PERANCANGAN KEAMANAN JARINGAN KOMPUTER MENGGUNAKAN *FIREWALL INTRUSION DETECTION SYSTEM* (IDS) TERHADAP SERANGAN *BRUTE FORCE* DAN IMPLEMENTASI ARP *LIST*

S.A. Puntadheva[1], Rr.Y.R. Kusumaningsih [2], J. Triyono[3]

Jurusan Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: stefanusarya872@gmail.com[1], yuliana@akprind.ac.id[2] , jack@akprind.ac.id[3]

Abstract

The urgency of good and sufficient internet security is needed in working activities so that the users could relish a safe and stable internet connection. Therefore, this research aimed to apply an internet security system so that the users could use the internet network maximally. The method used to the internet system security used brute force- and ARP list-based security system. Based on the several tests, it was needed four seconds to detect and to block the client's IP conducting the brute force attacks against the microtic routers whereas ARP list implementation restricted login access to the microtic routers for the IP that was not in the ARP list needed less than four seconds.
Keywords: *Brute Force, ARP list*, *security system.*

Abstrak

Pentingnya keamanan jaringan internet yang baik dan memadai sangat diperlukan dalam pekerjaan yang dilakukan supaya para pengguna dapat menikmati koneksi internet yang aman dan stabil. Penelitian ini bertujuan untuk menerapkan sistem keamanan jaringan agar setiap user dapat menggunakan jaringan internet secara maksimal. Metode yang digunakan dalam penelitian ini adalah dengan menggunakan sistem keamanan brute force dan ARP list. Berdasarkan hasil dari beberapa kali pengujian dibutuhkan waktu empat detik untuk mendeteksi dan memblokir IP dari client yang melakukan serangan brute force ke router mikrotik sedangkan implementasi ARP list yang membatasi akses login ke router mikrotik untuk IP yang tidak ada dalam ARP list membutuhkan waktu kurang dari empat detik.

Kata kunci: *Brute Force*, ARP *list*, sistem keamanan.

Pendahuluan

Teknologi komunikasi berkembang dengan cepat. Hal tersebut selaras dengan perubahan karakteristik masyarakat modern yang memiliki mobilitas tinggi, mencari layanan yang fleksibel dan mudah, dan mengejar efisiensi di segala bidang. Di PT. Primadaya sudah memanfaatkan jaringan internet sebagai penunjang aktivitas kegiatan sehari-hari pegawai yang ada. Namun belum terdapat keamanan jaringan komputer sedangkan pada zaman sekarang banyak serangan dari luar yang dapat mengancam keamanan jaringan.

Keamanan Jaringan komputer merupakan salah satu hal penting dan mendasar dalam pemanfaatan sebuah sistem. *Vulnerability* dalam sebuah sistem jaringan komputer seringkali dikesampingkan, hingga apabila terjadi suatu ancaman atau serangan *logic* maupun *physic* yang merusak pada sistem tersebut [1]. *Intrusion Detection System* (IDS) adalah sebuah aplikasi perangkat lunak ataupun perangkat keras yang dapat mendeteksi aktifitas yang mencurigakan dalam sebuah sistem atau jaringan. IDS dapat melakukan inspeksi terhadap lalu lintas *inbound* dan *outbound* dalam sebuah sistem atau jaringan, melakukan analisis dan mencari bukti dari percobaan penyusupan [2]. *Bruteforce* merupakan salah satu gangguan keamanan jaringan berupa usaha mendapatkan hak akses router secara paksa dengan mencoba berbagai *password* sehingga dapat menjadi berbahaya jika mendapatkan hak akses ke router tersebut. Selain ancaman keamanan jaringan *brute force*, pembatasan hak akses juga perlu ditingkatkan untuk mencegah orang yang tidak bertanggungjawab agar tidak masuk kedalam router. Penelitian mengenai IDS telah dilakukan oleh beberapa penelitian sebelumnya.

Achmad dan Siti, telah melakukan implementasi IDS pada keamanan PC server terhadap serangan *flooding data* dengan hasil penelitian tersebut membuktikan bahwa *traffic* pada sebuah jaringan komputer dapat dipantau melalui sebuah komputer dan jika terjadi masalah dapat lansgung diketahui oleh IDS tersebut [3], sedangkan Sutarti membahas bahwa metode penyerangan IDS *snort* mampu mendeteksi adanya serangan seperti *Ping of Death* dan *Port Scan*, *log* yang dihasilkan dapat membaca suatu serangan dan penyalahgunaan jaringan sesuai dengan metode pengujiannya dengan mengatur bagian *rule* dari *snort* [4]. Sedangkan penelitian terkait serangan *brute force* juga telah dilakukan oleh Gunawan. Pada penelitian ini tertulis algoritma *brute force* dapat melakukan serangkaian serangan dengan menggunakan penerkaan kombinasi kunci yang sangat sederhana serta melakukan pembajakan dan pencarian kode secara acak dengan cara yang jelas dan lempang [5]. Penelitian ini membahas bagaimana merancang keamanan jaringan pada router terhadap serangan *brute force* dengan menggunakan *firewall* IDS yang terdapat dalam router mikrotik. Dengan mengaktifkan *firewall* IDS dan membuat *rules* menyesuaikan dengan kebutuhan keamanan jaringan maka dapat mendeteksi dan mengatasi serangan *brute force*. ARP (*Address Resolution Protocol*) adalah protokol yang berfungsi untuk memetakan alamat IP ke alamat MAC.

ARP merupakan protokol yang penting pada komunikasi jaringan LAN terutama menggunakan ethernet sebuah *frame* ethernet memerlukan alamat fisik tujuan agar berhasil dikirimkan. Proses resolusi alamat yang dilakukan oleh ARP dalam jaringan berlangsung sangat cepat dan tidak terlihat sehingga sulit untuk diamati [6]. Firewall adalah suatu sistem yang dirancang untuk mencegah akses yang tidak diinginkan dari atau ke dalam suatu jaringan internal. *Firewall* bekerja dengan cara melacak dan mengendalikan jalannya data serta memutuskan aksi untuk melewatkan (*pass*), menjatuhkan (*drop*), menolak (*reject*), mengenkripsi atau melakukan pencatatan aktifitas (*log*) data. *Firewall* menjamin agar data sesuai dengan aturan (*rule*) yang terdapat di dalam kebijakan keamanannya (*security policy*) yaitu seperangkat aturan yang telah didefinisikan di dalam keamanan jaringan internal. Umumnya, sebuah *firewall* digunakan untuk membatasi atau mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini istilah *firewall* menjadi istilah lazim yang merujuk pada sistem yang mengatur komunikasi antar dua macam jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan juga tentu saja jaringan berbadan hukum di dalamnya, maka perlindungan terhadap perangkat digital perusahaan tersebut dari serangan para peretas, permata-mata, ataupun pencuri data lainnya, menjadi kenyataan. Istilah *firewall* berasal dari dunia arsitektur bata-dan-mortir. Di bangunan, firewall adalah dinding yang dibangun dari bahan tahan panas atau api seperti beton yang dimaksudkan untuk memperlambat penyebaran api melalui suatu struktur. Dalam dengan cara yang sama, pada jaringan firewall dimaksudkan untuk menghentikan lalu lintas yang tidak sah dari bepergian dari satu jaringan ke jaringan lainnya. Penyebaran firewall yang paling umum terjadi antara jaringan tepercaya dan yang tidak tepercaya, biasanya internet [7].

Metodologi Penelitian

Pengambilan data dilakukan dengan cara metode observasi dan studi kepustakaan. Metode Observasi, yakni dengan melakukan pengamatan dan proses perbandingan terhadap rancangan desain dan sistem keamanan jaringan. Dari metode ini diperoleh ruangan Kantor PT. Primadaya, kebutuhan spot jaringan di masing-masing ruangan, jumlah perangkat yang akan terhubung. Sedangkan Metode Studi Kepustakaan, yakni dengan melakukan pengumpulan data dan referensi atau buku acuan yang berkaitan dengan sistem keamanan jaringan. Diperoleh data tentang analisis jaringan komputer, perancangan sistem keamanan jaringan, dan metode Pendekatan Kuantitatif yang digunakan pada sistem keamanan jaringan.

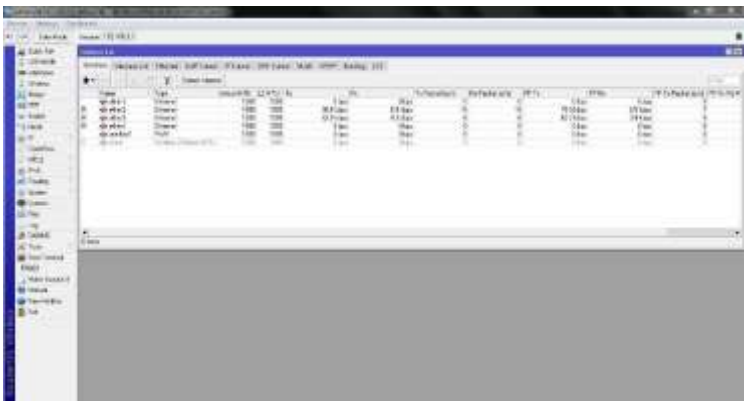
Analisis terhadap keamanan jaringan yang telah dikonfigurasi dilakukan dengan menggunakan metode pendekatan kuantitatif. Metode kuantitatif yang akan digunakan untuk mengukur seberapa cepat respon sistem keamanan IDS dalam mendeteksi dan mengatasi ancaman yang berupa *brute force*.

Pada uji coba sistem keamanan *firewall* ini pengujian dilakukan beberapa kali uji coba. Pada beberapa kali uji coba tersebut akan dibagi menjadi uji coba sebelum diaktifkan *rule* pada *firewall* untuk sistem keamanan *brute force* dan sesudah diaktifkan *rule* pada *firewall* untuk sistem keamanan *brute force*. Hasil yang diperoleh akan memberikan simpulan terhadap objek yang diuji.

Hasil dan Pembahasan

Pengujian dilakukan dengan cara *login* ke router mikrotik menggunakan *winbox*, tanpa mengaktifkan *firewall rules* yang terdapat dalam router mikrotik *client* yang mencoba login akan bisa tetap masuk melalui *winbox* walaupun melakukan percobaan *login* sebanyak apapun. Pengujian dapat dilihat pada gambar 1 dan 2.

Gambar 1. Percobaan login melalui *winbox*



Gambar 2. Tampilan pertama setelah *login winbox*

Setelah mengaktifkan *firewall rules client* yang mencoba *login* hanya dapat melakukan percobaan sesuai dengan batas yang ditentukan oleh *firewall rules*, jika melakukan percobaan lebih dari batas yang ditentukan maka IP dari *client* tersebut akan masuk ke dalam *list* yang telah dibuat dan secara otomatis akan diblokir oleh *rules drop* yang terdapat dalam *firewall rules*.

Gambar 3.Tampilan login saat IP diblokir

Saat mulai mengalami kendala berupa proses *connecting* yang lama, ada proses yang berjalan di dalam *firewall rules*. Proses tersebut berupa *packets* dalam *rules* lain yang juga berjalan menandakan IP yang melakukan percobaan *login* mulai dicurigai melakukan serangan *brute force* dan langsung dimasukkan ke dalam *list* yang terdapat dalam *firewall rules* kemudian akan langsung diblokir oleh *rules drop*.

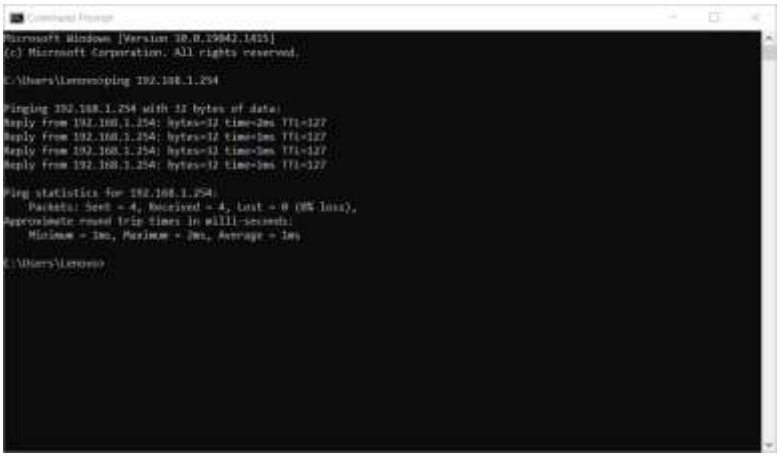
Gambar 4. Tampilan firewall rules saat proses memblokir IP

Berdasarkan hasil pengujian serangan *brute force* dengan menerapkan metode sistem keamanan *firewall* IDS terhadap router mikrotik dan dilakukan dengan beberapa kali serangan mendapatkan hasil seperti pada tabel 1.

Tabel 1. Hasil Pengujian *firewall* IDS

Serangan	Hasil
Brute force sederhana	➢ Pada saat tidak menggunakan *firewall* IDS *client* yang melakukan *brute force* tetap dapat mengakses router jika sudah dapat *login* ke melalui winbox. ➢ Pada saat *firewall* IDS diaktifkan *client* yang melakukan serangan *brute force* tidak dapat mengakses router jika telah melewati batas percobaan dan IP yang digunakan terblokir otomatis.
Brute force dictionary	➢ *Client* yang melakukan serangan *brute force* saat *firewall* IDS diaktifkan tidak dapat *login* ke router melalui winbox dan IP yang digunakan langsung terblokir. ➢ *Client* yang melakukan serangan *brute force* saat *firewall* IDS tidak aktif tetap dapat *login* ke router walau melebihi batas percobaan *login*.
Brute force hybrid	➢ Sebelum *firewall* IDS diaktifkan IP dari *client* yang melakukan serangan *brute force* tidak tercatat dalam *blacklist* yang telah dibuat dan tetap dapat masuk ke dalam router melalui winbox. ➢ Sesudah *firewall* IDS diaktifkan *client* yang melakukan serangan *brute force* tidak dapat *login* ke dalam router mikrotik jika sudah melebihi batas percobaan dan IP yang digunakan akan diblokir dalam jangka waktu yang ditentukan.

Penerapan sistem keamanan ARP *list* digunakan untuk membatasi *client* yang dapat mengakses router mikrotik. Pengujian ARP *list* dilakukan dengan uji coba *ping test* ke *client* dalam satu jaringan yang sama jika mendapat *reply* berarti *client* sudah terhubung dan dapat berkomunikasi dalam jaringan tersebut. Karena IP yang dapat terkoneksi dalam jaringan hanya IP yang terdapat dalam ARP *list* sekalipun perangkat lain mendapat IP dari router namun jika tidak termasuk dalam ARP *list* tetap tidak akan dapat terkoneksi. Pengujian *ping* ini dapat dilihat pada gambar 5.



Gambar 5. Pengujian ping ke client dalam satu jaringan

Kesimpulan

Hasil dari perancangan keamanan jaringan yang ada di PT. Primadaya menggunakan *cisco packet tracer* sebagai *software* untuk membuat desain dari rancangan jaringan tersebut dan *firewall* IDS sebagai sistem keamanan jaringan, *firewall* IDS sebagai sistem keamanan cukup efektif karena dapat mendeteksi sekaligus mengatasi masalah yang terjadi pada router mikrotik sesuai dengan konfigurasinya. Sistem keamanan yang digunakan kali ini untuk mendeteksi dan mengatasi serangan *brute force* ke router mikrotik, pada saat terjadi serangan *brute force firewall* IDS langsung mendeteksi adanya indikasi serangan *brute force* dan langsung melakukan protokol keamanan sesuai dengan *rules* yang telah dikonfigurasi. Implementasi ARP *list* pada jaringan ini digunakan untuk membatasi *client* yang dapat mengakses router dengan cara menentukan IP melalui ARP *list* sehingga *client* yang akan masuk ke jaringan hanya dapat menggunakan IP tersebut, jika menggunakan IP dari luar atau menggunakan IP yang tidak sesuai dengan yang ada dalam ARP *list* maka *client* tidak akan dapat terhubung ke dalam jaringan.

Berdasarkan hasil pengujian penerapan sistem keamanan *brute force* pada jaringan mikrotik dapat merespon dengan baik ketika ada indikasi serangan *brute force* ke router mikrotik yang ditandai dengan berjalannya *rules* yang terdapat dalam *firewall* IDS dan proses yang lama saat mencoba *login* dari sisi *client* yang melakukan serangan *brute force*. Respon dari sistem keamanan yaitu memblokir IP yang dicurigai melakukan serangan *brute force* karena melakukan percobaan *login* melebihi batas yang telah ditentukan sehingga IP tersebut masuk ke dalam *address list* dan tidak dapat digunakan selama batas waktu yang telah ditentukan. Hasil dari beberapa kali pengujian dibutuhkan waktu 4 detik untuk memblokir IP yang melakukan serangan *brute force* ke router mikrotik, sedangkan implementasi ARP *list* yang membatasi *client* untuk mengakses router juga dapat dengan cepat membatasi IP yang akan terhubung ke dalam jaringan, sehingga IP yang tidak dikenal atau tidak ada dalam ARP *list* tidak akan dapat terhubung walaupun menggunakan IP yang sekiranya masih dalam satu jaringan.

Daftar Pustaka

[1] J. E. Canavan, Fundamentals of Networks Security, Massachusets: ARTECH HOUSE, INC, 2001.

[2] Y. Arta, “Implementasi Intrusion Detection System Pada Rule Based System Menggunakan Sniffer Mode Pada Jaringan Lokal,” *IT Journal Research and Development,* vol. 2 No. 1, pp. 43-50, 2017.

[3] A. dan S. , “Implementasi Intrusion Detection System (IDS) Pada Keamanan PC Server Terhadap Serangan Flooding Data,” *Sainstech,* vol. 28 No.1, 2018.

[4] . S. . P. . A. P. . S. dan F. Isnanto, “Implementasi IDS (Intrusion Detection System) Pada SIstem Keamanan Jaringan SMAN 1 Cikeusal,” *Jurnal PROSISKO,* vol. 5 No. 1, 2018.

[5] G. Indra, “Modifikasi Keamanan File dengan Algoritma Hill Chiper Untuk Mengantisipasi Dari Serangan Brute Force,” *TECHSI,* vol. 11 No. 2, 2019.

[6] B. A. Forouzan, TCP/IP Protocol Suite, New York: Tata Mcgraw Hill, 2010.

[7] . V. Osipov, M. Sweeney dan . W. Weaver, Cisco Security Specialist's Guide To PIX Firewall, Massachusets: Syngress Publishing, Inc, 2002.