Keamanan Jaringan *Hotspot* Dengan *Simple Port Knocking* dan *Automated Backup* Menggunakan Mikrotik

Sigit Setyowibowo, Sujito dan Nirwan Moka

Teknologi Informasi, STMIK PPKIA Pradnya Paramita
Jl. L.A. Sucipto 249A Kota Malang
E-mail: sigit@stimata.ac.id, sujito@stimata.ac.id, alorampera@gmail.com

Abstrak

Kebutuhan internet yang tinggi di SMK Cakra Kusuma Jombang tidak diimbangi dengan sistem keamanan yang baik. Beberapa serangan yang digunakan antara lain *brute force*. Serangan *brute force* pada mikrotik mengakibatkan internet menjadi tidak stabil karena penyerang dapat mengubah konfigurasi mikrotik. Keamanan admin jaringan menjadi penting sebab admin merupakan *user* yang mengelola jaringan sekolah. *Simple port knocking* merupakan sebuah solusi bilamana terjadi serangan pihak luar yang ingin masuk lewat port mikrotik dengan *brute force*. Hasil pengujian dapat dilihat perbedaan tingkat keamanan dari serangan *brute force*. Dengan menerapkan *simple port knocking* dapat mencegah serangan *brute force* pada admin mikrotik. Walaupun dengan memasukkan *username* dan *password* yang benar tidak dapat masuk mikrotik karena ada *rule port* yang ada pada keamanan *simple port knocking*. Dengan *automated backup* sekolah tidak perlu lagi mendatangkan teknisi bila terjadi *error* pada mikrotik karena *backup* konfigurasi bisa digunakan untuk mengembalikan konfigurasi mikrotik

Kata kunci: Keamanan, *Automated Backup*, *Simple Port Knockin*g, Mikrotik.

Pendahuluan

SMK Cakra Kusuma Jombang adalah salah satu sekolah swasta yang berada di Jombang yang berdiri di bawah naungan Yayasan Sunan Pekik, beroperasi pada tahun 2015 bergerak di bidang pendidikan dengan satu jurusan yaitu Multimedia. Siswa dan guru di sekolah tersebut memanfaatkan fasilitas sekolah untuk menunjang pendidikan. Fasilitas yang ada adalah akses internet di lingkungan sekolah serta 1 laboratorium komputer. Pemakai internet yang mencapai angka 82 *client* diantaranya 60 siswa serta 17 guru dan 5 staff dengan *bandwidth* yang tersedia 10 MBps *dedicated*. Topologi jaringan yang digunakan adalah dengan menempatkan 1 *acces point* untuk 3 kelas sehingga semua kelas dapat terhubung dengan internet.

SMK Cakra Kusuma Jombang menggunakan jaringan intranet dan internet. Untuk jaringan intranet digunakan pada laboratorium komputer dan jaringan internet yang digunakan adalah jaringan *hotspot*. *Hotspot* sendiri merupakan area dimana seseorang atau *client* dapat terhubung dengan internet secara *wireless* atau tanpa kabel. Manajemen *bandwidth* selama ini menggunakan mikrotik karena fitur yang tersedia sudah sangat memadai. Manajemen *bandwidth* yang digunakan *simple queue* yang dibagi menjadi 3 *user* profil yaitu profil siswa, profil guru serta profil untuk admin. Selama ini untuk proses maintenance di lakukan oleh admin sekolah.

Pemanfaatan layanan internet tersebut digunakan untuk *browsing*, *download* dan *social media*. Kebutuhan internet yang tinggi di SMK Cakra Kusuma Jombang tidak diimbangi dengan sistem keamanan yang baik. Serangan ke mikrotik dilakukan pada admin mikrotik. Beberapa serangan yang digunakan antara lain *brute force*. Serangan *brute force* pada mikrotik mengakibatkan internet menjadi tidak stabil karena penyerang dapat mengubah konfigurasi mikrotik. Keamanan admin jaringan menjadi penting sebab admin merupakan user yang mengelola jaringan sekolah.

Menurut [1] *brute force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang bertujuan untuk memeriksa secara sistematis semua kemungkinan rahasia sampai yang benar ditemukan. Seringkali penyerang memasuki *port* di *server* dahulu dan penyerang melakukan *brute force* untuk mengetahui *username*

DOI : http://dx.doi.org/10.32409/jikstik.21.4.3109

dan *password* admin, penyerang memasuki *port* seringkali memanfaatkan kelemahan dari *firewall server* mikrotik. Salah satu cara yang digunakan adalah *simple port knocking*.

Simple port knocking merupakan sebuah solusi bilamana terjadi serangan pihak luar yang ingin masuk lewat *port* mikrotik dengan *brute force*. *Simple port knocking* merupakan metode membangun koneksi ke komputer jaringan yang tidak memiliki *port* terbuka pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu atau otentikasi mekanisme sistem *firewall* untuk membuka *port* secara dinamis kepada pihak-pihak yang diautentikasi saja [2]. Koneksi bisa berupa *Transmission Control Protocol* (TCP), *User Datagram Protocol* (UDP) maupuan *Internet Control Message Protocol (ICMP)*. Jika koneksi yang dikirimkan oleh *host* tersebut diotentikasi dan sudah sesuai dengan *rule knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan otorisasi ke *port* yang sudah ditolak. Selain itu bilamana terjadi *error* ataupun kerusakan pada mikrotik admin selalu *setting* ulang mikrotik. Sehingga perlu dibuatkan *automated backup* karena dengan adanya itu admin tidak perlu kerja dua kali untuk *setting* ulang mikrotik karena *backup* bisa diambil melalui email.

Jaringan Komputer

Jaringan komputer adalah interkoneksi antara dua komputer atau lebih yang terhubung satu sama lain melalui media transmisi yaitu dengan menggunakan kabel atau tanpa kabel yang biasa disebut dengan *wireless*. Pengertian interkoneksi adalah dua komputer yang terhubung dikatakan terhubung jika saling bertukar data atau informasi, berbagi sumber daya, seperti file, printer, dan media penyimpanan. Dalam jaringan komputer, komputer dapat memberikan layanan atau meminta layanan. Komputer yang memberikan layanan disebut komputer *server*, sedangkan komputer yang meminta layanan disebut komputer *klien* [3].

Internet

Internet merupakan jaringan dari jaringan komputer (*interconnected network*) di mana internet dapat digambarkan sebagai sebuah kota elektronik yang sangat besar di mana setiap penduduk memiliki alamat (Internet & e-mail *address*) yang dapat digunakan untuk berkirim informasi atau surat [4]. Internet telah dikembangkan, berevolusi, dan juga digunakan oleh banyak sekali kegiatan positifnya, misalnya dengan berinovasi dalam berbagi informasi dan edukasi, membantu kita dalam bidang kesehatan dan medis, atau beberapa inovasi lainnya yang tidak bisa disebutkan satu persatu. Namun di sisi lain, internet juga dapat disalahgunakan untuk melakukan aktivitas negatif atau ilegal, seperti peretasan dan serangan ilegal, penyebaran *malware* atau penipuan, situs pornografi, narkotika dan transaksi ilegal lainnya, dan banyak lagi.

Mikrotik

Sistem operasi (OS) Router MikroTik adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk mengubah komputer menjadi router jaringan yang andal, mencakup berbagai fitur yang dibuat untuk jaringan *Internet Protocol* (IP) dan jaringan nirkabel, cocok untuk digunakan oleh Penyedia Layanan Internet (ISP) dan penyedia *hotspot* (mikrotik Indonesia). MikroTik Router OS, adalah sistem operasi berbasis Linux yang ditujukan sebagai sistem router jaringan. Dirancang untuk memberikan kemudahan bagi penggunanya. Administrasi dapat dilakukan melalui Aplikasi Windows (WinBox). Selain itu, instalasi dapat dilakukan pada *Personal Computer* Standar (PC) untuk digunakan sebagai *router proxy* tidak memerlukan *resource* yang cukup besar untuk penggunaan standar, misalnya bertindak sebagai *gateway*. Untuk keperluan beban besar (jaringan kompleks, perutean kompleks) disarankan untuk mempertimbangkan pemilihan sumber daya PC yang memadai [5].

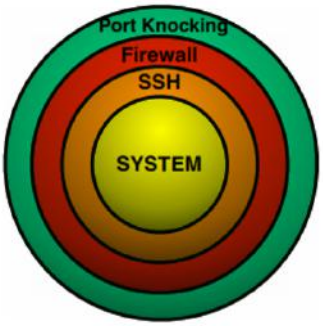
Simple Port Knocking

Penelitian [2] yang berjudul *Simple port knocking method*: *Against TCP replay attack and port scanning* menjelaskan bahwa *Port knocking* adalah teknik pertama yang diperkenalkan untuk mencegah penyerang menemukan dan mengeksploitasi layanan yang berpotensi rentan pada *host* jaringan, memungkinkan pengguna yang diautentikasi untuk mengakses layanan ini. Meskipun merupakan alat yang berguna, ia menderita berbagai kerentanan seperti pemutaran ulang TCP, pemindaian *port*, dll. Metode kinerja mengusulkan dengan mengukur waktu otentikasi untuk mengetuk *server*. Hasilnya, metode yang diusulkan bekerja lebih cepat daripada metode lain seperti *port knocking* dasar dan Fwknop + SPA. Ini menunjukkan bahwa metode yang diusulkan sederhana dan pada saat yang sama melawan serangan *replay* TCP dan pemindaian *port*.

Port knocking adalah metode yang dikembangkan oleh [6] untuk mem-*bypass* langkah-langkah keamanan yang digunakan oleh *firewall* untuk membangun koneksi antar *server*. Metode ini akan membangun komunikasi *host-to-host* di lingkungan *port* tertutup.

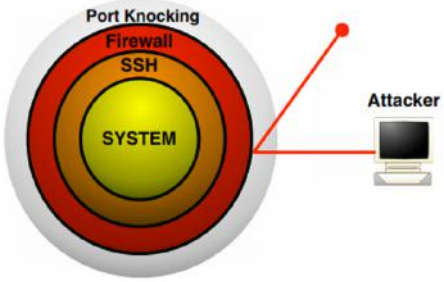
Awalnya, tujuan utama dari *port knocking* adalah untuk memberikan lapisan keamanan ekstra dengan menyediakan otentikasi dengan manfaat tambahan dari penyembunyian. Namun, *port knocking* sendiri menderita beberapa kerentanan seperti serangan *replay* TCP, Pemindaian *port*, ketidakjelasan keamanan, dan pengiriman paket yang rusak karena latensi jaringan.

Port knocking adalah sistem keamanan yang dapat melakukan fungsi memblokir akses yang tidak diinginkan. Pada prinsipnya *port knocking* berhasil menutup semua *port* yang ada di *server*. Jika pengguna membutuhkan akses ke *server*, pengguna melakukan "*tap*" untuk menggunakan layanan, kemudian jika pengguna selesai mengakses *port* ditutup kembali. Gambar 1 di bawah ini menggambarkan bagaimana sistem yang menjalankan SSH (*Secure Shell*) dapat dilindungi menggunakan *port knocking layer* [7].



Gambar 1: port knocking layer

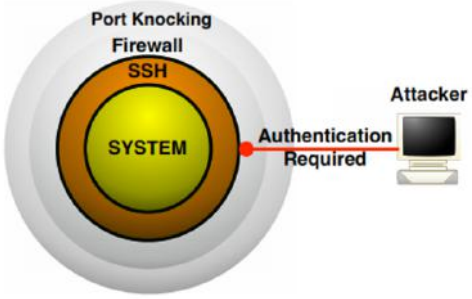
Gambar 2 menggambarkan situasi di mana *daemon port knocking* gagal 'dengan aman'. *Firewall* tetap tertutup, artinya tidak ada yang dapat terhubung ke layanan apa pun.



Gambar 2: *Port knocking* Gagal dengan Aman - semua *port* ditutup

Gambar 3, adalah 'gagal terbuka'. Situasi ini dapat terjadi, misalnya, jika pengguna mengetuk untuk membuka *port*, dan *daemon* pengetuk *port* gagal sehingga *port* tidak ditutup secara otomatis sebagaimana mestinya.

Refensi [8] *Port knocking* adalah bentuk komunikasi *host-to-host* yang bergantung pada upaya koneksi TCP yang sengaja gagal. Informasi dikodekan ke dalam urutan *port*. Klien mencoba untuk memulai beberapa jabat tangan tiga arah dan tidak menerima balasan. Upaya koneksi ini dipantau oleh *daemon* yang menafsirkan nomor *port* tujuan mereka sebagai data. Mekanisme ini memiliki kerentanan yang dapat dieksploitasi oleh peretas dengan bantuan data yang diendus dari jaringan. Melalui sinkronisasi, kerentanan ini dapat diminimalkan. Urutan tap kurang rentan terhadap replay dan serangan *brute force* jika umurnya lebih pendek.



Gambar 3: Port Knocking Fails Open

WinBox

Winbox adalah *software* atau utilitas yang digunakan untuk mentransfer *proxy server* dari jarak jauh ke mode GUI (*Graphical User Interface*) melalui sistem operasi Windows. Jika untuk mengkonfigurasi *proxy* dalam mode teks atau CLI (*Command Line Interface*) melalui PC itu sendiri, maka untuk mode GUI yang menggunakan Winbox kami mengkonfigurasi *proxy* melalui komputer klien. Konfigurasi *proxy* melalui *winbox* lebih banyak digunakan karena selain penggunaannya yang mudah dan sederhana, kita juga tidak harus menghafal perintah *console* [9].

Brute Force

Serangan *brute force SSH* adalah salah satu serangan paling umum di jaringan komputer. Serangan ini ditujukan untuk mendapatkan akses tanpa syarat ke akun pengguna dengan mencoba banyak kombinasi kata sandi yang berbeda. Deteksi jenis serangan ini di tingkat jaringan dapat mengatasi masalah skalabilitas metode deteksi berbasis host.

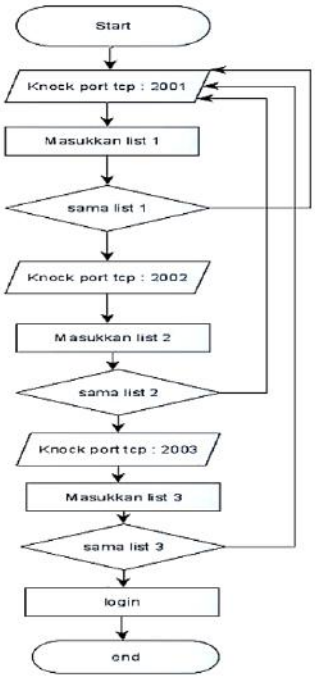
Penelitian yang dilakukan [10] melakukan pendekatan pembelajaran mesin untuk mendeteksi serangan *brute force* SSH di tingkat jaringan. Karena mengekstrak fitur diskriminatif untuk tugas pembelajaran mesin apa pun adalah langkah mendasar, kami menjelaskan proses mengekstrak fitur diskriminatif untuk mendeteksi serangan *brute force*. Kami menggabungkan pengetahuan domain tentang serangan *brute force* SSH serta analisis kumpulan data representatif untuk menentukan fitur. Kami mengumpulkan lalu lintas SSH nyata dari jaringan kampus. Kami juga menghasilkan beberapa data *login* yang gagal yang dapat dihasilkan oleh pengguna yang sah yang lupa kata sandi mereka sebagai lalu lintas normal yang mirip dengan lalu lintas serangan *brute force* SSH.

Pemeriksaan kami terhadap data *brute force Netflow* yang dikumpulkan dan data *login* gagal SSH yang dihasilkan secara manual menunjukkan bahwa fitur *Netflow* tidak cukup diskriminatif untuk membedakan *traffic brute force* dari *traffic*

login gagal yang dihasilkan oleh pengguna yang sah. Kami memperkenalkan agregasi *Netflows* untuk mengekstrak fitur yang tepat untuk membangun model pembelajaran mesin. Hasil kami menunjukkan bahwa model yang dibangun di atas fitur ini memberikan kinerja yang sangat baik untuk mendeteksi serangan *brute force*.

Automated Backup (*backup* otomatis)

Dalam teknologi informasi, backup mengacu pada penyalinan data, di mana data tersebut merupakan salinan dari data yang dapat dipulihkan jika ada data yang hilang. *Backup* melindungi sistem file dari kesalahan pengguna, *disk* atau kegagalan perangkat keras lainnya, kesalahan perangkat lunak yang dapat merusak sistem file dan bencana alam. Penggunaan cadangan yang paling umum adalah untuk memulihkan file yang terhapus secara tidak sengaja oleh pengguna dan untuk memulihkan dari kegagalan *disk*.



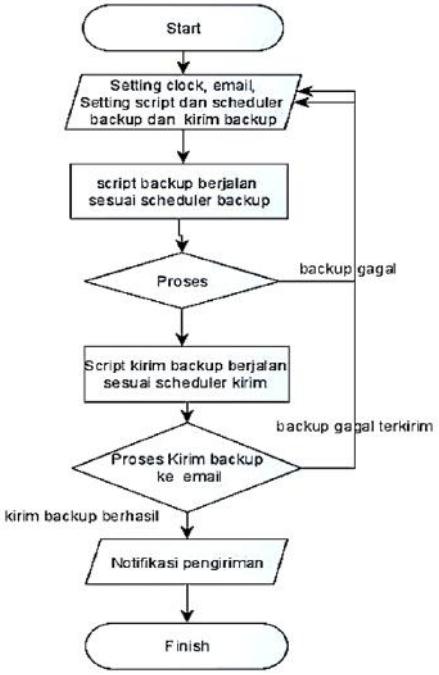
Gambar 4: *Flowcart Simple Port Knocking*

Metode Penelitian

Pemodelan *Simple Port Knocking*

Pengaturan akses untuk mikrotik sepenuhnya pada admin sekolah. Admin sekolah dapat mengakses mikrotik dengan menerapkan konfigurasi *simple port knocking* sehingga selain admin sekolah tidak diizinkan mengakses mikrotik. Dengan *simple port knocking* selain admin sekolah tidak dapat mengakses mikrotik walaupun mengetahui *username* dan *password* mikrotik melalui cara *brute force*. Arsitektur sistem keamanan mikrotik dengan menggunakan metode *simple port knocking* terdapat *flowchart*. Berikut merupakan *flowchart simple port knocking* yang disajikan pada Gambar 4.

Simple port knocking automated backup digunakan untuk mengamankan bilamana terjadi *error* atau kerusaakan pada mikrotik. *Automated backup* memerlukan dua email sebagai pengirim *backup* mikrotik dan penerima *backup* mikrotik. Email pengirim akan mengirimkan *backup* konfigurasi mikrotik secara berkala melalui email penerima yaitu admin sekolah. Bilamana terjadi *error* pada mikrotik, admin tidak perlu konfigurasi ulang karena admin bisa langsung mengambil *backup* konfigurasi mikrotik di email dan dapat langsung di pasang di mikrotik. Arsitektur sistem keamanan mikrotik dari *error* atau rusaknya mikrotik dengan menggunakan metode *automated backup* terdapat *flowchart*. Berikut merupakan *flowchart automated backup* yang disajikan pada Gambar 5.

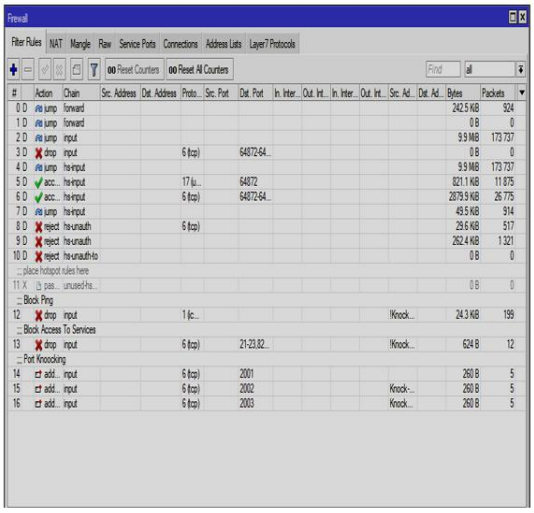


Gambar 5: *Flowcart Automated Backup*

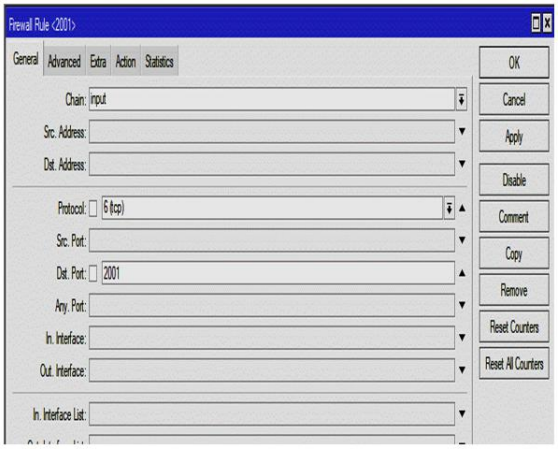
Rancangan Sistem *Simple Port Knocking*

Konfigurasi *simple port knocking* pertama yang dilakukan yaitu dengan menambahkan konfigurasi *simple port knocking* pada *Firewal*, Yaitu dengan klik menu IP lalu pilih *Firewall*. Setelah masuk *Firewall* lalu ke *tab filter rules* maka konfigurasi *simple port knocking* disajikan pada Gambar 6.

Pada konfigurasi ini akan dilakukan membuat rule pertama yaitu *chain* nya *input* yaitu membuat *rule* admin yang mengakses / memasuki mikrotik. Admin yang ingin mengakses mikrotik harus melalui port 2001: tcp seperti pada Gambar 7.

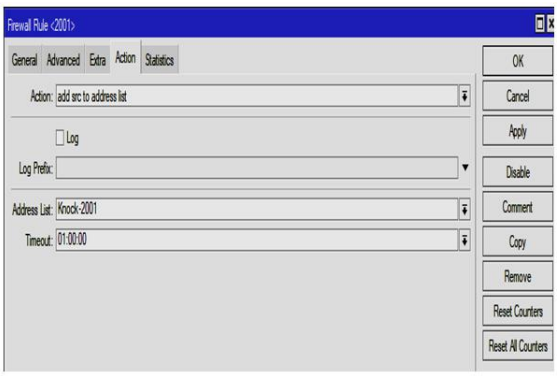


Gambar 6: Konfigurasi *Simple Port Knocking*



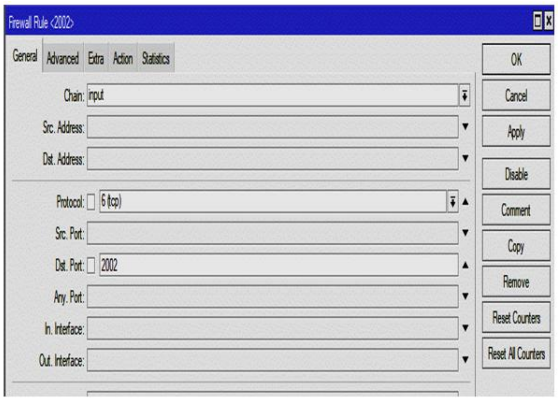
Gambar 7: *Setting Rule* Pertama

Setelah memasuki mikrotik lewat port 2001:tcp akan dimasukan ke address list "knock-2001" seperti pada Gambar 8.



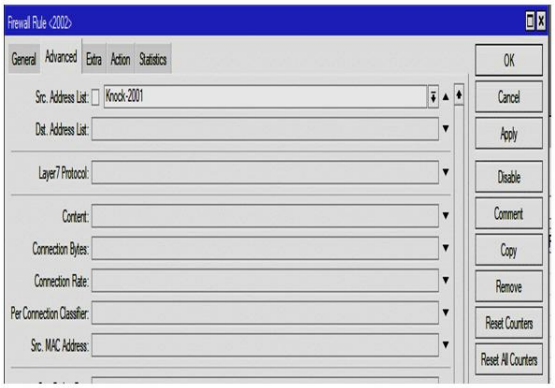
Gambar 8: *Setting Address List Rule* Pertama.g

Setelah masuk ke port 2001:tcp dan dimasukan *addres list* "*knock*-2001" maka Admin harus masuk lagi melalui port 2002:tcp seperti pada Gambar 9.



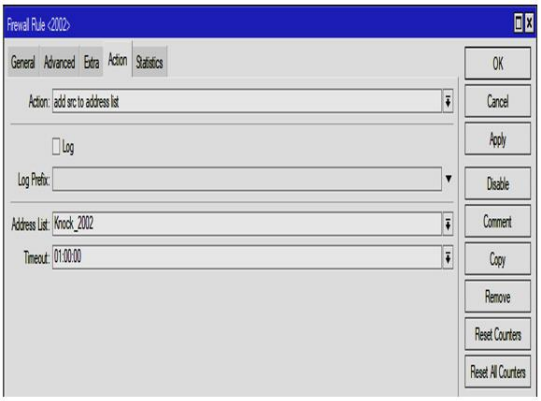
Gambar 9: *Setting Rule* Kedua.g

Syarat untuk masuk ke port 2002: tcp harus dari addres list "*knock* 2001" seperti pada Gambar 10.



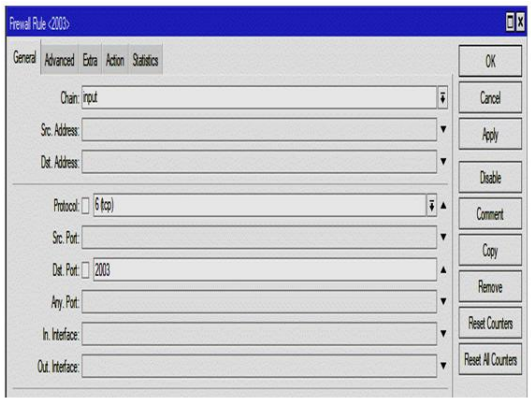
Gambar 10: *Address List Rule* Keduag

Setelah memasuki port 2002:tcp dan berhasil dari *addres list* "*knock*_2001" selanjutnya akan dimasukan ke *address list* "knock_2002" seperti pada Gambar 11.



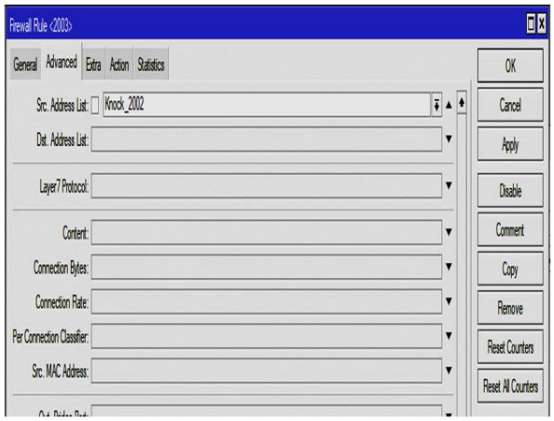
Gambar 11: *Setting Action Rule* Kedua. g

Setelah masuk ke port 2002:tcp dan dimasukan addres list "*knock*_2002" maka Admin harus masuk lagi melalui port 2003:tcp seperti pada Gambar 12.



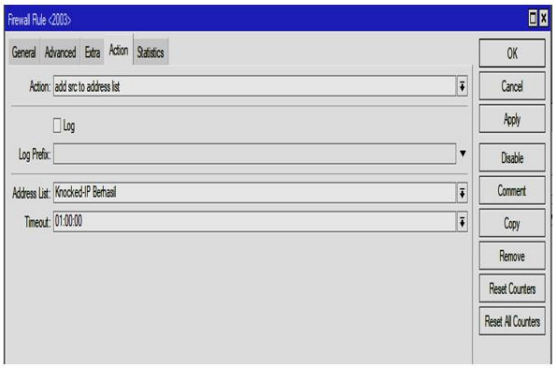
Gambar 12: *Setting Rule* Ketiga

Syarat untuk masuk ke port 2003:tcp harus dari *addres list* "*knock* 2002" seperti pada Gambar 13.



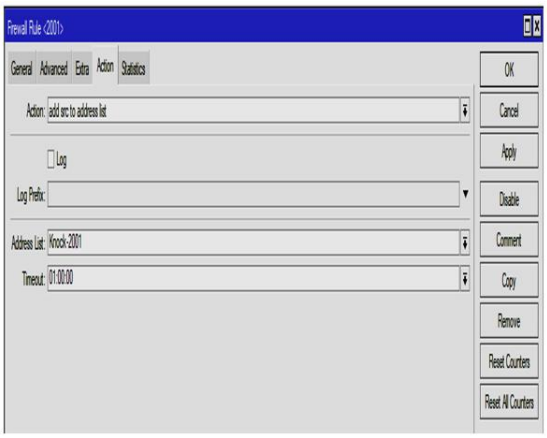
Gambar 13: *Setting Address List Rule* Ketiga

Setelah memasuki port 2003:tcp dan berasal dari *addres list* "knockip-Berhasi" selanjutnya akan dimasukan ke *address list* "*knock*-Berhasil" seperti pada Gambar 14 *knock*-Berhasil.



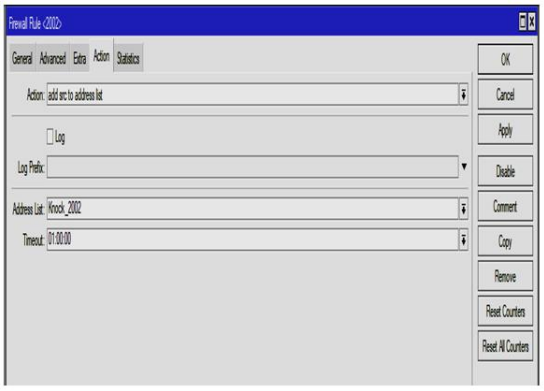
Gambar 14: Knock-Berhasil

Syarat untuk masuk ke mikrotik harus dari *addres list* "knockip_2001" seperti pada Gambar 15.



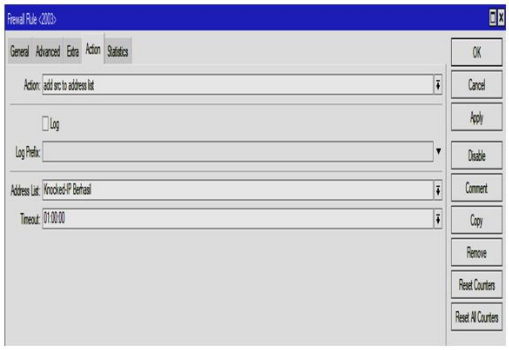
Gambar 15: *Setting Address List Rule* Keempat

Selanjutnya masuk lagi ke *address list* *Knock*_2002 seperti pada Gambar 16.



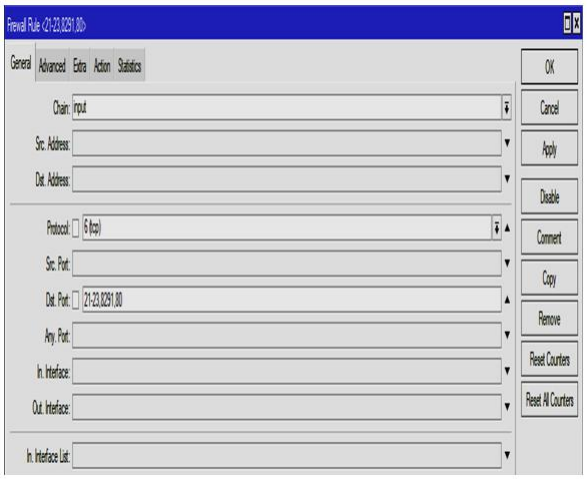
Gambar 16: *Setting Action Rule* Keempat

Selanjutnya masuk lagi ke *address list* *Knock*_2003 /knockedip Berhasil seperti pada Gambar 17.



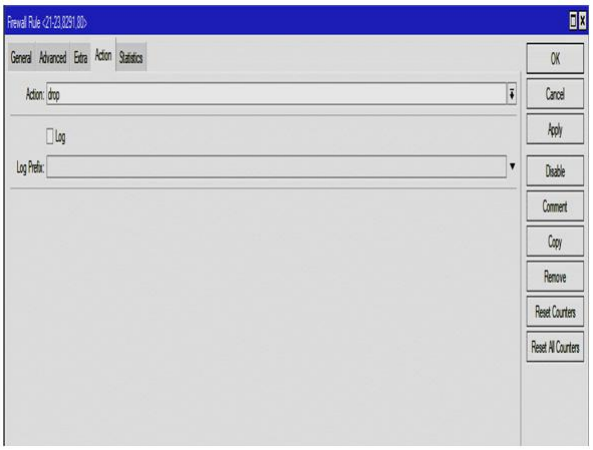
Gambar 17: Address list Knock_2003 /knockedip Berhasil

Selanjutnya membuat *rule* yang mencegah *user* yang ingin masuk ke mikrotik lewat *port* 21-23,(ssh), 80 (web), dan 8291 (winbox) seperti pada Gambar 18.

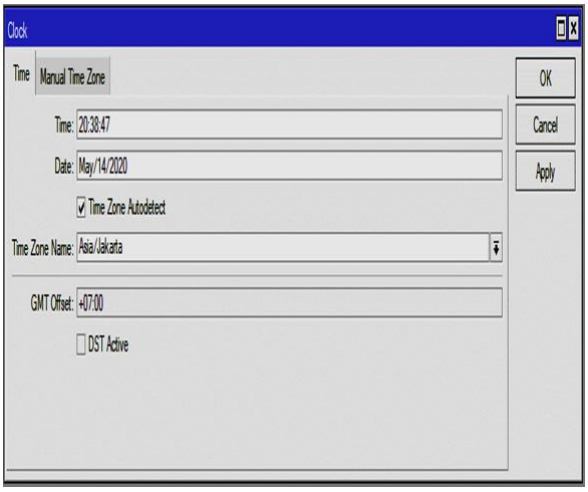


Gambar 18: Setting Action Rule Keenam

Lalu akan di arahkan ke *action drop* agar tidak bias masuk seperti pada Gambar 18 Artinya sebelum melewati *rule* yang telah dibuat tidak akan bisa masuk lewat *port* yang berada pada Gambar 19.



Gambar 19: Setting Action Rule Keenam

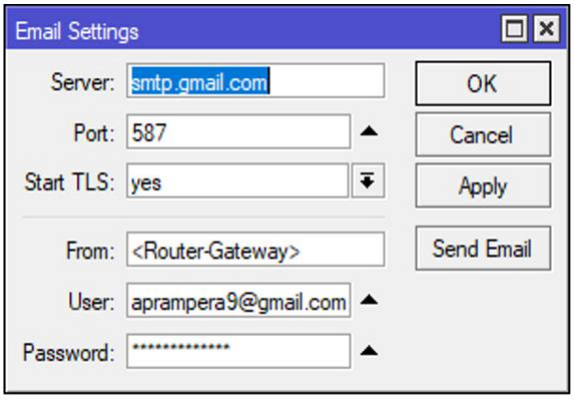


Gambar 20: *Setting Clock* di Mikrotik

Rancangan Sistem Automated Backup

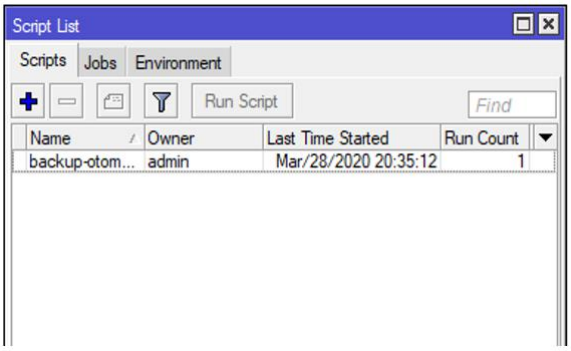
Konfigurasi *Automated Backup* pertama yang dilakukan yaitu dengan konfigurasi *clock* untuk proses *backup* di mikrotik. *Setting clock* seperti Gambar 20.

Pengaturan email digunakan untuk pengiriman *backup* mikrotik. Dalam pengaturan ini membutuhkan email sebagai pengirim *backup* mikrotik. *Setting* email seperti Gambar 21.



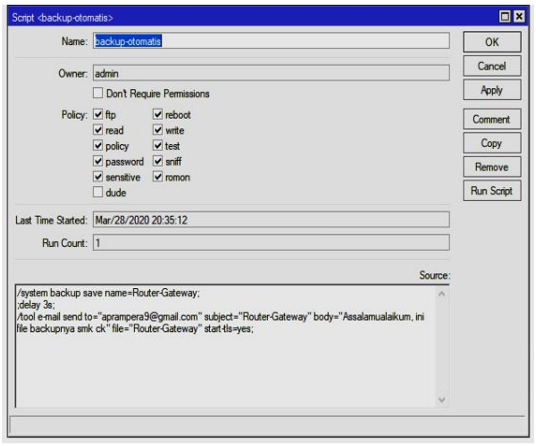
Gambar 21: Setting Email Pengirim Backup

Kemudian klik menu sistem =>> *script* di mikrotik terlihat terdapat 1 *script* seperti Gambar 22.



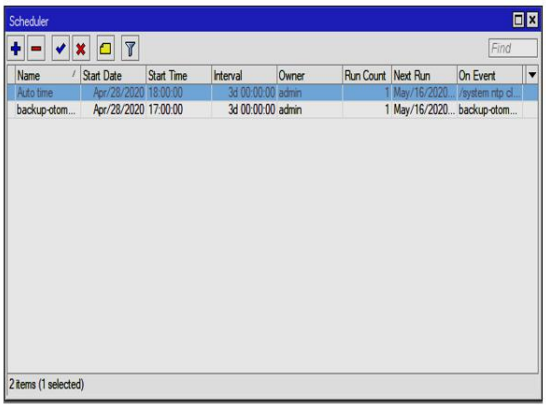
Gambar 22: *Setting Script* Mikrotik

Script " *backup*" digunakan sebagai pengirim file *backup* ke email admin mikrotik yang disajikan pada Gambar 23.



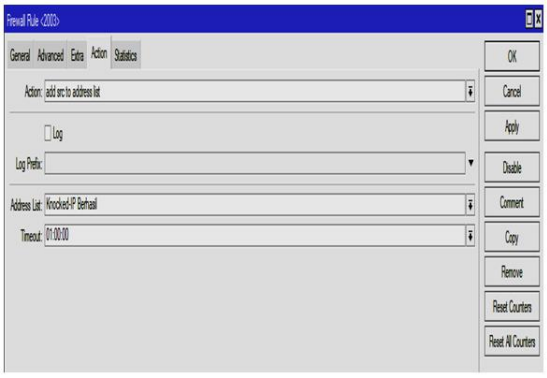
Gambar 23: *Setting Script* Kirim *Backup*

Setelah konfigurasi *script* di mikrotik kemudian membuat *scheduler* (jadwal pengiriman file *backup*) seperti pada Gambar 24.



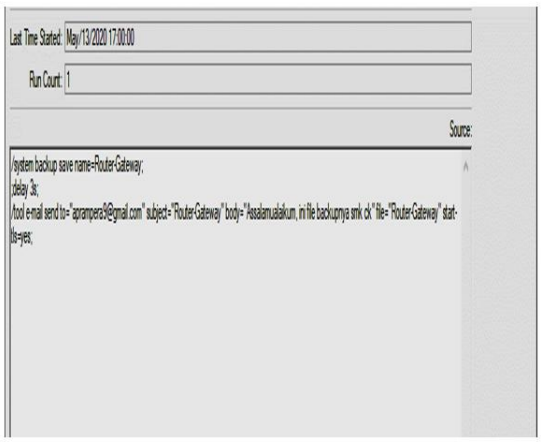
Gambar 24: Jadwal Pengiriman File Backup

Schedule auto backup digunakan untuk menentukan jadwal untuk menjalankan *script file auto backup* disajikan pada pada Gambar 25.



Gambar 25: Jadwal *Script Auto Backup*

Scrip send email digunakan untuk menentukan jadwal untuk menjalankan *script* file "*backup-otomatis*" seperti pada Gambar 26.

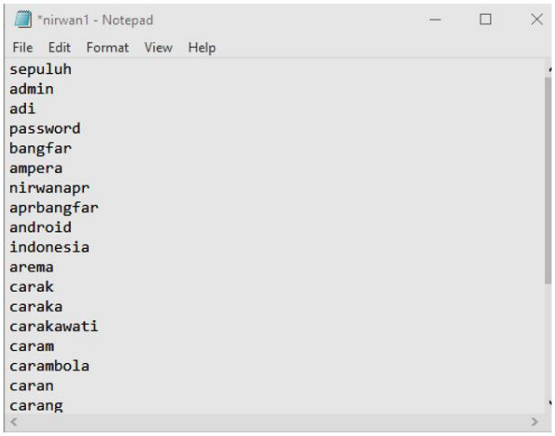


Gambar 26: Jadwal Script Send Email

Hasil dan Pembahasan

Pengujian Login Mikrotik Tanpa Keamanan Simple Port Knocking

Pengujian ini dilakukan dengan memanfaatkan *wordlist* dengan *file size* yang lebih kecil. penguji menggunakan (The Hacker Choice) THC-Hydra. Pada File nirwan1.txt pengujian ini dilakukan dengan memanfaatkan *wordlist* dengan *file size* yang lebih kecil. Pengujian ini relatif lebih cepat dibanding *wordlist* dari internet sehingga pengujian ini sangat baik untuk pengujian tingkat keamanan *login* admin mikrotik. Pengujian ini membutuhkan waktu kurang lebih 2 menit karena ukuran *wordlist* yang kecil. *Wordlist* seperti Gambar 27. Pengujian disajikan pada Gambar 28.

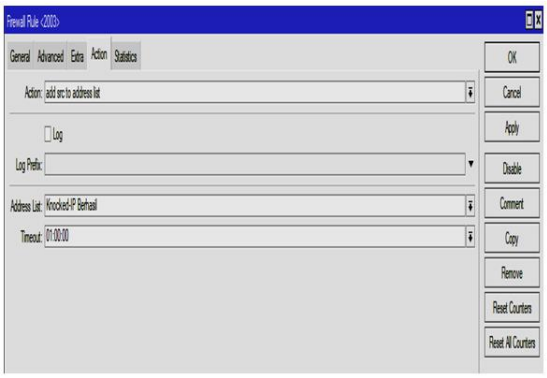


Gambar 27: *Wordlist login* mikrotik

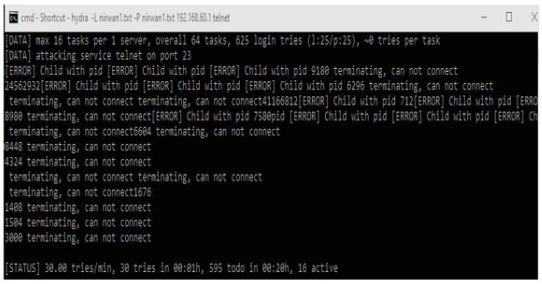
Pengujian Login Mikrotik Dengan Keamanan *Simple Port Knocking*

Pengujian ini dilakukan dengan memaksukkan *username* dan *password* yang telah di dapat dari pengujian *brute force* dengan *tools* hydra. Hasil dari pengujian ini adalah pengukuran tingkat keamanan admin mikrotik dari serangan *brute force*. Keamanan

simple port knocking dapat berjalan dengan baik dalam mengatasi serangan *brute force*. Pengujian tersebut pada Gambar 29.



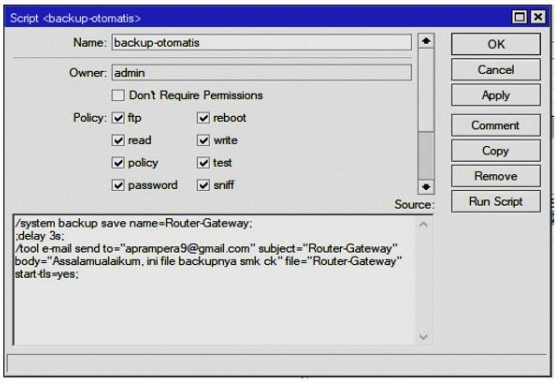
Gambar 28: *Brute Force* dengan *Wordlist* nirwan.txt



Gambar 29: Pengujian Brute Force Dengan Kemananan Simple Port Knocking

Pengujian *Automated Backup* Pada Mikrotik

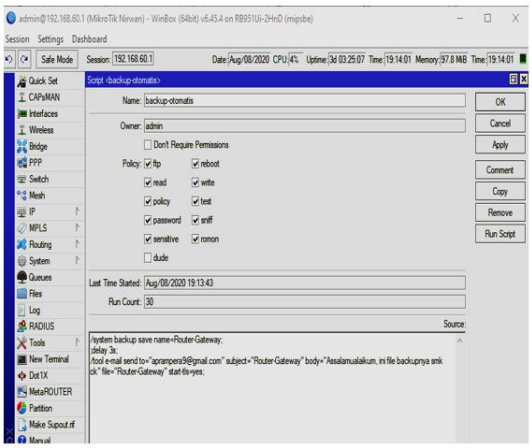
Pengujian *Script backup* adalah *script* untuk menjalankan *backup* mikrotik. *Backup* mikrotik dapat berjalan dengan menjalankan *run script* pada *script backup*. Hasil dapat dilihat di menu files di mikrotik, jika file *backup* ada dalam menu files bisa di simpulkan *script backup* dapat berjalan dengan baik. Pengujian *script backup* pada Gambar 30.



Gambar 30: Pengujian *Script Backup*

Pengujian *Script* Kirim *Backup*

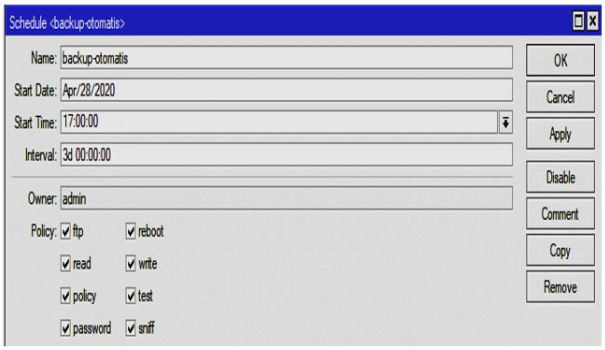
Script untuk menjalankan kirim *backup* mikrotik melalui email yang sudah di tentukan sebagai email admin mikrotik. *Script* kirim *backup*, kirim backup di jalankan sebanyak 30 kali dapat berjalan dengan menjalankan *run script* kirim *backup*. Hasil dapat dilihat di email, apabila file *backup* terkirim maka *script* kirim *backup* dapat berjalan dengan baik. Pengujian *script* kirim *backup* pada Gambar 31.



Gambar 31: Pengujian Script Kirim Backup

Pengujian Scheduler Backup

Scheduler backup adalah jadwal untuk melakukan proses *backup* pada *script backup*. *Script backup* tidak dapat berjalan secara otomatis tanpa ada *scheduler backup*. Hasil dari *scheduler* dapat dilihat apabila proses *backup* mikrotik dapat berjalan sesuai *scheduler* yang ditentukan. *Scheduler backup* pada Gambar 32.



Gambar 32: Pengujian scheduler backup

Pengujian *Scheduler* Kirim *Backup*

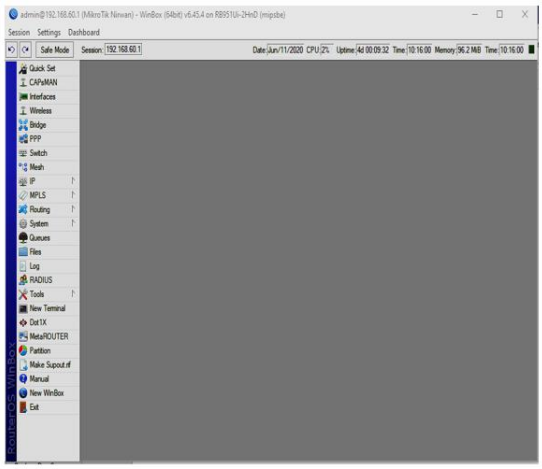
Scheduler kirim email adalah jadwal untuk melakukan proses kirim backup ke email pada *script* kirim *backup*. *Script* kirim email tidak dapat berjalan secara otomatis tanpa ada *scheduler* kirim ba*ckup*. Hasil dari *scheduler* dapat dilihat di email admin mikrotik apabila *backup* mikrotik terkirim

email sesuai jadwal maka *scheduler* dapat berjalan dengan baik. *Scheduler* kirim *backup* pada Gambar 33.

Gambar 33: Pengujian Scheduler Kirim Backup

Hasil Pengujian Tanpa Menggunakan Keamanan Simple Port Knocking

Pada tahap ini dapat menjadi ukuran untuk tingkat keamanan admin mikrotik. Hasil pengujian ini dapat mengetahui kelemahan tingkat keamanan mikrotik sehingga dapat menjadi acuan untuk meningkatkan sistem keamanan mikrotik. Hasil pengujian dapat dilihat pada *login* dengan *usename* dan *password* yang sudah di dapatkan dengan *tools* hydra di mikrotik. Hasil *login* seperti pada Gambar 34.

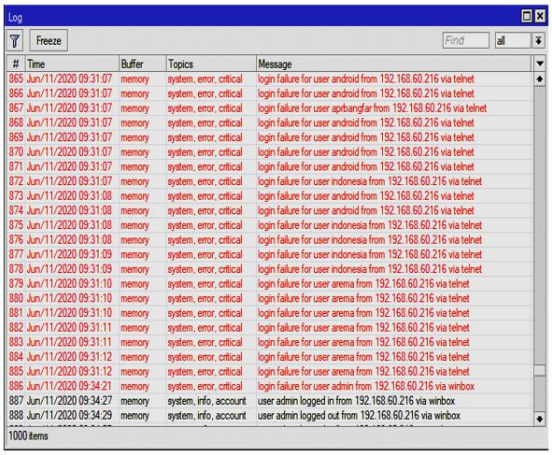


Gambar 34: Hasil *Login* dengan *Username* dan *Password* dari *Tools* Hydra

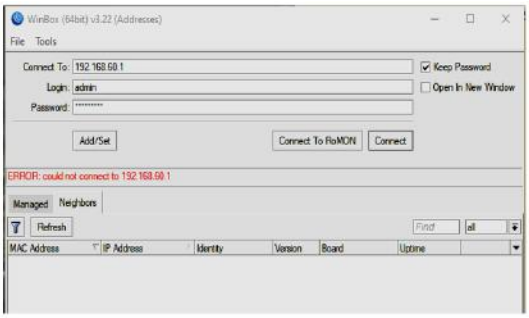
Dari gambar di atas dapat dilihat bahwa dengan cara *brute force* dapat mengetahui *username* dan *password* admin sehingga dapat masuk mikrotik. Hasil *login* dapat dilihat pada menu log di mikrotik. Log *login* berhasil masuk pada Gambar 35.

Hasil Pegujian Dengan Keamanan Simple Port Knocking

Hasil pengujian dapat dilihat perbedaan tingkat keamanan dari serangan *brute force*. Dengan menerapkan *simple port knocking* dapat mencegah serangan *brute force* pada admin mikrotik. Walaupun dengan memasukkan *username* dan *password* yang benar tidak dapat masuk mikrotik karena ada *rule port* yang ada pada keamanan *simple port knocking*. Hasil *login* tidak bisa masuk mikrotik pada Gambar 36.



Gambar 35: Hasil *Log Login* Mikrotik Berhasil Masuk



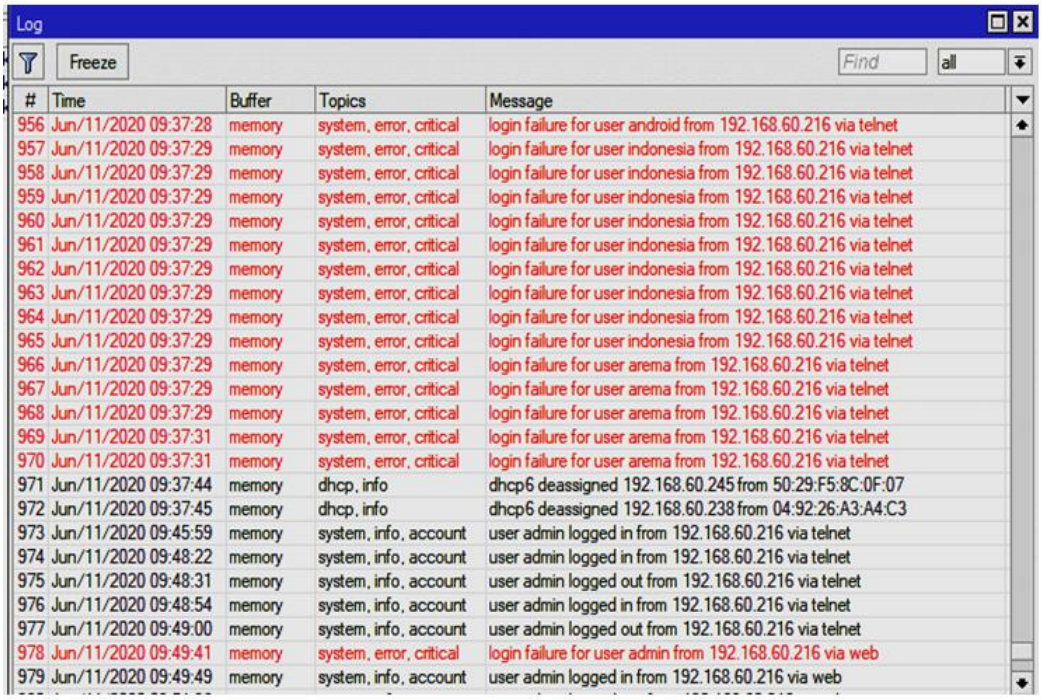
Gambar 36: *Login* Gagal Masuk Mikrotik.

Hasil bahwa dengan cara *brute force* tidak dapat menembus keamanan *simple port knocking* dapat dilihat pada menu log di mikrotik. Hasil log seperti Gambar 37.

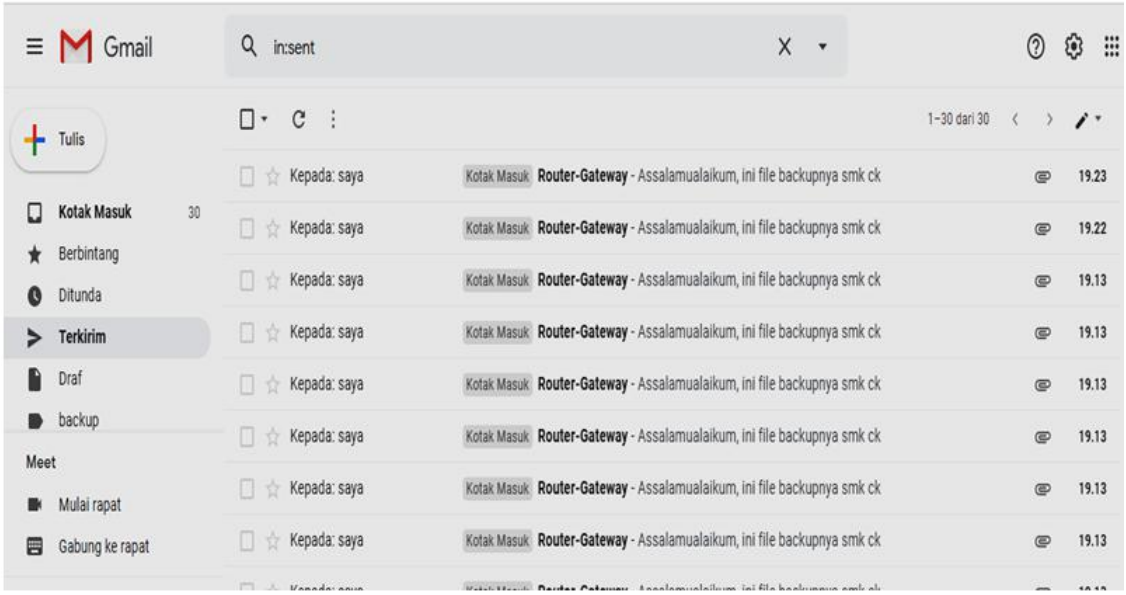
Hasil Pengujian Script Kirim Backup Dan Scheduler Kirim Backup

Pada tahap ini *script* kirim *backup* dapat berjalan sesuai *scheduler* kirim *backup*. Hasil pengujian dapat dilihat pada email admin sebagai penerima *backup* mikrotik. Hasil dari kirimm *backup* dapat dilihat pada Gambar 38.

Detail untuk file yang terkirim di email dapat dilihat di *inbox* pada email penerima *backup* mikrotik. Hasil dapat di lihat pada Gambar 39.



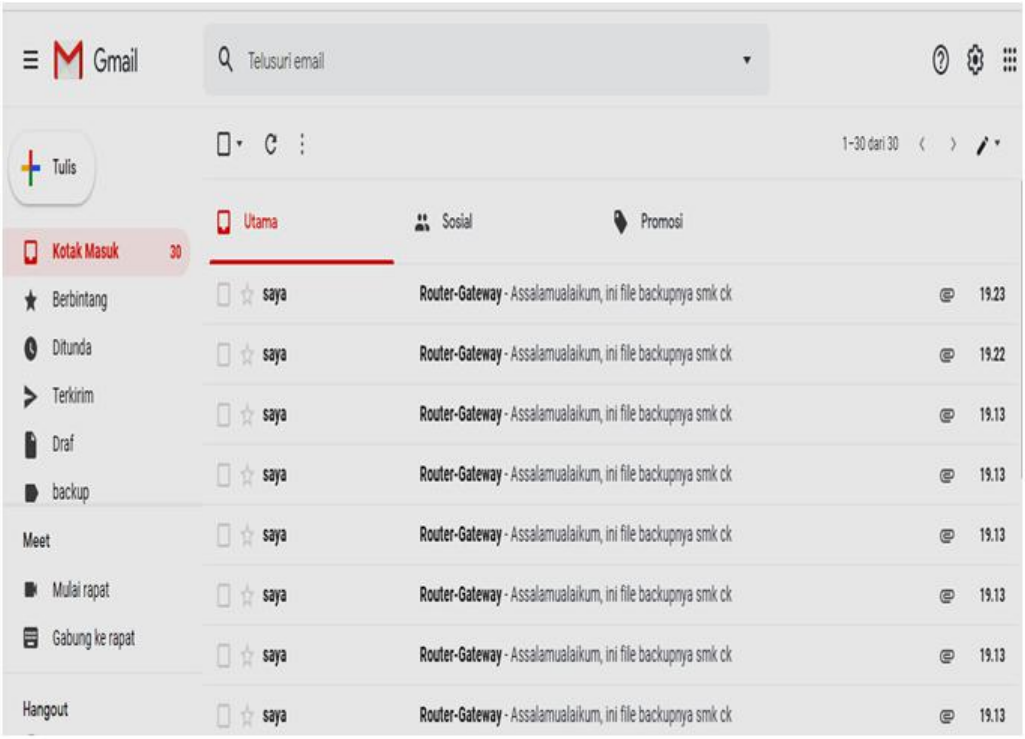
Gambar 37: Hasil Log *Login* dengan Keamanan *Simple Port Knocking*



Gambar 38: Hasil Dari Script Dan Scheduler Kirim Backup

Penutup

Berdasarkan hasil pengujian denagn *tools hydra* diperoleh metode keamanan *simple port knocking* dapat mencegah serangan *brute force* karena sebelum masuk mikrotik harus memasukkan *rule port* yang ditentukan. Dengan *automated backup* sekolah tidak perlu lagi mendatangkan teknisi bila terjadi *error* pada mikrotik karena *backup* konfigurasi bisa digunakan untuk mengembalikan konfigurasi mikrotik.



Gambar 39: Backup Mikrotik Yang Sudah Terkirim Email.

Daftar Pustaka

[1] I. Gunawan, "Penggunaan *Brute Force Attack* dalam Penerapannya Pada Crypt8 dan Csa-Rainbow Tool untuk Mencari Biss", InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan), vol. 1, no. 1, pp. 52–55, doi: 10.30743/infotekjar.v1i1.48, 2016.

[2] Fakariah Hani Mohd Ali, Rozita Yunos and Mohd Azuan Mohamad Alias, "Simple Port Knocking Method: Against TCP replay attack and port scanning", International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp. 247–252, 2012.

[3] R. D. H. Ontoseno, M. N. Haqqi dan M. Hatta, "Limitasi Pengguna Akses Internet Berdasarkan Kuota Waktu dan Data Menggunakan Pc Router Os Mikrotik", Tek. Eng. Sains J., vol. 1, no. 2, p. 125, doi: 10.51804/tesj.v1i2.134.125-130, 2017.

[4] S. Jarot dan Sudarma, "Buku super pintar internet", MediaKita, 2012.

[5] E. A. Darmadi, "Manajemen Bandwidth Internet Menggunakan Mikrotik Router di Politeknik Tri Mitra Karya Mandiri", IKRA-ITH Teknol. J. Sains Teknol., vol. 3, no. 3, pp. 7–13, 2019.

[6] M. Krzywinski, "Port Knocking-Network Authentication Across Closed Ports", SysAdmin Mag., vol. 10, no. 6, pp. 12-17, 2003.

[7] S. Jeanquier, "An Analysis of Port Knocking and Single Packet Authorization", MSc Thesis, Information Security Group Royal Holloway College, University of London, 2006.

[8] T. Popeea, V. Olteanu, L. Gheorghe, and R. Rughiniş, "Extension of a port knocking client-server architecture with NTP synchronization", Proc. - RoEduNet IEEE Int. Conf., doi: 10.1109/RoEduNet.2011.5993704, 2011.

[9] I. D. M. Widia, "Implementation of bandwitdh management using microtic router", IOP Conf. Ser. Mater. Sci. Eng., vol. 801, no. 1, doi: 10.1088/1757-899X/801/1/012143, 2020.

[10] M. M. Najafabadi, T. M. Khoshgoftaar, C. Calvert and C. Kemp, "Detection of SSH brute force attacks using aggregated netflow data", Proc. - 2015 IEEE 14th Int. Conf. Mach. Learn. Appl. ICMLA 2015, pp. 283–288, doi: 10.1109/ICMLA.2015.20, 2016.