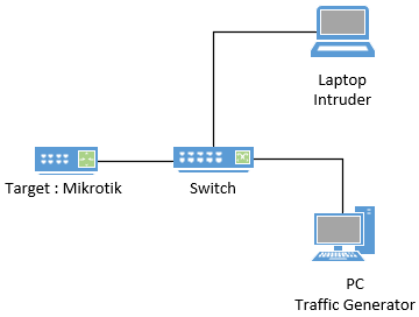
5. Gambar 6 merupakan setting rule agar router melakukan action reject terhadap koneksi dari IP yang melakukan serangan.



Gambar 6. Rules untuk reject akses (penolakan akses)

4. Skema Pengujian IDS

Skema pengujian IDS ini seperti yang terlihat pada gambar 7, satu buah PC yang akan digunakan sebagai traffic generator, satu bauh laptop yang akan dipergunakan sebagai penyusup atau intruder, serta satu buah router mikrotik sebagai target yang sudah dikonfigurasi sebagai IDS, semuanya terhubung dalam satu buah switch, sebagaimana yang terlihat pada gambar 7.



Gambar 7. Skema pengujian IDS

Traffic penyerangan dilakukan oleh laptop intruder menggunakan bantuan software Neptune untuk SYN Flood

Penentuan nilai threshold untuk pengujian dilakukan dengan cara melakukan learning process terlebih dahulu. Nilai threshold yang didapat dari learning process seperti yang terlihat pada tabel 1 dibawah ini.

Tabel 1. Nilai threshold hasil learning process

Jenis DoS	Parameter Threshold (per menit)	Batas Atas	Nilai yang Disarankan
SYN flood	Source ports	1.775	1.525
UDP flood	Jumlah paket UDP	1.715	1.455
ICMP flood	Jumlah paket ICMP	431	400
Smurf	Jumlah paket ICMP alamat broadcast	2.000	1.665
Port scan	Destination ports	375	295
Host scan	Destination IP Addresss	8	4

5. Analisa IDS

Pada tahap ini akan dilakukan Analisa mengenai performa dari IDS yang sudah dibuat. Analisa berdasarkan nilai-nilai sebgai berikut :

1. Akurasi pendeteksian
2. Utilisasi CPU
3. Pemakaian Memory

5.1. Akurasi Pendeteksian

Pada tabel 2 nilai-nilai didapat dari serangan yang diidentifikasi oleh system IDS dengan beberapa intensitas nilai traffic packet per second (pps), dimana dilakukan 15 contoh serangan yang di generate oleh laptop intruder, dan semuanya (15 serangan) langsung

terdeteksi sebagai serangan, akurasi mencapai 100%.

Tabel 2 Alert dari traffic attack

Jenis DoS	Intensitas Background Traffic (pps)						
	5.000	6.000	7.000	8.000	9.000	10.000	11.000
SYN flood	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
UDP flood	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
ICMP flood	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
Smurf	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
Port scan	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
Host scan	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)

Sedangkan pada tabel 3, system diuji dengan traffic biasa dari PC traffic generator yang juga dengan beberapa nilai intensitas traffic yang sama, tetapi karena bukan merupakan serangan maka system tidak mendeteksi apapun dari traffic yang masuk, nilai deteksi 0. Dengan demikian system mampu memilah mana traffic yang merupakan serangan atau bukan.

Tabel 3. Alert dari traffic generator

Jenis DoS	Intensitas Background Traffic (pps)						
	5.000	6.000	7.000	8.000	9.000	10.000	11.000
SYN flood	0	0	0	0	0	0	0
UDP flood	2	0	0	0	0	0	0
ICMP flood	1	5	0	0	0	0	0
Smurf	0	0	0	0	0	0	0
Port scan	0	0	0	0	0	0	0
Host scan	556	621	600	621	855	486	624

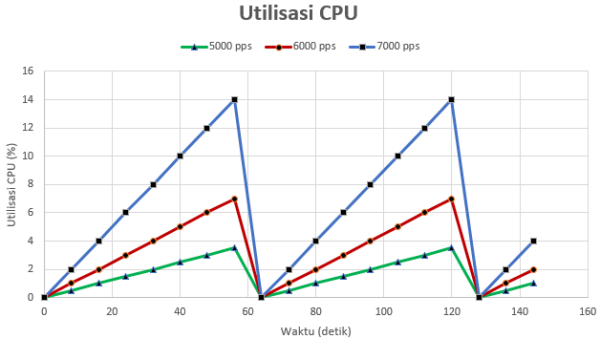
Selanjutnya dilakukan pengujian dengan menggunakan traffic campuran antara traffic serangan dan traffic normal, menggunakan 15 serangan per jenis serangan dan dilakukan secara simultan dengan interval 30 menit, hasilnya seperti yang terlihat pada tabel 4, serangan berhasil terdeteksi secara akurat 100% walaupun bercampur dengan traffic normal lainnya.

Tabel 4. Alert dari campuran traffic generator dan attack

Jenis DoS	Intensitas Background Traffic (pps)						
	5.000	6.000	7.000	8.000	9.000	10.000	11.000
SYN flood	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
UDP flood	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
ICMP flood	11	14	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
Smurf	12	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)	15 (100%)
Port scan	15 (100%)	15 (100%)	12	11	15	11	15 (100%)

5.2. Utilisasi CPU

Pada saat pengujian akurasi pendeteksian dilakukan juga pengamatan utilisasi CPU yang terjadi, pengamatan tersebut terlihat pada grafik gambar 8.



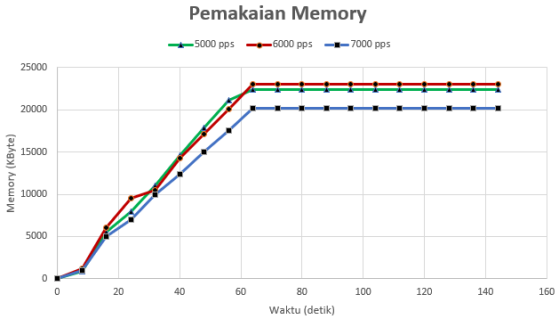
Gambar 8. Grafik utilisasi CPU Router pada saat terjadi serangan

Utilisasi CPU berlangsung mencapai puncaknya pada detik ke-60, hal ini dikarenakan system IDS harus mengkasifikasikan jenis packet data yang masuk apakah merupakan serangan atau bukan.

5.3. Pemakaian Memory

Pemakaian memori juga merupakan salah satu yang diamati untuk melihat performa system IDS ini, pada saat pengujian berlangsung terlihat penggunaan memori mulai naik secara bertahap pada 60 detik pertama, kemudian setelah itu memory stabil di sekitar angka 23 Mbyte, seperti yang terlihat pada gambar 9 di bawah ini.

Dari pengamatan ini, sepertinya pemakaian memory tidak terpengaruh oleh intensitas traffic yang terjadi.



Gambar 9. Grafik pemakaian Router pada saat terjadi serangan

6. Kesimpulan

Pada penelitian ini penentuan threshold yang sesuai merupakan langkah penting dalam menentukan keberhasilan pengujian IDS maupun implementasi IDS.

Tingkat akurasi pendeteksian suatu system IDS sangatlah bergantung pada penentuan ambang batas/threshold, penentuan ambang batas ini harus benar-benar sesuai dengan tingkat akurasi pendeteksian yang diingainkan.

Dalam pengujian ini semua serangan DoS (6 jenis serangan) dapat dideteksi dengan baik oleh system.

Penentuan ambang batas/threshold yang terlalu rendah akan mengakibatkan false-alarm, namun tidak semua false-alarm ini tidak penting, karena itu tetap harus dianalisa mengenai kemungkinan serangan yang terjadi.

DAFTAR PUSTAKA

[1] Dony Ariyus, M. Kom.,"Intrusion Detection System", CV Andi Offset, Yogyakarta, 2007.
[2] Harijanto Pribadi, "Firewall Melindumgi Jaringan dari DDoS Menggunakan Linux dan Mikrotik", CV Andi Offset, Yogyakarta, 2008.
[3] John Kevin & Dennis Mwangi, "Intrusion Detection and Intrusion Prevention Systems in an Information Security Study Lab Environment", Lulea University of Technology, Lulea Swedia, 2013.
[4] Zheni Svetoslavova Stefanova, "Machine Learning Methods for Network Intrusion Detection and Intrusion Prevention Systems", University of South Florida, Florida US, 2018.
[5] Thomas J. Mowbray, PhD, "Cybersecurity Managing Systems, Conducting Testing, and Investigating Intrusions", John Wiley & Sons, Inc.,Indianapolis, 2014.
[6] Rifkie Primartha, "Security Jaringan Komputer Berbasis CEH", Informatika, Bandung, 2018