Journal Sistem Informasi, dan Teknologi Informasi

Vol. 1, No2, Agustus 2022

https://journal-siti.org/index.php/siti/ Published By HPTAI

Penanganan Serangan Brute Force dan Port Scanning Pada Router Mikrotik

Deden Hardan Gutama[1], Adhien Kenya Anima Estetikha[2], Rahmad Arif Setiawan[3]

[1] Program Studi Informatika, Universitas Alma Ata Yogyakarta
[2,3] Program Studi Magister Teknik Informatika, Universitas Amikom Yogyakarta
Email: [1]hardan@almaata.ac.id, [2]kenyaakae@students.amikom.ac.id,
[3]rahmad.arif@students.amikom.ac.id

Abstract

Dalam menjaga integritas serta validitas data, kemanan pada jaringan sebuah instansi adalah salah satu urgensi yang harus diperhatikan. Agar dapat menjamin pelayanan yang selalu tersedia untuk para pengguna. Sistem yang digunakan untuk mendeteksi penyusup pada sebuah jaringan pada era 4.0 umumnya dapat melakukan pendeteksian dengan jenis yang beragam akan tetapi belum mampu melakukan tindakan perfentif, akan tetapi dari sisi penggunakan user sangat membutuhkan adanya teknologi informasi dan hal ini yang menjadi salah satu penyebab kasus keamanan pada sebuah jaringan meningkat setiap tahunnya dimana ini terjadi karena rendahnya keperdulian organisasi pada keamanan sebuah jaringan. Oleh karena itu dibutuhkan sebuah system yang mampu mempermudah administrator jaringan untuk memonitoring traffict jaringan dengan Intrusion Prevention System (IPS).

Keywords: Brute force, Port scanning, Mikrotik, IPS

1. PENGANTAR

Dalam sebuah organisasi yang mengguanakan jaringan computer, keamanan adalah salah satu hal yang wajib diperhatikan guna mempertahankan kualitas, validitas, dan integritas pada sebuah data juga dapat menjaga ketersediaan pelayanaan system untuk para pengguna. System pendeteksian dari para penyusup yang ada pada jaringan saat ini pada umumnya mampu melakukan pendeteksian serangan namun belum mampu untuk mengambil tindakan penanganan lebih jau .[4].

Jika kita menelisik sisi lain timbul problem lain yang dirasa cukup serius yaitu kemanan pada jaringan akan tetapi manusia sudah sangat bergantung dengan system. Masalah ini menyebabkan meningkatnya masalah masalah keamanan jaringan setiap tahunnya.

Pada era 4.0 saat ini teknologi telah berkembang semakin cepat, kebutuhan keamanan jaringanpun meningkat pula seiring majunya ilmu di bidang hacking dan

cracking. Telah banyak situs tempat belajar menjadi hacker dan open source sehingga mau tidak mau kita harus meningkatkan pula kemampuan dalam menangani masalah keamanan pada jaringan.

2. METODE

Langkah yang digunakan pada penelitian ini adalah pengumpulan data, konsep teori, dan perancangan system. System yang kami bangun memanfaatkan library dan source code yang ada pada github yang kemudian kami modifikasi sedikit agar memiliki perbedaan dengan pembangunan system terdahulu. Berikut uraian metode penelitian yang digunakan pada penelitian ini :

2.1 Pengumpulan Data

Pada bagian ini data dikumpulkan untuk digunakan sesuai tujuan yang telah ditetapkan oleh tim peneliti. Agar penelitian yang dilakukan tidak berubah haluan maka peneliti melakukan langkah langkah :

1.Analisis

Pada tahapan ini dilakukan analisis untuk melakukan analisis rancangan yang telah diciptakan, analisis proses dari serangan pada jaringan hingga pemberitahuan melalui email

2.Perancangan

Tahapan perancangan ini menerjemahkan kebutuhan yang telah didapat pada tahapan analisis menjadi sebuah perangkat lunak yang nantinya akan di implementasikan.

3.Pengujian

Pengujian ini menggunakan software guna memperoleh hasil yang baik.

4.Dokumentasi

Pada dokumentasi ini peneliti menjalani proses literature studi pustaka dengan membaca serta mempelajari berbagai buku acuan, dokumen, dan sumber lain yang masih ada kaitannya dengan penelitian ini

2.2 Dasar Teori

Teori-teori yang ada dipenelitian ini adalah :

2.2.1 Router

Menurut sofana router adalah peralatan jaringan yang dapat melakukan koneksi antara jaringan satu dengan jaringan lain. Secara eksplisit router memiliki kemiripan dengan bridge akan tetapi router memiliki kelebihan yang tidak dimiliki bridge yaitu lebbih cerdas. Router dapat memanajemen ip, subnet dan lain lain sedangkan bridge tidak dapat. Router sendiri bekerja dengan memanfaatkan tabel routing yang tersimpan di memori router tersebut guna menciptakan keputusan "kemana paket data akan dikirim" dan "router terbaik mana yang dapat mempersingkat waktu dalam pengiriman data" [16].

2.2.2 Firewall

Menurut Maiwald, firewall sendiri dapat di definisikan sebuah perangkat atau sistem aplikasi yang ada di sebuah jaringan yang berfungsi melakukan pemantauan pengiriman data, dan menolak lalulintas yang tidak dipercaya dengan tujuan agar jaringan selalu aman dari serangan-serangan hacker serta memberikan otorisasi lalulintas yang sudah dipercaya masuk ke jaringan. Firewall sendiri adalah benteng utama yang menjadi garda terdepan untuk melindungi jaringan dan paket data didalam jaringan tersebut [17].

Firewall memiliki posisi pada layer 3 dan layer 4 atau transport layer dari protokol 7 OSI layer. Layer 3 sendiri adalah layer yang menangani perihal penentuan alamat IP, sedangkan layer 4 sendiri bertugas menangani perihal port yang digunakan komunikasi apakah itu TCP atau port UDP.

Firewall atau IP filtering biasanya digunakan untuk mengontrol trafik yang masuk atau keluar (dari/atau ke sistem jaringan komputer internal). Umumnya IP Filtering atau firewall difungsikan untuk menangkal adanya serangan dari jaringan luar. Firewall sendiri dikembangkan dari hardanware, software, atau kombinasi dari software dan hardware yang dimana ada pada segmen jaringan yang berbeda serta memiliki tugas yaitu melakukan pemeriksaan traffict yang berjalan melewatinya sesuai dengan otorisasi yang ditentukan [18].

2.2.3 Protocol

Menurut Steinke adanya protokol agar komputer dapat saling berkomunikasi satu sama lain, komputer yang telah terhubung pada suatu jaringan wajib memiliki satu lingkup peraturan atau rules yang sama. Peraturan-peraturan tersebut, disebut dengan protokol.

Sebagai analogi, terdapat beberapa orang yang berkebangsaan berbeda satu sama lain, maka agar mereka dapat saling berkomunikasi satu dengan yang lainnya maka memerlukan seorang penerjemah atau mengguanakan salah satu bahasay yang familiar misalnya bahasa inggris. Oleh karena itu ada badan dunia yang menangani masalah protokol dari standarisasi dan prosedur didalamnya yaitu ISO (International Standardization Organization) dimana merekalah yang menciptakan aturan baku yang kemudian dinamakan dengan OSI (Open System Interconnection) [19].

2.2.4 Web Server

Pada umumnya web server berperan sebagai server yang memberikan layanan kepada komponen yang meminta informasi berkaitan dengan web, dalam web yang telah dirancang dalam internet. Menurut Sibero web server ialah komputer yang disusun sedemikian rupa dari beberapa hardware serta perangkat lunak [20]. Sedangkan Kustiyahningsih mengatakan web server ialah komputer yang berfungsi sebagai media penyimpanan dokumen atau data sebuah website, komputer tersebut mampu melayani request data website baik itu file maupun sourcode website itu sendiri dari klien yang melakukan request halaman website [21]. Jika kita lihat dari kedua penjelasan tersebut peneliti mengambil kesimpulan bahwa web server ialah komputer yang memiliki spesifikasi khusus yang berguna sebagai media menyimpan dokumen serta dapat melakukan akses serta request untuk menampilkan halaman web tersebut melalui komputer pengakses situs tersebut [6].

Server web, untuk berbicara dengan kliennya (browser internet) memiliki konvensi sendiri, lebih tepatnya HTTP (Hypertext Transfer Protocol) adalah konvensi jaringan lapisan aplikasi yang digunakan untuk kerangka kerja data yang sesuai dan kooperatif dan menggunakan hypermedia. Seperti yang ditunjukkan oleh Hidayatullah dan Kawistara, "Hypertext Transfer Protocol (HTTP) adalah konvensi sehingga klien dan server dapat berbicara dengan 10 gaya reaksi permintaan. HTTP memutuskan bagaimana pesan diatur dan cara sesuatu dikirim, serta bagaimana internet browser tanpa henti menanggapi perintah yang berbeda"[3]. Sementara itu, menurut Handoko, Aditya Irfan Puji, "Hypertext Transfer Protocol (HTTP) adalah konvensi jaringan lapisan aplikasi yang digunakan untuk kerangka data yang disebarluaskan, kooperatif, dan hypermedia. Berdasarkan hipotesis di atas, sangat mungkin beralasan. bahwa HTTP adalah konvensi jaringan lapisan aplikasi yang digunakan untuk kerangka kerja data yang diedarkan, kooperatif, dan hypermedia, di mana konvensi, misalnya, klien dan server dapat menyampaikan dalam gaya reaksi ajakan [2].

Normalisasi web server dalam penggunaan pemanfaatannya diberikan oleh W3C (World Wide Web Consortium), IETF (Internet Engineering Task Force), dan beberapa asosiasi yang berbeda. Sampai saat ini, lebih dari 110 rincian telah disampaikan oleh W3C (W3C Recommendations). [7]

Contoh normalisasi server web meliputi:
1. Detail HTML, CSS, DOM dan XHTML (W3C)
2. Spesifikasi Javascript (ECMA)

3.URL, HTTP (IETF) sebagai arsip RFC

2 2.5 Snort

Snort adalah ilustrasi program Sistem Deteksi Intrusi Berbasis Jaringan, yaitu program yang dapat mengenali upaya gangguan pada kerangka jaringan PC. Snort adalah open source dengan GNU General Purpose License sehingga produk ini dapat digunakan untuk mendapatkan kerangka kerja server tanpa membayar biaya izin.[8][9][10]

Kerangka kerja IDS harus lintas tahap, memiliki kesan kerangka kerja yang ringan, dan dirancang dengan mudah oleh para eksekutif kerangka kerja yang memerlukan pelaksanaan pengaturan keselamatan dalam kerangka waktu yang singkat. Eksekusi dapat berupa sekumpulan program yang dapat dihubungkan dalam melakukan gerakan untuk menjawab keadaan keamanan tertentu. Selain itu. Kerangka kerja IDS juga harus kuat dan cukup mudah beradaptasi untuk digunakan sebagai bagian yang sangat tahan lama dari kerangka kerja organisasi.

Snort memenuhi model-model ini, misalnya sangat baik dapat dirancang dan diizinkan untuk berjalan untuk periode yang diperluas tanpa memerlukan pengawasan atau dukungan manajerial sebagai fitur dari pengaturan keamanan terpadu dari kerangka kerja organisasi. Snort juga dapat berjalan di semua tahapan kerangka kerja di mana libpcap dapat berjalan. Sampai saat ini, Snort telah dicoba untuk dijalankan pada kerangka kerja RedHat Linux, Debian Linux, MkLinux, HP-UX, Solaris (x86 dan Sparc), x86 Free/Net/OpenBSD, Windows dan MacOS X.

2 2.6 Intrusion Prevention System

Interruption Prevention System (IPS) adalah metodologi yang dalam banyak kasus digunakan dalam kerangka keamanan PC, IPS mengkonsolidasikan prosedur firewall dan strategi Intrusion Detection System (IDS) dengan cukup baik. Inovasi ini dapat dimanfaatkan untuk mencegah serangan yang akan masuk ke jaringan tetangga dengan cara memeriksa dan merekam semua paket semua bundel dan mengenali bundel dengan sensor, ketika serangan telah dibedakan, IPS akan menolak akses (blok) dan log (log) semua yang dibedakan. bundel informasi. itu. Jadi IPS berperilaku seperti firewall yang akan mengizinkan dan menghalangi bergabung seperti IDS yang dapat mengidentifikasi paket secara menyeluruh. IPS menggunakan tanda untuk mengidentifikasi pergerakan lalu lintas pada organisasi

dan terminal, di mana identifikasi parsel yang mendekat dan aktif (inbound-outbound) dapat dicegah sesegera mungkin sebelum merusak atau mengakses jaringan lingkungan.[11][12]

2 2.7 Lapisan OSI (Interkoneksi Sistem Terbuka)

1. Lapisan Fisik
   Lapisan ini bertanggung jawab untuk memberdayakan dan menangani titik koneksi aktual organisasi PC. Pada lapisan ini, koneksi antara titik interaksi peralatan diawasi seperti koneksi antara DTE dan DCE. Antarmuka yang dicirikan pada lapisan ini meliputi: 10BaseT, 100BaseTX, V35, X.21 dan High Speed Serial Interface (HSSI).[13][14]
2. Lapisan DataLink
   Lapisan ini berhubungan dengan geografi organisasi, peringatan kesalahan dan kontrol aliran. Tugas mendasar dari lapisan antarmuka informasi adalah sebagai kantor transmisi informasi mentah dan mengubah informasi menjadi saluran yang terbebas dari kesalahan transmisi.
   Sebelum dikirim ke lapisan organisasi, lapisan antarmuka informasi menjalankan tugas ini dengan mengizinkan sumber untuk memecah informasi menjadi berbagai garis besar informasi (biasanya ratusan atau ribuan byte). Kemudian lapisan penghubung informasi mengomunikasikan selubung ini secara berurutan, dan memproses garis penegasan yang dikirim kembali oleh penerima.[15]
3. Network Layer
   Kemampuan lapisan network layer untuk mengontrol aktivitas subnet dengan mengirimkan bundel dimulai dengan satu hub kemudian ke hub berikutnya dalam organisasi. Masalah rencana yang signifikan adalah cara untuk memutuskan arah pengiriman bundel dari sumber ke tujuan.
4. Transport Layer
   Kemampuan penting dari lapisan kendaraan adalah untuk mendapatkan informasi dari lapisan pertemuan, memecah informasi menjadi potongan-potongan yang lebih sederhana jika penting, meneruskan informasi ke lapisan organisasi, dan menjamin bahwa setiap bit informasi muncul di sisi yang berlawanan. akurat. Demikian juga, hal-hal ini harus diselesaikan secara efektif, dan rencana untuk melindungi lapisan atas dari perubahan inovasi peralatan yang tak terhindarkan.
5. Session Layer

Lapisan pertemuan memungkinkan klien untuk mengatur pertemuan dengan klien yang berbeda. Lapisan ini membuka, mengawasi dan menutup pertemuan antar aplikasi.

6. Presentation Layer

Lapisan pertunjukan melakukan peran yang disebutkan secara spesifik untuk menjamin pengungkapan jawaban keseluruhan untuk masalah tertentu. Selain menawarkan kantor dukungan untuk transformasi informasi, perancangan dan enkripsi, show layer juga bekerja dengan ASCII, EBCDIC, JPEG, MPEG, TIFF, PICT, MIDI, dan catatan desain Quick Time.

9.Lapisan Aplikasi

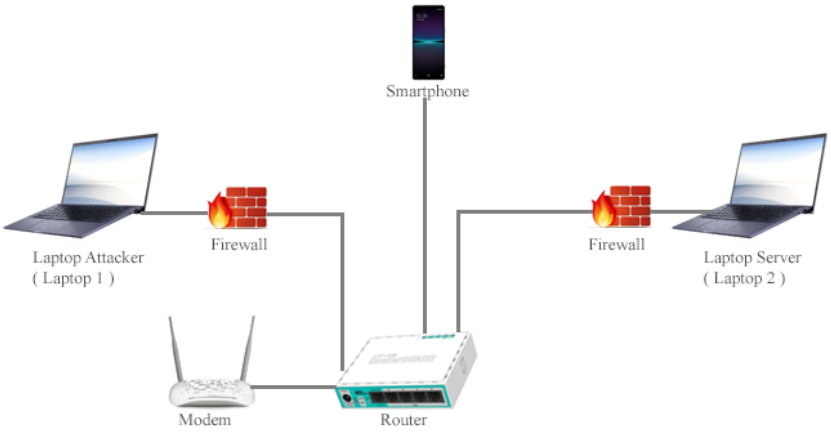
Lapisan ini bertanggung jawab untuk menawarkan kantor dukungan langsung kepada klien, sebagai aplikasi dan menyampaikan dari satu program ke program lainnya. Jika kita sedang mencari record dari document server untuk digunakan sebagai aplikasi word handling, maka pada saat itulah siklus ini mengatur layer ini. Demikian juga, dengan asumsi kita mengirim email, membaca web, berbicara, membuka rapat telnet, atau menjalankan FTP, maka banyak siklus ini diselesaikan pada lapisan ini.

2 2.8 Diagram Alir

Pada tahap ini, proses perbaikan flowchart selesai dengan memanfaatkan diagram-diagram yang memaknai suksesi metode program yang akan dirangkai. Flowchart ini akan memudahkan para software engineer untuk menangani masalah ke dalam baris kode [1].

2.3 *Perancangan Program*

Implementasi jaringan pada penelitian ini melibatkan dua buah laptop dimana laptop pertama diposisikan sebagai attacker yang menggunakan system operasi windows 10 sedangkan laptop kedua diposisikan sebagai server dengan menggunakan windos 10 dan winbox. Terdapat juga router TP-Link satu, modem TP-Link satu buah dan satu buah smartphone android yang digunakan untuk memberikan informasi serangan yang terjadi.



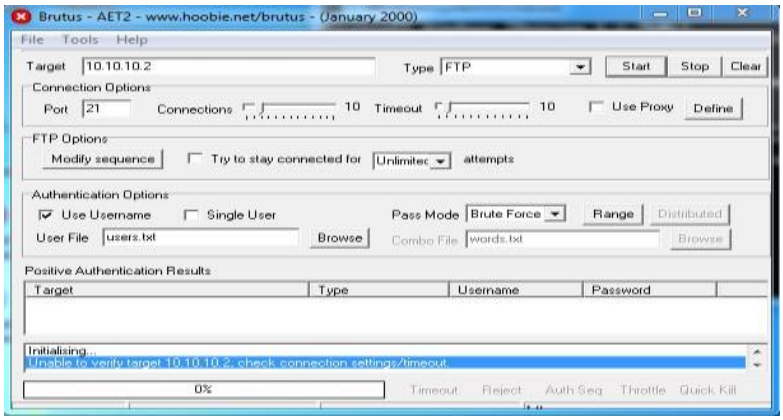
Gambar 1. Perancangan *Intrusion Prevention system*

Berdasarkan gambar 1 dapat kita lihat attacker berusaha mencoba melakukan penyerangan ip server dengan melakukan brute force yaitu berusaha memasukkan username juga password yang selanjuutnya server akan melakukan respon terhadap tersangan tersebut dan melakukan report melalui email. Tujuan mengapa terdapat report email adalah untuk memberi informasi kepada administrator jika ada upaya pembobolan menggunakan brutforce. Server juga mendapatkan report mengenai serangan yang dilakukan oleh attacker berupa layanan log.

3. HASIL DAN DISKUSI

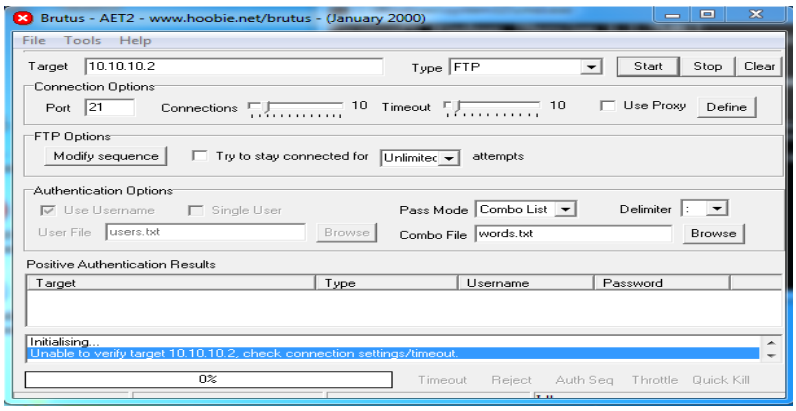
3.1 Pengujian Setelah Menerapkan IPS pada Server

Pengujian IPS pada mikrotik peneliti menggunakan pengujian dengan melakukan penyerangan brute force untuk membobol password, berikut tampilan software brutus yang digunakan untuk melakukan penyerangan :



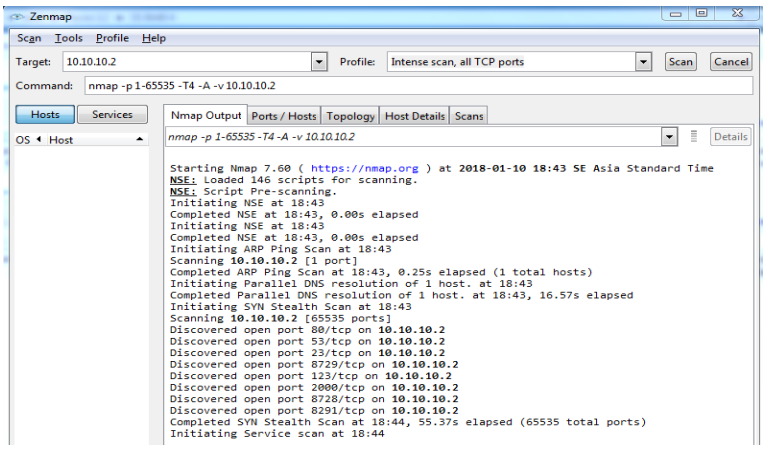
Gambar 2. Serangan *Brute force* dengan Brutus Berhasil Dicegah

Pada gambar 2 tersebut serangan brute force menggunakan software brutus aet, pada proses serangan ini brutus akan berusaha untuk login menggunakan database user radom dan pada tahapan ini IPS terbukti mampu melakukan pencegahan serangan ditunjukkan dengan keterangan "*Unable to verifity* 10.10.10.2, *check connection setting/time out*" yang artinya *intruder* mengalami timeout. Kemudian serangan kedua dilakukan ke server mikrotik, pada penelitian ini uji coba dilakukan dengan brute force pass mode = combo list.



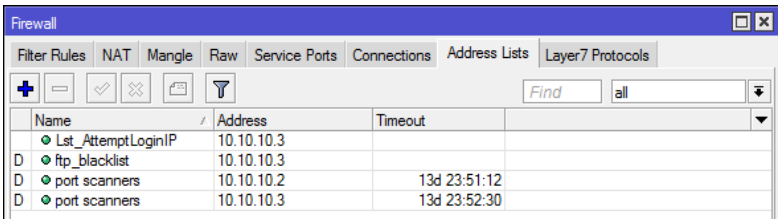
Gambar 4. Penyerangan dengan cara *Brute force Pass Mode = Combo List*

Serangan brute force pass mode = combo list tersebut dilakukan dengan software brutus aet. Selama proses penyerangan tersebut IPS melakukan pencegahan serangan dan dapat dilihat pada result terdapat keterangan "*Unable to verifity* 10.10.10.2, *check connection setting/ time out*" yang artinya intruder timeout. Setelah serangan brute force, peneliti melakukan serangkaian serangan kembali pada server mikrotik, tentunya serangan dilakukan setelah IPS berhasil diterapkan pada Mikrotik, serangan yang diluncurkan dengan mencoba melakukan port scanning dengan Zenmap, berikut hasil scanning port menggunakan zenmap :



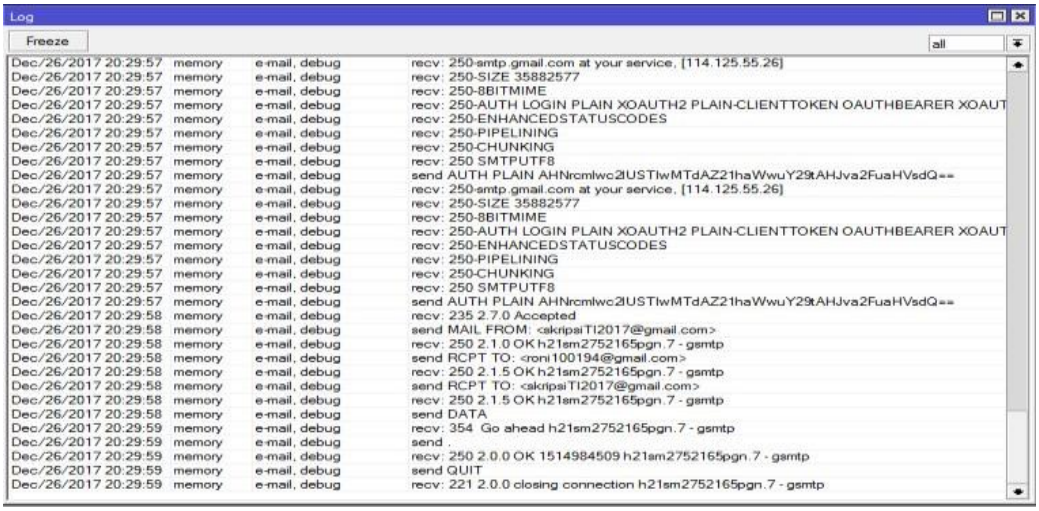
Gambar 5. Penyerangan *Port Scanning* telah dicegah

Penyerangan port scanning dengan zenmap dilakukan dengan laptop client satu dengan menggunakan IP target penyerangan 10.10.10.2, dapat kita lihat bahwa client satu sedang melancarkan serangan port scanning akan tetapi tidak dapat mendeteksi port 21 dikarenakan mikrotik telah menerapkan IPS.



Gambar 7. Tampilan *Address List* Pada *Firewall*

Berikut adalah tampilan *log* mikrotik setelah penerapan *IPS* :



Gambar 8. Tampilan *Log* Mikrotik Setelah Penerapan *IPS*

Gambar 8 diatas menampilkan rincian kegiatan mikrotik yang telah terjadi dimana pada 26 desember 2017 tidak ada lagi *login failure for user* admin *from* 10.10.10.3 via ftp.

Tabel 1. Perbandingan Sebelum dan Setelah Penerapan *IPS*

Action	**Sebelum Menerapkan IPS**		**Setelah Menerapkan IPS**	
Nama Aplikasi Penyerang	Zenmap	Brutus Aet	Zenmap	Brutus Aet
Jenis Penyerangan	Port Scanning	Brute force	Port Scanning	Brute force
Hasil Serangan	Port 21 Open	Password dan username berhasil didapatkan	Port 21 terfilter	Koneksi Timeout
Tampilan Log Mikrotik	-	Login Failur	-	-

Email Pemberitahuan Serangan	-	Send to Roni100194@gmail.com	-	-

Pada tabel diatas dapat kita lihat beberapa poin perbandingan nama aplikasi yang digunakan untuk penyerangan, hasil, dan notifikasi yang di kirim ke email.

4. KESIMPULAN

Serangan menggunakan brute force dan port scanning mampu dicegah oleh mikrotik menggunakan ntusion Prevention System(IPS), serangan yang dilancarkan akan terdeteksi sesuai dengan pola yang ada pada ruleIPS itu sendiri oleh karena itu filter rules pada perangkat yang menerapkan IPS harus dikelola dengan baik serta rules rutin dikembangkan. Kendati port scanning yang menggunakan Nmap dapat dicegah namun masih belum bisa maksimal dikarenakan IPS yang digunakan masih memerlukan minimal tiga kali serangan agar dapat mendeteksi serangan dari IP yang sama.

REFERENSI

[1] Gutama, Hardan. (2019). Perancangan Sistem Pelelangan Berita Berbasis Website. Indonesian Journal of Business Intelligence, (2), 40-46.

[2] Handoko, Aditya Irfan Puji. 2017. Prototipe Pengendalian Lampu Panggung. Menggunakan Web Browser Melalui Jaringan Lokal Berbasis Arduino

[3] Hidayatullah, Priyanto., Jauhari Khairul Kawistara.2014. Pemrograman WEB. Bandung : Informatika Bandung. (jQuery). Kadir, Abdul. 2014

[4] Arta, Y. (2017). Penerapan Metode Round Robin Pada Jaringan Multihoming Di Computer Cluster. *Information Technology Journal Research And Development*, *1*(2), 26-35.

[5] Ariyus, Doni., 2006, *Internet Firewall*, Graha Ilmu, Yogyakarta

[6] Yeni Kustiyahningsih, Devie Rosa Anamisa, 2011.Pemograman Basis Data. Berbasis Web Menggunakan PHP & MySQL.Graha Ilmu : Yogyakarta.

[7] Nurmiati, Evy., 2012, Analisi dan Perancangan Web Server Pada Handphone Vol.5, No.2

[8] Affandi, Mohammad., Setyowibowo Sigit., 2013, Impelementasi *Snort* Sebagai Alat Pendeteksi Intrusi Menggunakan Linux Vol.4, No.2

[9] Kurniawan, Adhitya., Putri, Nabilla, Sayyidah., Hermanto, Dedy., 2016, Impelementasi *Intrusion Prevention System (IPS)* Menggunakan *Snort,* IP *Tables,* dan *Honeypot* pada Router Mikrotik.

[10] Towidjojo, Rendra., 2016, Mikrotik Kungfu, Jasakom.com

[11] Suhartono, Didit., Riyanto, Dwi, Andi., Astomo, Widy, Yogi., 2015., *Intrusion Detection Prevention System (IDPS)* Pada *Local Area Network (LAN)* Vol.8, No.1

[12] Ariyadi, Tamsir., Kunang, Novaria, Yesi., Santi Rusmala., 2012., Impelementasi *Intrusion Prevention System (IPS)* Pada Jaringan Komputer Kampus B Universitas Bina Darma

[13] Syafrizal, Melwin., 2017, 7 *Layer Osi*, Yogyakarta

[14] Yugianto, Gin-Gin, Rachman, Oscar., 2012, Router Teknologi, Konsep, Konfigurasi, dan Troubleshooting, INFORMATIKA, Bandung

[15] Syukur, A. (2018). Analisis Management Bandwidth Menggunakan Metode Per Connection Queue (PCQ) dengan Authentikasi RADIUS. *IT Journal Research And Development, 2*(2), 78 - 89.

[16] Iwan Sofana, (2013), Teori dan Modul Praktikum Jaringan Komputer. Bandung, Indonesia: Modula.

[17] Maiwald, Eric. 2004. Fundamentals of Network Security. McGraw-Hill.

[18] Purbo, Onno W. 2006. Buku Pegangan Internet, Wireless dan Hotspot. Jakarta: Elex Media Komputindo.

[19] Steinke, S., Wehmeyer, L., et al. (2002a). The encc Energy Aware Compiler Homepage

[20] Alexander F.K Sibero. 2013. Web Programing Power Pack.mediaKom. Yokyakarta

[21] Yeni Kustiyahningsih, Devie Rosa Anamisa, 2011.Pemograman Basis Data. Berbasis Web Menggunakan PHP & MySQL.Graha Ilmu : Yogyakarta.

[22] Hidayatullah, Priyanto., Jauhari Khairul Kawistara.2014. Pemrograman WEB. Bandung : Informatika Bandung. (jQuery). Kadir, Abdul. 2014