SITEKIN: Jurnal Sains, Teknologi dan Industri, Vol. 19, No. 1, Desember 2021, pp.1 - 8
ISSN 2407-0939 print/ISSN 2721-2041 online

Implementasi Intrusion Detection System Pada Local Area Network (Studi Kasus : Yayasan Pendidikan Tanah Tingal Tangerang)

Nanang Nuryadi[1], Elia Christine Nainggolan[2]

[1]Jurusan Ilmu Komputer, Fakultas Teknik dan Informatika, Universitas Bina Sarana Informatika
Tegal Jl.Sipelem No.22 Depan Mall Rita Tegal Barat
Email : nanang.nyd@bsi.ac.id

[2] Jurusan Ilmu Komputer, Fakultas Teknik dan Informatika, Universitas Nusa Mandiri
Jl. Jatiwaringin No. 2 Jakarta Timur, 13620
Email : eliachristinen@gmail.com

ABSTRAK

Jaringan internet saat ini sudah menjadi kebutuhan yang sangat umum, menyadari pentingnya peran dan penggunaan internet dalam kehidupan sehari-hari, internet saat ini tidak hanya menjadi media penyambung untuk berkomunikasi atau bertukar informasi, tapi juga menjadi media pertukaran data serta penyimpanan data yang bersifat sangat pribadi bagi individu atau rahasia bagi suatu perusahaan maupun lembaga, termasuk lembaga pendidikan di Yayasan Pendidikan Tanah Tingal. Seluruh data sekolah yang mencakup data pribadi siswa, maupun data pribadi lembaga pendidikan tersebut merupakan data yang harus tetap dijaga kerahasiaannya. Semakin canggih dan berkembangnya internet masa kini, semakin cerdas para peretas (*cracker* atau *hacker*) mempelajari celah pada jaringan internet untuk mencuri data yang nantinya bisa berakibat fatal dan merugikan. Oleh karena itu dengan mengimplementasikan IDS (*Intrusion Detection System*) menggunakan fitur *Filtering Firewall* mikrotik pada jaringan internet merupakan hal yang tepat untuk mencegah serangan masuk dengan cara mencegah dan mendeteksi jika adanya serangan-serangan jahat di dunia internet yang dapat menyerang dan merusak sistem jaringan internet. Selain untuk mencegah dan mendeteksi, konfigurasi IDS pada *Filtering Firewall* Mikrotik juga dapat melakukan *monitoring traffic* jaringan internet masuk. Hasil pengujian implementasi dari fitur Filtering Firewall IDS membuktikan bahwa IDS dapat mencegah dan mendeteksi adanya serangan yang masuk pada sistem jaringan LAN Yayasan Pendidikan Tanah Tingal sehingga pencegahan *intrusion* pun dapat dilakukan.

Kata Kunci: *Intrusion Detection System, Filtering Firewall, Ping Flood*

ABSTRACT

The internet network nowadays is being a very common need, realizing the importance of the role and using of the internet in everyday life, the internet is not only a media for communicating or exchanging information, but also a media for exchanging data and storing data that is very personal for individuals or privacy for a company or institution, including educational institutions in the Tanah Tingal Education Foundation. All school data which include students' personal data, as well as the educational institution's personal data are data that must be kept confidential. The more sophisticated and the development of internet networks today, the more intelligent hackers (Crackers or Hackers) learn the gaps in the internet network to steal data which can later be fatal and detrimental. Therefore, by implementing IDS (Intrusion Detection System) using the Mikrotik Filtering Firewall feature on the internet network is the right thing to prevent incoming attacks by filtering network configuration so that it can ward off evil attacks in the internet world that can fight and damage the system Internet Network. In addition to preventing and activating, configuring IDS on the Mikrotik Firewall Filtering can also monitor incoming internet network traffic. The results of testing the implementation of the IDS Firewall Filtering feature prove that IDS can prevent and prove that an attack has entered the LAN system of the Tanah Tingal Education Foundation so that it can prevent intrusion attacks.

Keywords: *Intrusion Detection System, Filtering Firewall, Ping Flood*

PENDAHULUAN
Latar Belakang Masalah

Jaringan internet saat ini sudah menjadi kebutuhan yang sangat umum. Siapapun membutuhkan jaringan internet baiksecara pribadi untuk diri sendiri, maupun secara umum seperti halnya organisasi, perusahaan atau lembaga-lembaga yang menggunakan internet untuk kelangsungan hidup organisasi, perusahaan atau lembaga tersebut. Dengan jaringan internet semua dapat berinteraksi di dunia maya, membagikan atau bertukar informasi, data, file, dokumen dan berbagai macam *attachment* lainnya. selain untuk membagikan atau bertukar infromasi dan data, internet juga dapat menyimpan berbagai data yang disimpat terpusat seperti *cloud computing* yang memungkinkan *user* mengakses data pribadi mereka melalui komputer atau *gadget* dengan akses internet, dengan tersedianya layanan internet yang memungkinkan *user* menyimpan data hal itu tentu dapat menghemat biaya *user* dengan tidak perlu membeli memori fisik seperti *hardisk* untuk menyimpan data. Data tersebut dapat disimpan pada server yang disediakan oleh penyedia layanan *cloud computing*, sehingga *user* dapat dengan mudah mengaksesnya kapan saja dan dimana saja selama terhubung dengan jaringan internet.

Komunikasi data pada internet melibatkan masalah keamanan, kemudahan dan kecepatan transfer (pertukaran data). Hal ini harus diperhatikan oleh pemilik dan administrator sistem informasi suatu perusahaan dalam melakukan kegiatan didunia internet, sehingga kerahasiaan informasi suatu perusahaan bisa terjaga dengan baik dan kemudahan dan kecepatan (pertukaran data) bisa diimplementasikan sehingga dapat menjadi nilai yang bisa berpengaruh pada *cost* perusahaan [1].

Penelitian terdahulu pernah melakukan pendeteksian adanya penyusup yang mencoba menembus jaringan internet komputer [2]. Penelitian sistem keamanan jaringan komputer dilakukan dengan cara menggabungkan fungsi IDS dan IPTables system untuk mencegah adanya penyusupan. Sistem tersebut dirancang dengan memberikan blocking alamat IP yang tidak dikenali. Penelitian tersebut menunjukkan sistem pendeteksi tersebut terfokus pada jenis serangan yang datang dan memberikan notifikasi melalui pesan (SMS). Begitu juga dengan penelitian menggunakan sistem IDS *wireless* (tanpa kabel), hasil penelitian menunjukkan bahwa IDS berhasil mendeteksi berbagai jenis serangan yang dapat dilihat IP Address penyusup melalui grafik yang ditunjukkan [3]

Saat ini yang menjadi masalah pada Yayasan Pendidikan Sekolah Tanah Tingal, terutama divisi SD Tanah Tingal yaitu belum adanya keamanan jaringan ataupun *monitoring* setiap *traffic* jaringan. Seperti kasus yang pernah terjadi pada tahun 2018 oleh admin sekolah ketika men*download* suatu file dan ternyata isi file tersebut merupakan file *corrupt* yang berisi virus, saat file sudah dalam proses *downloading* baru terdeteksi bahwa adanya kejanggalan dalam file tersebut. Saat file berhasil terunggah maka koneksi jaringan dan kinerja program pada PC tersebut menjadi lambat. Tindakan utama yang dilakukan oleh administrator sekolah dan bagian IT adalah dengan cara menonaktifkan akses internet pada PC tersebut dan menghapus file yang baru saja diunduh tanpa membuka file tersebut.

Sekolah Tanah Tingal merupakan sekolah yang memanfaatkan jaringan internet untuk menunjang dan mendukung kegiatannya sehari-hari mulai dari penyimpanan data-data penting yang berkaitan dengan siswa seperti raport siswa, data biaya pembayaran sekolah siswa, dan data-data umum maupun privacy lainnya yang hanya boleh diketahui oleh pihak sekolah dan yayasan. Permasalahan saat ini pada sistem jaringan internet di Sekolah Tanah Tingal sebagai berikut:

1. Belum adanya keamanan jaringan yang dapat membatasi akses keluar masuk pada jaringan internet sehingga membuat jaringan internet sekolah menjadi rentan terserang oleh berbagai macam serangan seperti virus atau serangan lainnya berupa paket yang dapat menyerang fisik maupun *logic*, hal itu tentunya akan berdampak buruk bagi pihak sekolah dan bahkan bisa menyebabkan kerugian.
2. Belum adanya sistem yang dapat membantu administrator/IT sekolah untuk melakukan *monitoring traffic* jaringan yang keluar masuk, sehingga sulit untuk mengetahui dan melacak dari mana akar permasalahan yang timbul atas kejadian yang terjadi pada sistem jaringan komputer sekolah saat adanya anomali atau kejadian-kejadian yang tidak normal seperti biasanya.
3. Belum adanya penerapan secara permanen yang dilakukan untuk mencegah terjadinya serangan pada jaringan internet sekolah yang disebabkan oleh kurangnya pengetahuan mengenai metode-metode yang dapat digunakan untuk melindungi jaringan internet.

Adapun maksud dan tujuan penulisan ini, yaitu :

1. Meningkatkan keamanan jaringan di Yayasan Sekolah Tanah Tingal untuk mengurangi resiko penyusupan atau terserang oleh virus-virus yang dapat menghilangkan data penting sekolah.
2. Mengimplementasikan IDS pada keamanan jaringan di Yayasan Sekolah Tanah Tingal

menggunakan *router* mikrotik dengan konfigurasi melalui aplikasi *Winbox*.
3. Menerapkan batas limit serangan *ping-flood* untuk mencegah serangan DoS, konfigurasi *rule* ICMP, menerapkan metode *Port Scan* dan *Port Knocking*.
4. Mendeteksi dan mencegah adanya penyusupan atau penyerangan pada jaringan komputer Yayasan Sekolah Tanah Tingal.

METODE PENELITIAN

Metode penelitian yang dilakukan terdiri dari 3 metode yaitu observasi, wawancara dan studi pustaka. Sementara metode penelitian yang dilakukan yaitu mengimplementasikan IDS (*Intruction Detection System*) pada jaringan internet di yayasan pendidikan sekolah Tanah Tingal.

IDS (Intrusion Detection Systsem)

Menurut Depkominfo dalam jurnal [4] menyimpulkan bahwa:
Intrusion Detection System (IDS) adalah tahap awal dari sistem yang memiliki fungsi sebagai pendeteksi apabila terjadi anomali pada lalu lintas paket data di jaringan. Apabila sistem *Intrusion Detection System* (IDS) mendeteksi anomali tersebut, langkah selanjutnya adalah mencatat data tersebut ke sebuah *log* lalu memberi peringatan kepada administrator jaringan.

Menurut Ariyus dalam jurnal [5] berpendapat ada beberapa alasan untuk memperoleh dan menggunakan IDS (*Intrusion Detection System*), diantaranya adalah:
1. Mencegah resiko keamanan yang terus meningkat dikarenakan banyaknya ditemukan kegiatan ilegal yang diperbuat oleh seseorang atau oknum-oknum yang tidak bertanggung jawab sehingga jika kegiatan ilegal tersebut terdeteksi.
2. Mendeteksi serangan dan pelanggaran keamanan sistem jaringan yang tidak dapat dicegah oleh sistem umum, sehingga terjadi banyaknya lubang keamanan, seperti :
   a. *Legacy* sistem, sistem operasi tidak *patch* maupun *update*.
   b. *Patch* tidak diperhatikan dengan baik, sehingga menimbulkan masalah baru dalam hal keamanan.
   c. *User* yang tidak memahami sistem, sehingga jaringan dan protokol yang mereka gunakan memiliki lubang keamanan.
   d. *User* dan *administrator* membuat kesalahan dalam konfigurasi dan dalam menggunakan sistem.
3. Mendeteksi serangan awal.
4. Mengamankan file yang keluar dari jaringan.
5. Sebagai pengendali untuk rancangan keamanan dan *administrator*, terutama bagi perusahaan yang pesat.
6. Menyediakan informasi yang pasti dan akurat terhadap gangguan yang datang secara langsung, meningkatkan diagnosis, *recovery*, dan mengoreksi faktor-faktor penyebab serangan.

Intrusion merupakan salah satu serangan dan penyusupan yang berhubungan dengan integritas, konfidensialitas dan ketersediaan pada jaringan internet dan media perangkat, serangan *intusion* (penyuspan) dapat merusak *hardware*, *software* bahkan data-data yang terdapat pada suatu sistem komputer dimana sistem tersebut terhubung pada jaringan internet. Selain mengakibatkan kerusakan, *Intrusion* dapat menyerang jalur komunikasi yang menggunakan internet sebagai media penghubungnya [6].
Dibawah ini merupakan 2 macam *intrusion* pada jaringan internet :
a. *Ping Flood*
   Ping Flood atau banjir ping merupakan sebuah serangan DoS (Denial of Service) atau DDoS (Distributed Denial Of Service), cara kerja penyerangannya yaitu dengan membanjiri *traffic* jaringan internet dengan mengirimkan ping dalam jumlah yang sangat banyak pada suatu jaringan sehingga membuat target jaringan tersebut menjadi down. Jumlah ping yang dikirim dapat menyebabkan error bahkan kerusakan.
b. *Port Scan*
   Port scan merupakan serangan yang dilakukan dengan cara memindai suatu port jaringan target, menganalisa port jaringan target kemudian mencari celah agar port target dapat terbuka.

Dalam jurnal penelitian terdahulu [7] *Intrusion Detection System* memiliki cara kerja untuk menganalisa setiap paket data yang keluar/masuk dalam sistem jaringan yang kemungkinan dianggap sebagai serangan atau penyusupan, antara lain:
a. *Knowledge Based* (*Misuse Detection*)
   Cara kerja *knowledge based* dalam IDS dengan cara melihat dan mengenali lalu lintas paket data dalam sistem internet dengan *database rule* pada IDS.
b. *Behavior Based* (*Anomaly Based*)
   Cara kerja *behavior based* dalam IDS yaitu dengan cara mendeteksi setiap lalu lintas paket data dalam jaringan, kemudian mengamati adanya kemungkinan serangan berdasarkan kejanggalan-kejanggalan yang terjadi pada

sistem internet yang tidak berjalan normal seperti biasanya.

Mikrotik Routerboard

Menurut Amarudin, 2018 dalam [8] berdasarkan penulisan penelitian sebelumnya menjelaskan bahwa mikrotik merupakan perangkat jaringan komputer perpaduan antara software dan hardware yang dapat difungsikan sebagai *switching*, *router*, alat untuk *filtering* jaringan internet, dan yang lainnya. *Hardware* mikrotik bisa berupa router PC yang dapat diinstal maupun berupa *routerboard*.

Dalam tulisan yang dikutip oleh [9] menurut Sopandi (2010:19) *router* merupakan perangkat keras jaringan yang digunakan untuk menghubungkan beberapa jaringan yang sama maupun jaringan yang berbeda, kemudian jaringan-jaringan tersebut di teruskan oleh *router* melalui paket data dengan cara memilih jalur *route* tercepat dan terbaik. Mikrotik *router* tipe RB941-2nD-TC yang memiliki 4 port dengan arsitektur SIMPS-BE dan RAM sebesar 31MB akan menjadi alat penunjang untuk membantu mengimplementasikan jaringan usulan.

Gambar 1. Router Mikrotik

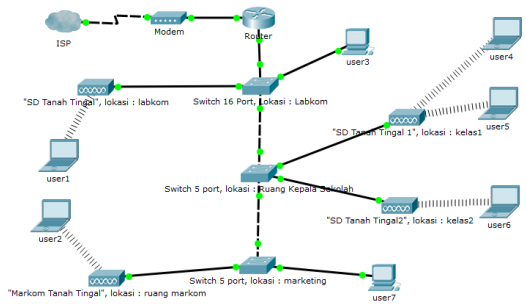
Winbox v6.29.1

Winbox merupakan *software* (perangkat lunak) yang dapat digunakan untuk mengontrol sebuah server mikrotik ke dalam mode GUI (*Graphical User Interface*) melalui Sistem Operasi *Windows* [10]. Fungsi utama pada aplikasi *winbox* yaitu untuk mengatur atau mengkonfigurasi mikrotik dengan tampilan GUI. Jaringan internet mikrotik yang telah selesai di *setting* atau di konfigurasi juga dapat dipantau oleh aplikasi *winbox* [11]. Dalam hal ini winbox dapat digunakan untuk mengimplementasikan jaringan komputer.

HASIL DAN PEMBAHASAN

Skema Jaringan Berjalan

Dibawah ini merupakan gambar skema jaringan SD Tanah Tingal berdasarkan hasil riset.



Gambar 2. Skema Jaringan Berjalan

Topologi jaringan yang berjalan saat ini di Yayasan Pendidikan Sekolah Tanah Tingal yaitu menggunakan topologi *star*. Jaringan internet pada gambar diatas berfungsi sebagai media komunikasi, pengiriman data atau file, *printer*, *scanner*, dan CCTV.

Keterangan pada gambar :

a. *Provider* jaringan internet di SD Tanah Tingal yaitu PT. Remala sejak tahun 2017.
b. Topologi yang digunakan pada jaringan internet SD Tanah Tingal adalah topologi *Star*.
c. Modem mikrotik sebagai penghubung antara ISP (*Internet Service Provider*) dan internet sekolah kemudian disalurkan melalui *switch* dan *access point* ke seluruh area sekolah.
d. *Setting*-an network menggunakan kabel UTP (*Unshield Twisted Pair*) sebagai media penghubung dari komputer ke komputer maupun komputer ke perangkat lainnya seperti *switch* dan *router*.

Analisa Permasalahan

Keamanan Jaringan di SDS Tanah Tingal saat ini masih menjadi pertimbangan bagi IT sekolah. Karena saat ini, pengaturan alamat IP Address masih menggunakan DHCP, termasuk komputer-komputer yang ada di ruang lab komputer. Dengan menggunakan mikrotik, upaya yang dilakukan saat ini untuk mengamankan jaringan internet yaitu dengan cara memblokir kata-kata yang sekiranya tidak cocok untuk siswa SD melalui *firewall*. Sementara pada masing-masing komputer/PC *client* yang berada diruang lab komputer maupun di masing-masing ruang *staff* dipasang aplikasi antivirus.

Usulan Pemecahan Masalah

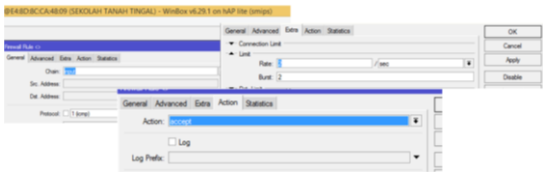
Berdasarkan permasalahan yang terjadi pada sistem jaringan internet Sekolah Tanah Tingal yaitu belum adanya pemecahan masalah yang diterapkan untuk mencegah adanya kerusakan atau kerugian. Alternatif pemecahan masalah yang

disarankan pada pihak Sekolah Tanah Tingal yaitu dengan mengimplementasikan IDS (*Intrusion Detection System*) pada sistem jaringan dengan 2 metode pencegahan *instrusion* yaitu Ping *Flood*, *Port Knocking* dan *Port Scanning*.

Rancangan Aplikasi

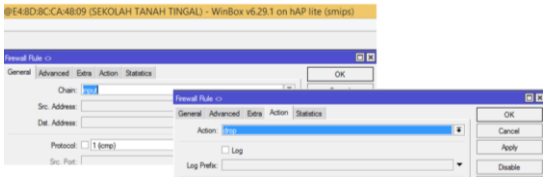
1. *Ping Flood Limit*

Ping flood merupakan salah satu jenis serangan *intrusion* (penyusupan) dengan cara membanjiri sistem jaringan dengan memberikan paket ping secara terus menerus, hal itu akan membuat jaringan menjadi lambat. Untuk mencegah *intrusion* tersebut maka akan diberikan *limit*, berikut konfigurasinya.



Gambar 3. Konfigurasi *Limit Ping Flood Accept*

Setelah itu, melakukan konfigurasi *drop ping flood.* Berikut konfigurasinya

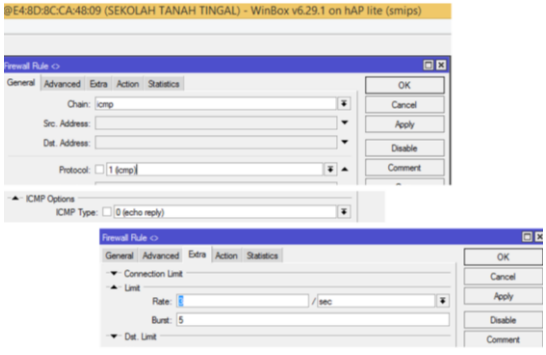


Gambar 4. Konfigurasi *Limit Ping Flood Drop*

Dengan memberikan limit 2 (dua) pada masing-masing *Rate* dan *Burst*, jika ada paket asing yang datang untuk minta *reply*, maka secara otomatis status akan berubah menjadi *request time out* jika ping yang datang melebihi batas di setiap detiknya.

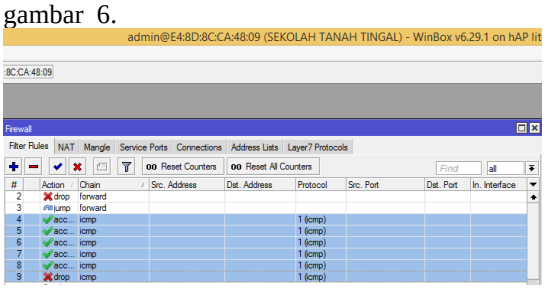
2. ICMP *Message Rule*

Selanjutnya membuat *rule* pesan pada ICMP. Berikut konfigurasinya



Gambar 5. Konfigurasi ICMP *Message Rule*

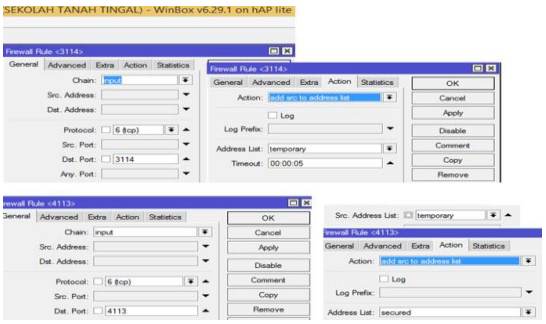
Chain yang digunakan pada konfigurasi di atas adalah ICMP, umumnya pada *router* mikrotik hanya terdapat 3 (tiga) *chain* yaitu *forward*, *input* dan *output*, namun kita bisa menambahkankan *chain*. Tambahkan *chain* ICMP untuk dapat konfigurasi ICMP *Message Rul*e. Hasilnya seperti gambar 6.



Gambar 6. ICMP *Flood*

3. Port *Knocking*

Port *Knocking* merupakan metode membuka pintu port *router*. Salah satu serangan *intrusion* yaitu dengan mencari celah pada jalur pintu port sehingga ia dapat memasuki *router* pada sistem jaringan target. Berikut adalah konfigurasi yang di setting untuk mengamankan port *router* dari serangan intrusion.

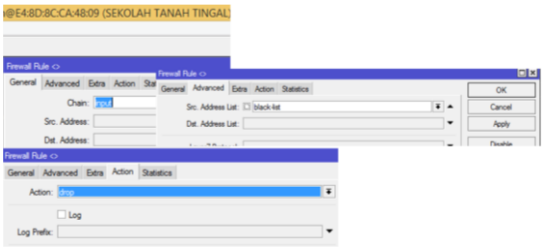


Gambar 7. *Port Knocking*

Konfigurasi ini artinya yaitu, jika ada paket jaringan yang mau masuk ke port tersebut maka diberi waktu selama 5 detik untuk mengisi port pasangannya.

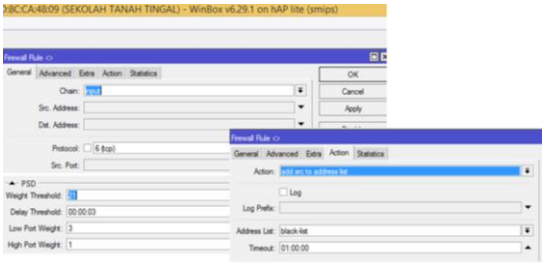
4. Port *Scan*

Port *scan* merupakan metode *intrusion* dimana paket data asing melakukan *scanning* port *router* untuk mengintip apakah ada celah terbukanya pintu port *router* agar *intruder* dapat masuk ke sistem jaringan melalui port *router* tersebut. Untuk melindungi port *router* dari serangan *scanning* berikut adalah langkah-langkah konfigurasi yang dilakukan.



Gambar 8. Konfigurasi *Port Scan*

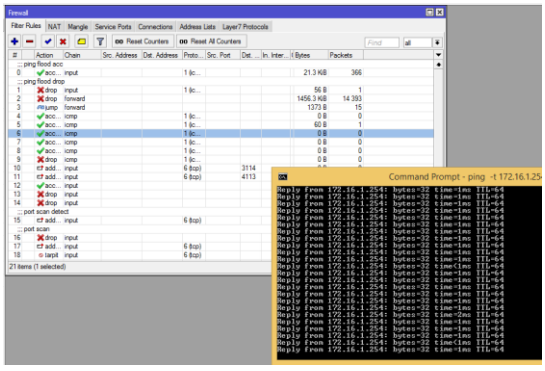
Gambar selanjutnya merupakan konfigurasi untuk mendeteksi saat terjadinya port *scan*.



Gambar 9. Konfigurasi *Port Scan Detect*

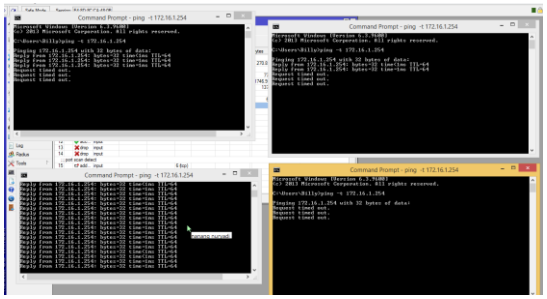
Pengujian Jaringan

Pada tahap pengujian, dilakukan uji coba dengan mengaktifkan konfigurasi *rule* yang sudah dibuat kemudian melakukan perintah ping menggunakan *command prompt* melalui *client* atau perangkat komputer yang terhubung langsung ke *router* utama selama kurang lebih 10 s/d 15 menit. Seperti gambar dibawah ini dapat dilihat adanya perbedaan jumlah *Bytes* dan *Packets* yang membuktikan bahwa adanya aktifitas jaringan dan aktifitas jaringan tersebut terus bertambah.



Gambar 10. Pengujian Ping menit ke-10

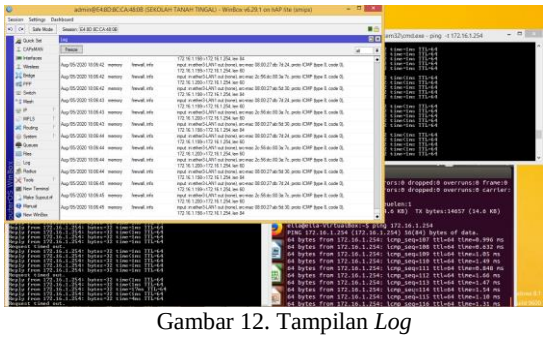
Setelah mencoba *ping flood* pada satu terminal dan hasilnya *router* tetap memberikan *reply* atau balasan, pengujian selanjutnya yaitu menggunakan 4 *command prompt* untuk menguji apakah *rule firewall* yang telah dikonfigurasi berfungsi menghentikan *ping flood*, seperti yang telah dijelaskan sebelumnya serangan *ping flood* dapat mempengaruhi kinerja sistem jaringan komputer, bahkan jika dikirim dengan jumlah yang sangat banyak dengan menggunakan beberapa *host* dalam satu waktu bisa berakibat fatal. Berikut pengujian yang dilakukan dengan memanggil *Ping –t 172.16.1.254* dalam waktu yang bersamaan dengan menggunakan 4 *command prompt*.



Gambar 11. Pengujian Ping Flood 4 CMD

Berdasarkan hasil pengujian diatas, tiga diantara empat *command prompt* yang mengirimkan paket *ping flood* mengalami kegagalan saat meminta balasan dari *router* dan hanya satu yang terus memberikan *reply* atau balasan. Hal ini membuktikan bahwa hasil konfigurasi yang diterapkan dapat menghentikan secara otomatis permintaan *ping flood* yang dikirim dalam waktu bersamaan.

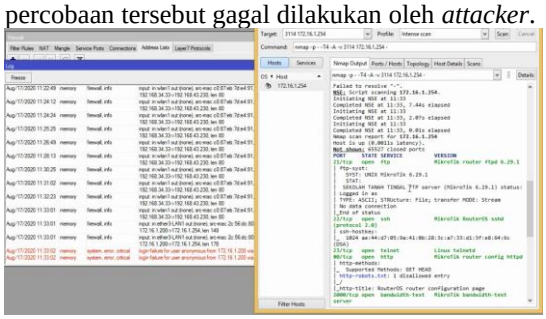
Selanjutnya, setelah melakukan uji coba *ping flood* melalui *windows* kemudian melakukan uji coba dengan menggunakan *virtual box* untuk menguji jaringan dari berbagai *IP Address* yang berbeda. Adapun Sistem Operasi yang digunakan melalui *Virtual Box* yaitu *Windows XP* dan *Linux Ubuntu*. Aktifitas yang berjalan ketika meminta *reply* melalui *Ping* 172.16.254 tercatat pada *log* mikrorik, sehingga dapat terlihat sumber paket jaringan yang masuk kedalam sistem jaringan internet.



Gambar 12. Tampilan *Log*

Pengujian jaringan selanjutnya yaitu pembuktian port *scanning* dengan menggunakan aplikasi NMAP, dimana yang menjadi tujuan yaitu port 3114 dengan alamat IP *Address Router* mikrotik 172.16.1.254.

Pada *log* terlihat notifikasi bahwa adanya percobaan untuk memasuki port *router* tersebut, namun percobaan tersebut gagal dilakukan oleh *attacker*.



Gambar 13. Tampilan *Port Scanning*

KESIMPULAN

Setelah melakukan analisa pada jaringan komputer LAN SDS Tanah Tingal Tangerang dan melakukan penelitian seperti yang telah diuraikan diatas, maka dapat disimpulkan bahwa jaringan yang telah di uji dengan menerapkan IDS (*Intrusion Detection System*) menggunakan *Filtering Firewall* mikrotik terbukti serangan dapat dicegah sebelum serangan itu masuk ke dalam sistem jaringan internet, konfigurasi *yang* dilakukan melalui *routerboard* mikrotik dengan menggunakan metode *Ping Flood, Port Scan, Port Knock* dan *Limit Connection* dapat membuktikan bahwa *intrusion* tidak dapat mengganggu sistem jaringan internet dikarenakan adanya batasan *rule* yang dikonfigurasi melalui *router* mikrotik, sejarah pencatatan atau *log* pada mikrotik dapat merekam serta menampilkan segala aktifitas yang terjadi didalam sistem jaringan internet secara akurat dan detail, hal tersebut membuktikan bahwa mikrotik dapat menyimpan *log* pada mikrotik dapat menjadi sumber pencarian terhadap paket-paket yang dirasa mencurigakan, serta pengujian akhir pada implementasi IDS *filtering firewall* menunjukkan *rule* dapat bekerja sesuai dengan konfigurasi, sehingga paket asing yang masuk dengan maksud yang mencurigakan tidak dapat menembus sistem jaringan.

Saran

Sebaiknya maintenance jaringan dilakukan secara berskala dengan konsisten untuk mengurangi adanya *error* yang terjadi pada pengaturan di *winbox* ataupun di mikrotik. Sebaiknya Yayasan Sekolah Tanah Tingal memperbaharui infrastruktur jaringan dengan menambahkan server jaringan agar database ada pada satu lokasi dan tersimpan dengan baik dan lebih teratur.

DAFTAR PUSTAKA

[1] M. Akbar, “Perancangan Software Ids Snort Untuk Pendeteksian Serangan Interruption (Netcut) Pada Jaringan Wireless,” 2018.

[2] Afirizial; Fitriani;, “Penerapan IPV4 dan IPV6 pada Jaringan yang Terhubung,” vol. 3, no. 1, pp. 2–6, 2019.

[3] Sutarti, P. Pancaro, Adi, and I. Saputra, Fembi, “Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal,” J. PROSISKO, vol. 5, no. 1, 2018, [Online]. Available; http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/download/584/592.

[4] E. Varianto And Mohammad Badrul, “Implementasi Virtual Private Network Dan Proxy Server Menggunakan Clear Os Pada Pt.Valdo International,” J. Tek. Komput. Amik Bsi, vol. 1, no. 1, pp. 55–56, 2015.

[5] R. Arfiansyah, “Analisa Dan Implementasi Virtual Private,” 2017.

[6] C. Kurnadi, “Rancangan dan Implementasi Jaringan Wireless Privat Pada Network Rs. Abdi Waluyo,” J. Chem. Inf. Model., vol. 53, no. 9, pp. 1689–1699, 2019, doi: 10.1017/CBO9781107415324.004.

[7] M. Raharjo, “Bab ii landasan teori Perancangan Performansi QoS Dengan Metode VRRP Pada PT. Pelita Cengkareng Paper Tangerang,” pp. 8–39, 2016.

[8] D. S. H. Panjaitan, “Filtering Content Dengan Metode String Menggunakan Router Mikrotik Pada Pt.Bebentara Perkasa Indonesia Jakarta,” 2019.

[9] C. A. Pamungkas, “Manajemen bandwith menggunakan mikrotik routerboard di politeknik indonusa surakarta,” Inf. Politek Media Notifikasi,” no. May, 2017.

[10] C. Iswahyudi, “Implementasi Intrussion Detection System (IDS) Dengan Menggunakan Jejaring Sosial Sebagai Media Notifikasi,” no. May, 2017.

[11] I. A. Sobari, “Rancangan Wireless Intrusion Detection System Menggunakan Snort,” vol. XII, no. 1, pp. 1–9, 2015.

[12] Panggabean Parningotan, “Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (Ids) Untuk Optimasi Keamanan Jaringan Komputer” vol. VI, no. 1, Mei 2018.

[13] Gondohanindijo Jutono, “Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System) vol. XII, 2015”

[14] Santoso Joko Dwi, “Keamanan Jaringan Nirkabel Menggunakan Wireless Intrusion Detection System” vol. I, no.3.

[15] D. Susianto, “Jurnal Manajemen Bandwidth Menggunakan Router Board Mikrotik,” J. Cendikia, vol. 12, no. 1, pp. 1–7, 2016.