Sibatik Journal
Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, dan Pendidikan
E-ISSN: 2809-8544

ANALISIS DETEKSI DAN PENCEGAHAN EKSPLOITASI JARINGAN BRUTE FORCE EXPLOIT MENGGUNAKAN FIREWALL PADA KANTOR BAPPEDA KOTA PALOPO

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
Universitas Cokroaminoto Palopo
Email: mudzakkar8@gmail.com[1], siaulhak@uncp.ac.id[2], jumarniati@uncp.ac.id[3]

Abstract

This study aims to analyze the security system of the office network with a focus on identifying potential security vulnerabilities. The research was conducted at the Office of Regional Development Planning Agency (Dinas Bappeda) of Palopo City using the Action Research method. The purpose of this research is to assist network administrators in improving their network security by understanding potential threats and knowing how to address them. The problem in this research is that the existing network is not equipped with adequate security systems, which creates a vulnerability for Brute Force Exploit attacks. Such incidents can pose a threat to the network security system at any time, whether the administrator is working or not. Firewall rules and notification alerts were implemented on the Mikrotik router, and the system was tested using Hydra, Ncrack, and Medusa. The analysis results showed that the security system of the Dinas Bappeda network has successfully protected it from Brute Force Exploit attacks.

Keywords: *Brute Force, Mikrotik, Firewall*

Abstrak

Penelitian ini bertujuan untuk menganalisis sistem keamanan jaringan kantor dengan menekankan pada identifikasi potensi celah keamanan. Penelitian ini dilaksanakan di kantor Dinas Bappeda Kota Palopo dengan menggunakan metode penelitian *Action Research*. Tujuan dari penelitian ini adalah membantu administrator jaringan dalam meningkatkan tingkat keamanan jaringan mereka dengan memahami potensi ancaman yang ada dan mengetahui bagaimana cara mengatasinya. Masalah pada penelitian ini yaitu Jaringan yang ada tidak dilengkapi dengan sistem keamanan yang memadai sehingga terdapat celah untuk dilakukan serangan *Brute Force Exploit*. Kejadian seperti ini dapat menimbulkan ancaman bagi sistem keamanan jaringan karena suatu serangan ke dalam jaringan komputer dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak. *Firewall rule* dan *Notifikasi alert* diterapkan pada *router* mikrotik dan pengujian sistemnya menggunakan *Hydra*, *Ncrack*, dan *Medusa*. Hasil analisis menunjukkan bahwa sistem keamanan jaringan Dinas Bappeda telah berhasil melindungi jaringan dari serangan *Brute Force Exploit*.

Kata kunci: Brute Force, Mikrotik, Firewall

PENDAHULUAN

Di era maju teknologi yang kini mengalami kemajuan yang pesat, terdapat dua jalur penggunaan jaringan yang umum digunakan sehari-hari, yaitu media kabel (*Local Area Network/LAN*) dan media nirkabel (*Wireless*). Teknologi nirkabel atau *wireless* merupakan salah satu bidang teknologi yang sering digunakan dalam kehidupan sehari-hari, terutama dalam bidang telekomunikasi dan komputer. Namun, kecanggihan teknologi ini tidak serta merta membawa dampak positif saja, melainkan juga membawa dampak negatif berupa tindakan kejahatan *siber* yang merugikan pengguna jaringan. Tindakan kejahatan *siber* tersebut biasanya dilakukan oleh individu atau kelompok yang sering disebut sebagai *hacker*. *Hacker* merupakan seorang ahli dalam teknologi informasi yang memiliki

kemampuan dalam melakukan kegiatan seperti penelitian, analisis, modifikasi, dan bahkan pembobolan sistem atau jaringan (Amarudin, 2018).

Peretas yang menargetkan sistem keamanan informasi menggunakan strategi atau taktik dalam menyerang suatu sistem. Salah satu metode yang biasa digunakan peretas adalah *exploit* yang merupakan sebuah kode, set kode, atau program yang memanfaatkan kelemahan suatu sistem. Dampak serangan *exploit* dapat bervariasi mulai dari kehilangan informasi pribadi pengguna sistem hingga kerugian pengguna secara pribadi, karena informasi yang dikumpulkan peretas seringkali digunakan untuk tujuan kriminal.

Kantor Bappeda Kota Palopo memiliki jaringan media *wireless* dan *wired* sebagai fasilitas pelayanan masyarakat. Namun Jaringan yang ada tidak dilengkapi dengan sistem keamanan yang memadai. Ini menyebabkan jaringan tersebut rentan terhadap serangan eksploitasi jaringan, seperti *Brute Force Exploit*. Tanpa adanya *firewall* yang efektif, jaringan Bappeda Kota Palopo akan rentan terhadap serangan dari pihak luar yang tidak bertanggung jawab. Hal ini dapat membahayakan informasi penting yang disimpan dalam sistem jaringan. Oleh karena itu, menganalisis dan mencegah serangan *Brute Force Exploit* melalui implementasi *firewall* menjadi hal yang sangat penting dan perlu dilakukan untuk melindungi sistem jaringan Bappeda Kota Palopo.

Permasalahan yang dihadapi adalah Jaringan yang ada tidak dilengkapi dengan sistem keamanan yang memadai untuk dapat mencegah serangan *Brute Force Exploit* pada *router* mikrotik, sehingga mempunyai celah untuk dilakukan eksploitasi, dimana mikrotik ini dapat dilakukan kegiatan *Brute Force Exploit* dimana kita bisa mengetahui *username* dan *password* login mikrotik yang digunakan, dikhawatirkan dapat mengakibatkan terjadinya kehilangan data data maupun penyalahgunaan jaringan. Dengan dasar ini, menjadi landasan untuk membuat sistem jaringan komputer yang lebih aman, sehingga pada penelitian ini dilakukan Analisis Deteksi dan Pencegahan Ekploitasi Jaringan *Brute Force Exploit* Menggunakan *Firewall* untuk mengamankan jaringan dari serangan orang-orang yang tidak bertanggung jawab.

Berdasarkan deskripsi diatas, sangat penting untuk memahami cara menangani dan menyelesaikan kerentanan pada sistem *router MikroTik* yang terbuka terhadap serangan *Brute Force Exploit*. Oleh karena itu, penulis memilih topik dengan judul "Analisis Deteksi dan Pencegahan Eksploitasi Jaringan *Brute Force Exploit* Menggunakan *Firewall* Pada Kantor Bappeda Kota Palopo".

TINJAUAN PUSTAKA

Analisis

Analisis adalah sebuah kegiatan atau aktivitas yang berisi tentang menguraikan sebuah komponen, membedakan objek sesuai kriteria tertentu dan mengetahui fungsi masing-masing dalam satu keseluruhan yang terpadu. Sehingga dapat menguraikan komponen komponen pembentuknya atau menyusun komponen tersebut untuk dikaji lebih lanjut. (Budiansyah, Widiarta, Yunanri,2020)

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

Deteksi

Deteksi merupakan proses pemeriksaan atau pengecekan terhadap sesuatu dengan menggunakan teknik dan cara tertentu. Dalam berbagai masalah, seperti sistem pendeteksi penyakit, deteksi digunakan untuk mengidentifikasi gejala yang terkait dengan penyakit. Tujuan utama dari deteksi adalah menyelesaikan masalah dengan metode yang sesuai, sehingga dapat menghasilkan solusi yang efektif (Rekno & Daniel, 2018).

Eksploitasi

Eksploitasi merujuk pada penggunaan sumber daya atau kesempatan yang tersedia untuk keuntungan pribadi atau kepentingan yang merugikan pihak lain. Dalam konteks umum, eksploitasi dapat merujuk pada eksploitasi lingkungan, eksploitasi tenaga kerja, eksploitasi keuangan, dan eksploitasi lainnya yang mengambil keuntungan dari kelemahan atau kerentanan suatu sistem atau individu.

Eksploitasi adalah tindakan memanfaatkan atau memeras seseorang untuk keuntungan pribadi. Tindakan tersebut dianggap tidak etis dan merugikan orang yang dieksploitasi (Sisma, 2016).

Brute Force

Brute Force adalah suatu pendekatan untuk memecahkan permasalahan, biasanya didasarkan pernyataan masalah dan definisi konsep yang dilibatkan. *Brute Force* memiliki pola piker yang sederhana, mampu menyelesaikan suatu permasalahan tanpa memakan banyak waktu. (Pribadi, Rahmawati, Heningtyas, 2021).

Jaringan Komputer

Menurut Kurniawan, jaringan komputer dapat diartikan sebagai kumpulan sejumlah perangkat yang meliputi beberapa komputer, printer, Lan card, dan peralatan lain yang terhubung satu sama lain secara integrative (Armanto, 2017).

Firewall

Firewall adalah teknik yang sangat berguna dan penting dalam mengamankan jaringan. Firewall merupakan model atau mekanisme sistem yang diterapkan pada perangkat keras, perangkat lunak, atau pada sistem itu sendiri dengan tujuan melindungi segmen pada jaringan pribadi dari jaringan luar yang tidak terpercaya. Tujuannya adalah untuk menyaring, membatasi, atau bahkan menolak semua koneksi dan aktivitas yang dilakukan pada segmen tersebut. Segmen pada jaringan pribadi dapat berupa *workstation, server, router,* atau jaringan *LAN* (Sugiyono, 2016).

METODE

Metode yang digunakan penelitian ini adalah *Action Research,* Penelitian yang bertujuan untuk memperbaiki atau meningkatkan kinerja suatu jaringan atau sistem jaringan dengan menerapkan *Action Research*. Dalam jenis penelitian ini, Peneliti melakukan analisis terhadap data jaringan untuk mengidentifikasi masalah yang muncul, mencari solusi yang

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

tepat, dan menerapkan perbaikan untuk meningkatkan kinerja jaringan. Tujuan dari penelitian *Action Research* adalah untuk meningkatkan efisiensi, keamanan, dan kinerja jaringan dalam organisasi atau instansi yang bersangkutan.

HASIL DAN PEMBAHASAN

Pada hasil penelitian ini, berikut tahapan penelitian yang digunakan dalam metode *Action Research* yang dimana tahapan ini digunakan sebagai pendekatan proses yang menggambarkan siklus atau tahapan awal hingga akhir dalam hasil analisis jaringan menggunakan router mikrotik yang mencakup 4 tahapan yaitu Melakukan Dianosa (*Diagnosing)* Rencana Tindakan (*Planning action)* Melakukan Tindakan (*Taking Action*) Melakukan Evaluasi (*Evaluation Action*).

1. Melakukan Diagnosa (Diagnosing)

   Pada tahap ini penulis melakukan diagnosis dengan cara menganalisis permasalahan yang ada pada Kantor Bappeda Kota Palopo. Penelitian telah dilakukan pada waktu dan tempat yang dijadwalkan. Sebelum melakukan penelitian, peneliti terlebih dahulu melakukan wawancara dengan pihak Instansi yang bertanggung jawab tentang jaringan yang diterapkan pada Instansi tersebut. Pada Kantor Bappeda Kota Palopo permasalahan yang dihadapi sekarang Jaringan yang ada tidak dilengkapi dengan sistem keamanan yang memadai sehingga terdapat celah untuk di lakukan serangan *Brute Force Exploit*, karena pada sistem yang berjalan sekarang tidak dapat mencegah apabila ada serangan pada sistem. Hal seperti ini dapat menimbulkan ancaman bagi sistem jaringaan karena suatu serangan ke dalam jaringan dapat terjadi kapan saja. Baik pada saat administrator yang sedang bekerja ataupun tidak yang ada di Instansi tersebut. Hal ini menjadi landasan untuk menjadikan sistem jaringan komputer yang lebih aman.
2. Rencana Tindakan (Planning Action)

   Tahap Selanjutnya yaitu Tindakan Perencanaan (*Planning Action*), pada tahap ini peneliti dalam mengambil dan mengumpulkan semua bahan, data-data dan kebutuhan yang di ambil dari permasalahan yang ada.
3. Melakukan Tindakan (Action Taking)

   Pada tahap ini peneliti melakukan Pengambilan tindakan dari Tahapan Perencanaan dengan melakukan implementasi, implementasi digunakan aplikasi *winbox* untuk sistem keamanan *Firewall* menggunakan mikrotik.

Impelementasi dan Konfigurasi Mikrotik

Konfigurasi mikrotik digunakan untuk mengatur agar mikrotik dapat terhubung ke jaringan dengan berbagai tujuan penggunaannya sehingga dapat membantu administrator jaringan dalam melakukan tugasnya, termasuk metode pengamanan jaringan yang dilakukan menggunakan mikrotik. Namun, sebelum digunakan, mikrotik harus dikonfigurasi terlebih dahulu agar dapat bekerja sesuai fungsinya.

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

Implementasi Dan Konfigurasi Exploit Brute Force Telnet

Pembuatan Rule Firewall untuk mendeteksi dan mencegah serangan brute force exploit telnet.

Gambar 1. List Firewall Rule Telnet

Impelementasi Dan Konfigurasi Exploit Brute Force SSH

Pembuatan Rule Firewall untuk mendeteksi dan mencegah serangan brute force exploit ssh.

Gambar 2. List Firewall Rule SSH

Implementasi Dann Konfigurasi Exploit Brute Force FTP

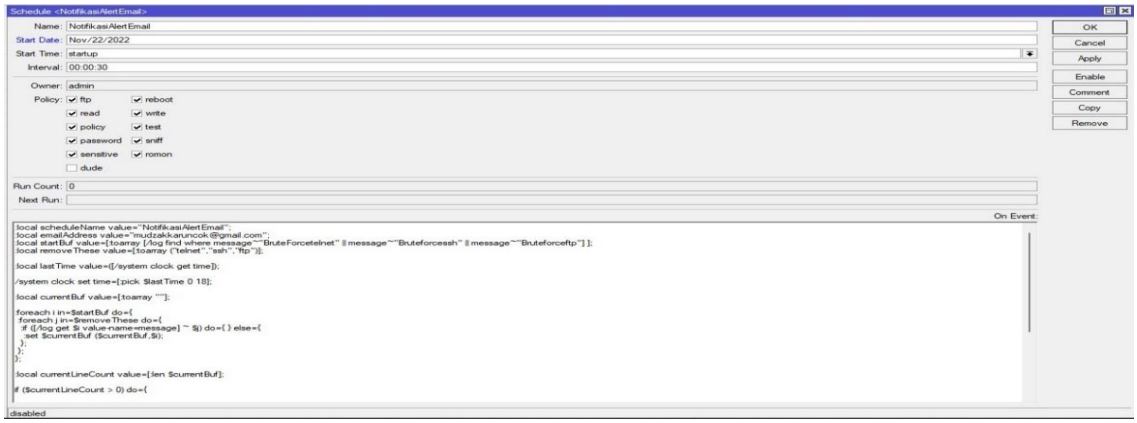
Pembuatan Rule Firewall untuk mendeteksi dan mencegah serangan brute force exploit ftp.

Gambar 3. List Firewall Rule FTP

Implementasi Dan Konfigurasi Notifikasi Alert

a. Notifikasi Email

Pembuatan Scheduler Notifikasi alert Email untuk mendeteksi serangan brute force exploit.

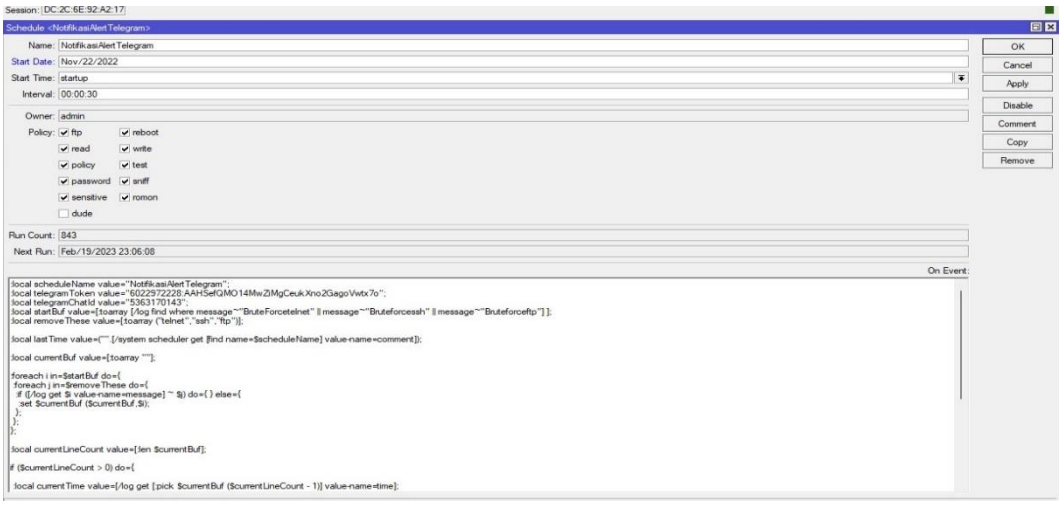


Gambar 4. Notifikasi Alert Email

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

b. Notifikasi Telegram

Pembuatan Scheduler Notifikasi alert telegram untuk mendeteksi dan mencegah serangan brute force exploit.



Gambar 5. Notifikasi Alert Telegram

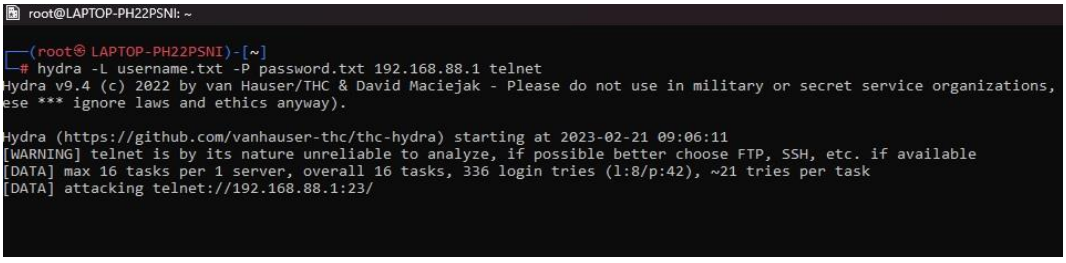
Melakukan Evaluasi (Evaluating)

Penulis secara aktif memantau kinerja sistem dan jaringan yang telah dibangun untuk memastikan bahwa semuanya berjalan sesuai rencana dan tujuan yang telah ditetapkan.

Pengujian Pada Sistem Setelah Sistem *Firewall Rule Brute Force*

a. Pengujian *Brute Force Telnet* Menggunakan hydra

Pengujian pertama dilakukan pada sistem yang telah diproteksi yaitu dengan Serangan *Brute Force* Menggunakan Hydra. Ketika penyusup melakukan serangan pada sistem atau mencoba masuk ke sistem, sistem dapat mendeteksi aktivitas. terlihat dari Gambar 6 bahwa Hydra tidak dapat memantau *username* dan *password Telnet* yang terbuka di *Router* Mikrotik . Dapat di lihat pada gambar di bawah ini:



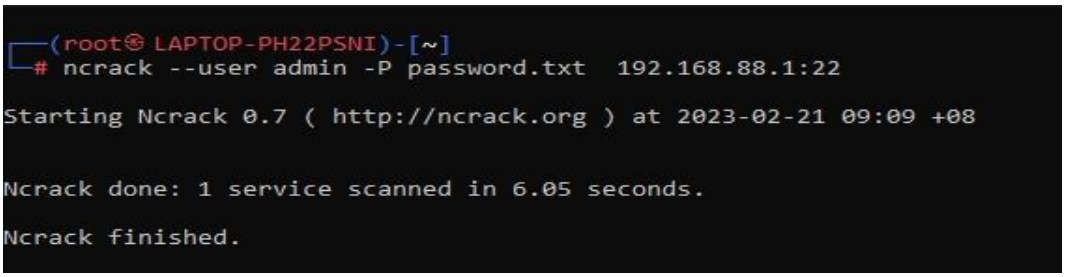
Gambar 6. *Brute Force Telnet Exploit* Setelah Sistem *Firewall Rule*

b. Pengujian Setelah *Brute Force SSH Exploit* Menggunakan *Ncrack*

Pengujian Selanjutnya dilakukan pada sistem yang telah diproteksi yaitu dengan Serangan *Brute Force SSH* Menggunakan ncrack. Ketika penyusup melakukan serangan pada sistem atau mencoba masuk ke sistem, sistem dapat mendeteksi aktivitas, terlihat

Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

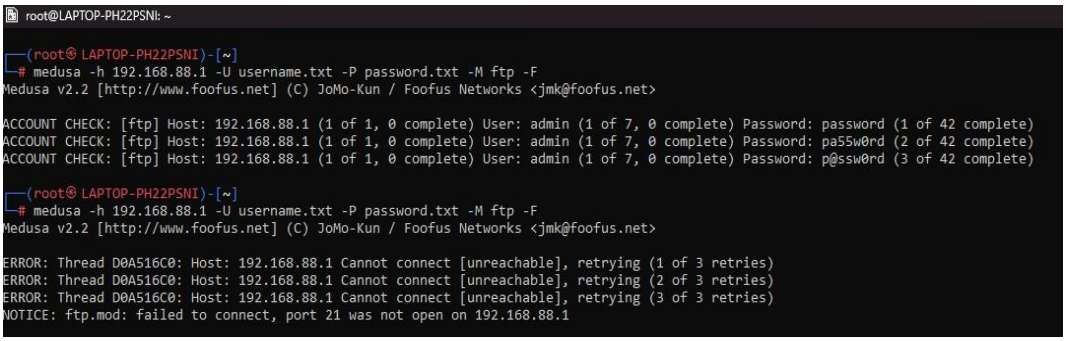
dari Gambar 7 bahwa ncrack tidak dapat memantau *username* dan *password SSH* yang terbuka di *Router* Mikrotik, Dapat di lihat pada gambar di bawah ini:



Gambar 7. *Brute Force SSH Exploit* Setelah Sistem *Firewall Rule*

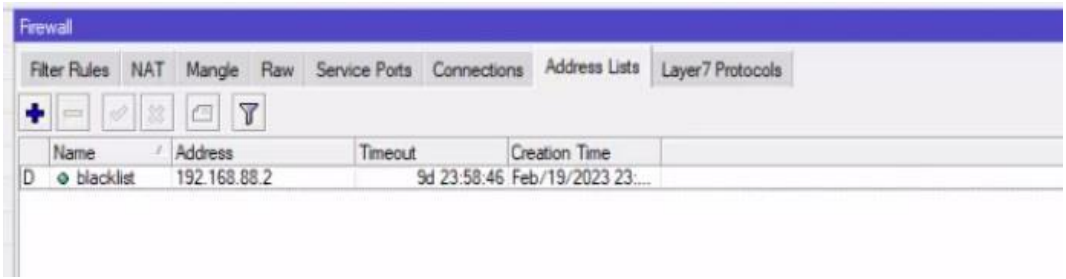
c. Pengujian *Brute Force FTP Exploit* Menggunakan Medusa

Pengujian Berikutnya dilakukan pada sistem yang telah diproteksi yaitu dengan Serangan *Brute Force FTP* Menggunakan *Tools* Medusa. Ketika penyusup melakukan serangan pada sistem atau mencoba masuk ke sistem, sistem dapat mendeteksi aktivitas. terlihat dari Gambar 8 bahwa Medusa tidak dapat memantau *username* dan *password FTP* yang terbuka di *Router* Mikrotik . Dapat di lihat pada gambar di bawah ini:



Gambar 8. *Brute Force FTP Exploit* Setelah Sistem *Firewall Rule*

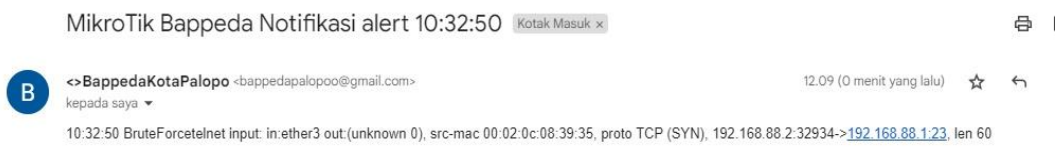
Rule Firewall yang dibuat telah melakukan tindakan pencegahan dengan mencegah penyerang melakukan operasi pemindaian. Dapat dilihat bahwa IP *address* yang mencoba melakukan Serangan *Brute Force* langsung diblokir.



Gambar 9. Pemblokiran *IP Address* Serangan *Brute Force*

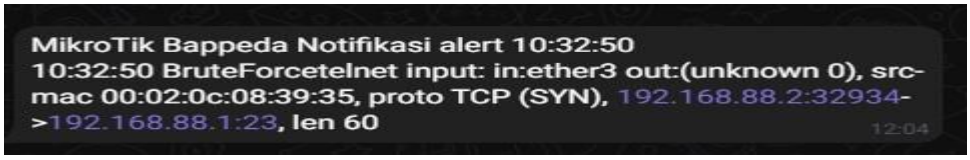
Mudzakkar[1], Siaulhak[2], Jumarniati[3]
DOI: https://doi.org/10.54443/sibatik.v2i4.718

Setelah Mendapatkan Serangan *Brute Force*, Router kemudian mengirimkan email notifikasi *alert* dari email yang sudah dihubungkan ke mikrotik



Gambar 10. Notifikasi *Alert* Serangan *Brute Force* Ke Email

Notifikasi *Alert* Serangan *Brute Force* juga dikirimkan ke telegram, sehingga apabila ada serangan *BruteForce* dapat cepat diketahui.



Gambar 11. Notifikasi *Alert* Serangan *Brute Force* Ke Telegram

Sehingga dapat ditarik kesimpulan bahwasanya menggunakan *Firewall Rule* yang di kombinasikan dengan *scheduler* notifikasi dapat membuat sistem jaringan yang aman dari serangan *Brute Force Exploit*, dapat dilihat pada tabel dibawah ini.

Tabel 1. Pengujian Sistem dengan Firewall Rule Brute Force

No.	Pengujian	Jenis Serangan	Hasil
1.	Pengujian 1	*Bruteforce telnet exploit menggunakan hydra*	Tidak dapat memantau *username & password login telnet* yang terbuka di router mikrotik. *Rule* pada *firewall* berhasil memblokir *IP address* dari pelaku yang sedang melakukan serangan, Serta Notifikasi Serangan *Bruteforce telnet* terkirim Ke Email dan Telegram.
2.	Pengujian 2	*Bruteforce ssh exploit menggunakan ncrack*	Tidak dapat memantau *username & password login ssh* yang terbuka di router mikrotik. *Rule* pada *firewall* berhasil memblokir *IP address* dari pelaku yang sedang melakukan serangan, Serta Notifikasi Serangan *Bruteforce ssh* terkirim Ke Email dan Telegram.

3.	Pengujian 3	*Bruteforce ftp exploit menggunakan medusa*	Tidak dapat memantau *username & password login ftp* yang terbuka di router mikrotik. *Rule* pada *firewall* berhasil memblokir *IP address* dari pelaku yang sedang melakukan serangan, Serta Notifikasi Serangan *Bruteforce ftp* terkirim Ke Email dan Telegram.

Sumber: Hasil Penelitian

PENUTUP

Kesimpulan

Berdasarkan hasil dari analisis dan pembahasan, maka dapat disimpulkan yaitu sebagai berikut:

1. Sebelum menggunakan *Firewall Filltering*, Serangan *Brute Force Exploit* dapat Melihat Username dan Password Login *Telnet , SSH, FTP* Pada Router Mikrotik. Setelah menggunakan *Firewall Filltering*, Serangan *Brute Force Exploit* tidak dapat Melihat Username dan Password Login *Telnet, Ssh, Ftp* Pada Router Mikrotik.
2. Notifikasi Alert Berfungsi dengan baik menyampaikan pesan serangan yang terjadi pada router.
3. Memberikan sistem keamanan pada jaringan dan dapat mengamanankan router mikrotik dari Serangan *Brute Force exploit* menggunakan aplikasi *Hydra, Ncrack* dan *Medusa*.

Saran

1. Peneliti selanjutnya sebaiknya melakukan penelitian yang lebih mendalam mengenai keamanan akses router mikrotik dengan mempertimbangkan kemungkinan metode serangan yang berbeda serta perkembangan teknologi yang semakin canggih.
2. Diharapkan penelitian selanjutnya melakukan penelusuran informasi terbaru dan memaksimalkan fasilitas dari perangkat router mikrotik untuk meningkatkan keamanan jaringan komputer secara efektif dan sesuai dengan kebutuhan instansi atau perusahaan.

DAFTAR PUSTAKA

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo, 12*(2), 35-38.

Armanto. (2017). Implementasi Jaringan Tunnel Berbasis Eoip (Ethernet Over Ip) dengan Mikrotik Router RB 2011 II-Rm di Silampari TV Lubuklinggau. *Jurnal Ilmiah Betrik* (Besemah Teknologi Informasi dan Komputer). *8*(1), 42-52.

Budiansyah, N., Widiarta, M., & Yunanri, W. (2020). Analisis Perbandingan Performa Freeradius dan Usermanager pada Mikrotik. *JINTEKS (Jurnal Informatika Teknologi dan Sains). 2*(3), 196-202.

Indah Sari Sinaga, D. ., Nurlaila, N., & Daim Harahap, R. . (2022). Analisis Penerapan Sak Etap Pada Bumdesa Yang Ada Di Kecamatan Pulo Bandring Kebupaten Asahan. Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(3), 97–118. https://doi.org/10.54443/sibatik.v1i3.16

Mohammad Arif, S. ., & Tri Habibie, M. . (2022). Analisis Perancangan Web E-Commerce Pt. Madani Sisfotel Sebagai Media Pemasaran Produk Umkm (Usaha Mikro Kecil Dan Menengah). Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(9), 1815–1824. https://doi.org/10.54443/sibatik.v1i9.240

Nurajizah, E. . (2022). Analisis Faktor Riwayat Kehamilan Dan Riwayat Bayi Terhadap Kejadian Stunting Pada Baduta Usia 6-24 Bulan Di Wilayah Kerja Puskesmas Palabuhanratu Sukabumi Tahun 2021. Sibatik Journal: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan, 1(6), 771–778. https://doi.org/10.54443/sibatik.v1i6.91

Rekno, D, P., & Daniel, A, P. (2018). *Sistem Informasi Pendeteksi Hama Penyakit Tanaman Padi Menggunakan Metode Fuzzy Tsukamoto Berbasis Android.* Jurnal Speed (Sentra Penelitian Engineering dan edukasi) . 10(2). 63-69.

Sisma, B. (2016). *Eksploitasi Pekerja Anak Pemulung.* Jurnal Equilibrum. 4(1). 77-86.

Pribadi, A., I., Rahmawati, Y., & Heningtyas, Y. (2021). Penerapan Algoritma *Brute Force* Pada Menu *Search* Website "Calonku" Dalam Rangka Pemilu Berbasis Web. *Jurnal Pepadun Ilmu Komputer Unila Publishing Network All Right Reserved. 2*(1), 60-70.

Sugiyono. (2016). Sistem Keamanan Jaringan Komputer Menggunakan Metode Watchguard Firebox pada PT. Guna Karya Indonesia. *Jurnal CKI On Spot. 9*(1). 1-8.