Majalah Ilmiah UPI YPTK
https://jmi-upiyptk.org/ojs
2020 Vol. 27 No. 2 Hal: 97-101 p-ISSN: 1412-5854, e-ISSN: 2502-8774

Sistem Monitoring Login Failure Dengan Via Telegram Dari Serangan Brutus Pada Router Mikrotik

Dian Kurnia[1], Juliandri[2]

[1]Sains dan Teknologi, Universitas Pembangunan Panca budi, Jl. Jend. Gatot Subroto Km 4,5 Medan
[2]Sains dan Teknologi, Universitas Pembangunan Panca budi, Jl. Jend. Gatot Subroto Km 4,5 Medan
email: andri@dosen.pancabudi.ac.id

Abstract

A monitoring system is needed to monitor a network topology from attacks that might occur at that time. A real-time monitoring system is needed to find out the attack. Therefore, in this study, an attack scenario on a proxy router was carried out using a brute force technique. The brute force technique is an efficient method that tries every possible login password character that the network administrator might use. This brute force technique already exists in the application used, namely Brutus. Brutus is executed by focusing the attack on port 23 telnet on the proxy router. The system log listed as a login failure caused by a brute attack on the proxy router will be forwarded by a script that is running to a notification with a network administrator telegram bot. From the results of research that has been carried out on the monitoring system on the proxy running in real time to notify the login failure message via telegram. The telegram notification will stop if the password has been found by Brutus or the Brutus dictionary does not find the password on the designed Mikrotik router network. Prevention is done by disabling open ports and activating the drop firewall menu if it finds a possible attacker's ip address on the mikrotik router to reduce attacks from the attacker.

Keywords: Login Failure, Mikrotik, Bot Telegram, Brute Force, Brutus

Abstrak

Sistem monitoring sangat diperlukan untuk memantau suatu topologi jaringan dari serangan yang mungkin saja terjadi saat itu juga. Dibutuhkan system monitoring yang secdara realtime untuk mengetahui serangn tersebut. Oleh karena itu dalam penelitian ini dilakukan skenario serangan pada router mikrotik dengan teknik brute force. Teknik brute force merupakan metode yang mangkus yang mencoba setiap kemungkinan karakter password login yang mungkin digunakan administrator network. Teknik brute force ini sudah ada pada aplikasi yang digunakan yaitu brutus. Brutus dijalankan dengan memfokuskan serangan pada port 23 telnet pada router mikrotik. Log system yang terlist login failure yang diakibatkan serangan brutus pada router mikrotik akan diteruskan oleh script yang di running ke notifikasi dengan bot telegram administrator network. Dari hasil penelitian yang telah dilakukan system monitoring pada mikrotik berjalan secara real time melakukan notifikasi pesan login failure melalui telegram. Notifikasi telegram akan berhenti jika password sudah ditemukan oleh brutus atau dictionary brutus tidak menemukan password yang ada pada jaringan router mikrotik yang di rancang. Pencegahan dilakukan dengan mendisable port yang terbuka dan mengaktifkan menu firewall drop jika menemukan kemungkinan ip address attacker pada router mikrotik untuk mengurangi serangan dari attacker.

Kata kunci: Login Failure, Mikrotik, Bot Telegram, Brute Force, Brutus

.

1. Pendahuluan

Perkembangan teknologi memungkinkan suatu perangkat jaringan di*remote* / diakses dari jarak jauh. Biasanya seorang administrator melakukan akses login pada suatu router untuk melakukan perbaikan dan monitoring jaringan untuk mengetahui apakah ada serangan yang masuk pada router[1]. Algoritma *brute force* adalah algoritma yang sederhana dan lempang yang dapat memecahkan masalah. Penyelesaian permasalahan password cracking pada login telnet port 23 mikrotik maka dengan menggunakan algoritma *brute force* akan mencoba menentukan panjang password tertentu dan memasukan dan

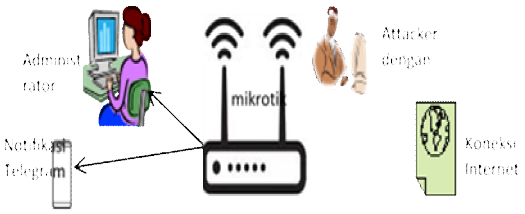
Diterima: 30-07-2020 | Revisi: 30-11-2020 | Diterbitkan: 30-12-2020 | DOI: 10.35134/jmi.v27i2.55

mengkombinasikan karakter tertentu sampai mendapatkan password yang sesuai[2]. Pengguna Algoritma *brute force* mengisi jumlah panjang karakter yang mungkin sesuai, dan memilih karakter set yang ada, maka akan di *generate* kombinasi karakter tersebut maka algoritma ini akan berhenti mencari jika menemukan solusi karakter yang sesuai dengan password asli yang telah di set pada aplikasi ataupun perangkat[3].

Penelitian sebelumnya, membahas beberapa aplikasi yang menggunakan teknik *brute force*, salah satunya aplikasi brutus yang digunakan secara *offline*, penelitian tersebut menghasilkan suatu kesimpulan teknik brute force akan berjalan lamban untuk menentukan password asli jika user mengeset password minimal 7 karakter dan kombinasi password yang terdiri dari kombinasi angka, huruf dan symbol[4]. Penelitian yang lain melakukan monitoring login dan logout secara realtime pada router mikrotik dengan notifikasi via telegram, pengecekan firewall UP atau DOWN bagi user yang melakukan ping berlebihan serta dapat memonitoring status cpu dan mengetahui jumlah user yang aktif pada jaringan hotspot [5].
Serangan crack login pada router mikrotik dengan teknik brute force mencoba semua karaktek yang mungkin di set oleh admin, hal ini perlu di monitoring menggunakan teknik notifikasi menggunakan via telegram bot oleh karena itu diperlukan bagaimana merancang suatu system yang realtime yang dapat mengidentifikasi langsung ketika *login failure* terjadi[6]. Pada dasarnya penelitian ini diperlukan dalam memonitoring suatu router untuk mengetahui aktifitas login ip address mana yang mengakses router mikrotik via telnet dan langsung notifikasi ke telegram[7]. Oleh karena itu penelitian ini mencoba merancang suatu scenario jaringan untuk memonitoring ip anymous mana saja yang mencoba login masuk dalam hal ini mengakses port 23 telnet pada router mikrotik. Skenario serangan juga di buat untuk mengetahui apakah system monitoring yang di rancang berjalan secara *realtime* dalam hal ini memberikan notifikasi via telegram dengan system bot telegram yang di rancang [8]. Serangan yang akan digunakan pada penelitian ini menggunakan serangan *offline* dengan aplikasi brutus yang setiap terjadi login *failure* akan dikirim notifikasi ke telegram.

2. Metode Penelitan

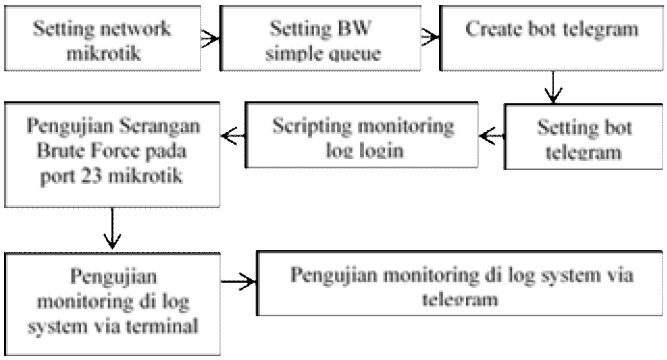
Rancangan gambar topologi selanjutnya peneliti mulai masuk ke pembahasan analisa keamanan pada login router mikrotik, untuk melakukan hal itu peneliti berencana melakukan serangan pada topologi jaringan 2 dengan melakukan attacker dan jenis serangan yang dilakukan berupa port serangan brute force menggunakan aplikasi brutus. Rancangan topologi jaringan dengan skema attacker dapat di lihat pada gambar 1 berikut :



Gambar 1 Skenario topologi jaringan yang dirancang

Pada gambar 1 di atas topologi jaringan sudah ditambahkan attacker dengan pemanfaatan jaringan LAN dan juga wireless, dimana IP gateway sumber internet adalah 192.168.43.1 kemudan ditransmitkan atau diroutekan kembali oleh router wireless dengan gateway 192.168.20.1. Skenario serangan attacker pertama dilakukan dengan memanfaatkan ether1 mikrotik yang terhubung internet.

Proses yang dilakukan selama penelitian hingga finalisasi dalam hal ini berupa implementasi router mikrotik dan monitoring log login system secara real time[9]s. Berikut bagan prosedur penelitian yang akan dilakukan.



Gambar 2 Tahapan-tahapan penelitian

Pada tahapan-tahapan penelitian perlu diketahui tahapan pertama dilakukan setting pada router mikrotik dengan skenario setting ip address, ip gateway, ip DNS Server. Diperlukan juga settingan management bandwidth (BW) yaitu akan dibatasi kecepatan bandwidth setiap client komputer pada laboratorium komputer LKP Medan Informatika Teknologi. Kebutuhan lainnya diperlukan settingan bot telegram yang mana bot ini menjadi server beta telegram khusus untuk mengirimkan pesan pesan yang terekam dari hasil log yang masuk pada log system mikrotik[10]. Kebutuhan selanjutnya dilakukan setting pada script agar router mikrotik secara realtime dapat mengirimkan hasil log system dengan notifikasi login failure pada router mikrotik. Script tersebut di set berjalan dan setiap 10 detik memonitoring dan mengirimkan notif ke ID kode telegram administrator network. Script ini berjalan jika skenario jaringan dilakukan yaitu serangan brute force dengan aplikasi brutus menyerang port yang terbuka yaitu port 23 (telnet) pada router mikrotik. Kemudian dilakukan pengumpulan data hasil log system setelah adanya serangan teknik brute force pada mikrotik. Hasil data notifikasi adanya login failure

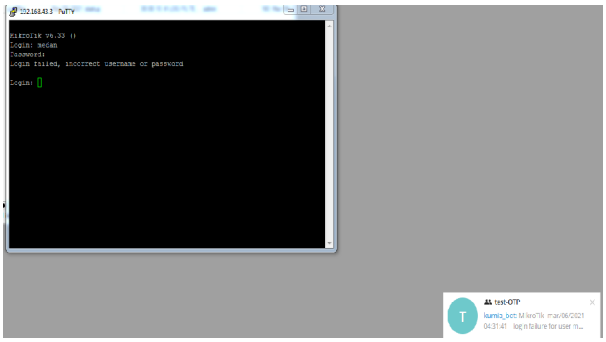
pengecekan langsung via terminal pada mikrotik dan pengecekan langsung pada telegram bot.

Parameter yang diamati berupa berapa banyak serangan brute force yang terjadi dan terdeteksi pada log system oleh router mikrotik dan di forward langsung ke administrator network dengan via telegram, login mana yang terjadi failure dan sumber ip mana yang menyerang.

3. Hasil dan Pembahasan

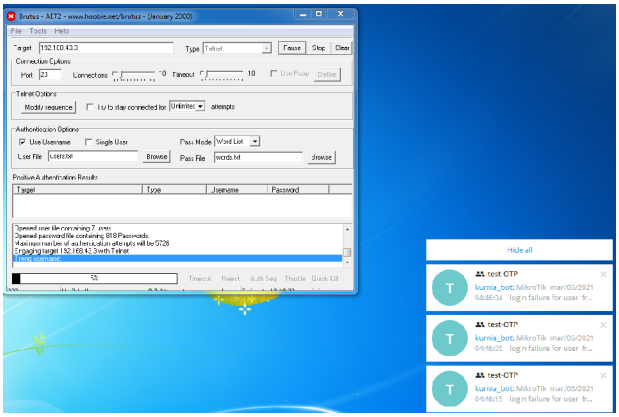
Pada aplikasi telegram di search botfather kemudian ketikan /start untuk membuat dan mengatur bot yang ingin dirancang. Untuk melanjutkan tahap selanjutnya membuat bot telebram versi yang dirancang diketikan perintah /newbot, kemudian dalam rancangan di buat bot dengan nama kurnia_bot, kemudian dicoba kembali dengan menggunakan nama bot yang lain yaitu : kurniamedanbot. Setelah berhasil maka akan didapat token untuk mengakses API dari HTTP. Token ini harus disimpan dengan aman karena bersifat rahasia untuk identitas dari bot kita. Secara langsung untuk meremote / komunikasi secara langsung jika token tersebut disisipkan pada coding php atau coding shell lainnya. Kemudian dilakukan /setjoingroups kemudian membuat member untuk sebuah group dalam hal di buat @kurniamedanbot, kemudian selanjutnya ketikan perintah Enable, untuk mengaktifkan bot dengan nama @kurniamedanbot dapat ditambahkan dalam sebuah group. Kemudian untuk mengecek nama bot yang telah dirancang dan di set maka ketikan /mybots.

Tahapan-tahapan pembuatan bot telah berhasil, dan ketika diketika perintah /mybots maka hasil kurnia_bot@kurniamedanbot. Hasil pengujian menggunakan aplikasi putty dengan dijalankan aplikasi putty dengan mengetikan ip address tujuan pilih port 23 telnet kemudian klik *connect*, akan tampil terminal baru kemudian ketikan *username* dan *password* yang sesuai dengan login router mikrotik. Jika *username* yang diinputkan tidak sesuai dengan username yang terdaftar pada list database mikrotik maka login teridentifikasi failure, identifikasi ini akan diteruskan link url API telegram, setiap 10 detik akan di kirim pesan via telegeram ke ID kode group seorang administrasi network, jika ada terindefikasi *login failure* pada *log system router* mikrotik yang dirancang dapat di lihat pada gambar 3 hasil login failure yang terindifikasi dan dinotifikasi melalui via telegram sebagai berikut :



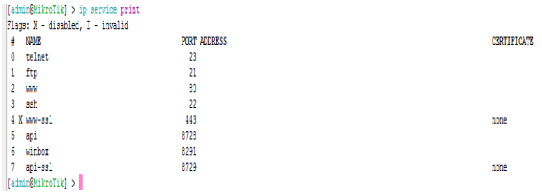
Gambar 3 Pengujian login menggunakan aplikasi putty via port 23

Pada gambar di atas pengujian masih sebatas salah input login username dan password di router mikrotik. Pengujian lainnya dapat di lihat pada pengujian serangan menggunakan aplikasi brutus. Adapun pengujian- pengujian serangan brute force pada port 23 telnet router mikrotik:



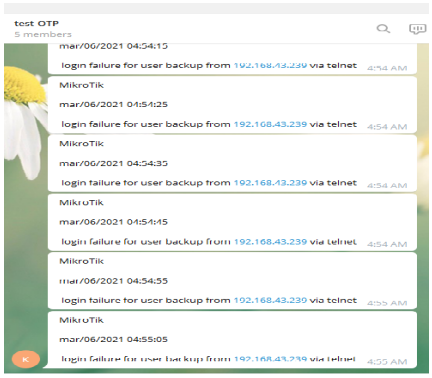
Gambar 4. Pengujian *login failure* dengan serangan aplikasi brutus

Cara kerja pengujian pada gambar di atas dengan menjalankan aplikasi brutus, kemudian ketikan ip target dalam hal ini ip ether1 mikrotik yaitu192.168.43.1 kemudian pilih fokus port yang terbuka untuk dijadikan target. Pada aplikasi brutus target port yang dapat diserang: http(Basic Auth), HTTP (form), FTP, POP3, Telnet, SMB (NetBios), Custom, NetBus. Pada pengujian ini dicontohkan serangan menggunakan port 23 yaitu port untuk Telnet. Jika port ini di open pada router mikrotik maka akan serangan menggunakan aplikasi brutus dengan teknik Brute Force, port yang terbuka pada mikrotik dapat diketik pada terminal mikrotik menggunakan perintah ip service print. Tampilan port yang terbuka pada router mikrotik yang di rancang dapat di lihat pada gambar 5 berikut :



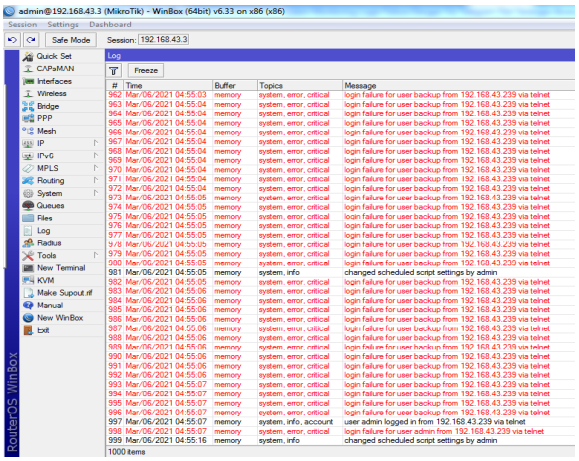
Gambar 5. Perintah *ip service print* menampilkan *port* yang terbuka pada router mikrotik

Pada gambar 5 diketahui tanda X berartiport tersebut disable tidak digunakan, jika ingin melakukan pencegahan serangan brutus maka porttelnet harus di ubah no portnya atau di disable service dari telnet tersebut. Hasil serangan brutus ketika melakukan cracking password menggunakan teknik brutus pada router mikrotik yang di rancang maka akan muncul login failure terus menerus dan berulang selama 10 detik. Hal ini karena brutus terus melakukan scanning pada port tersebut dan dicocokan dengan dictionary pada database brutus tersebut. Adapun gambar notifikasi telegram dapat di lihat pada gambar 6 berikut :



Gambar 6. Hasil pengujian *login failure* keseluruhan yang dinotifikasi kedalam bot telegram

Pada gambar 6 di atas diketahui sumber ip address dari penyerang yaitu 192.168.43.239 dengan username yang terakhir di coba oleh aplikasi brutus dengan userlist.txt yaitu backup dan password yang bervariatif. Notifikasi akan berhenti terkirim ke group telegram jika username dan password ditemukan atau username dan password tidak ditemukan sama sekali, dan brutus telah menscan semua isi dictionary dari userlist.txt dan wordlist.txt yang ada pada database brutus. Pengujian dilakukan yaitu dengan monitoring langsung via terminal pada aplikasi winbox mikrotik. Dengan login kedalam winbox, kemudian klik New Terminal. Adapun tampilan dapat di lihat pada gambar 7 berikut :



Gambar 7 Hasil log system terminal pada router mikrotik karena adanya serang brutus

Dari gambar di atas diketahui monitoring log system via terminal pada router mikrotik, dengan login didalam winbox, kemudian klik log menu. Akan tampil hasil log dari serangan teknik brute melalui aplikasi brutus. Proses pencocokan password sesuai dengan string yang terdapat pada dictionary userlist.txt dan wordlist.txt terjadi proses search sampai dengan 999 kali. Log system inilah yang di kirim ke group telegram yang didalamnya ada bot telegram yang di rancang. Pada proses 999 berhenti ketika ditest user = admin, serangan bersumber dari ip address 192.168.43.239, attacker memanfaatkan port 23 terbuka pada telnet.

4. Kesimpulan

Diketahui serangan dengan teknik *brute force* pada kasus *cracking password* login router mikrotik dapat terjadi karena ada port yang terbuka pada router mikrotik yang dirancang. Serangan *brute force* pada aplikasi brutus dapat menyerang *port* http(Basic Auth), HTTP (form), FTP, POP3, Telnet, SMB (NetBios), Custom, NetBus. Pada contoh kasus ini *port* telnet yang terbuka dapat menjadi jalur *attacker* untuk mencari *string* dari *username* dan *password* pada router mikrotik. Monitoring secara manual pada router mikrotik menggunakan via *log* pada fitur yang ada, sangatlah kurang efesien apabila network administrator tidak berada dekat dengan mikrotik. Monitoring secara *realtime* dengan memanfaatkan pesan-pesan pada *log system* router mikrotik diteruskan ke group telegram yang telah di set bot telegram didalamnya dapat menginformasikan langsung ke pihak administrator network. Pencegahan dapat dilakukan dengan men*disable* beberapa port yang terbuka khususnya yang menjadi sasaran serangan dari aplikasi brutus sendiri. Langkah yang lain dapat juga dilakukan drop pada ip sumber penyerang dan di *list* pada *firewall* router mikrotik.

Ucapan Terimakasih [jika ada]

Terima kasih kepada Fakultas Sains dan Teknologi UNPAB yang memfasilitasi untuk melakukan penelitian ini, serta LPPM Universitas Pembangunan Panca Budi (UNPAB) yang menjadi wadah untuk mengumpulkan penelitian ini, dan kepada periset sebelumnya yang saya ambil menjadi referensi dalam menunjang penelitian ini.

Daftar Rujukan

[1] Agung Sulistyo and Felix Andreas Sutanto, "Warning System Gangguan Konektivitas Jaringan Pada Bmkg Semarang Dengan Telegram Bot," *Pros. SINTAK 2018*, vol. ISBN: 978-, pp. 126–133, 2018.

[2] F. Teknologi, "Monitoring Jaringan Universitas Semarang Menggunakan the Dude Mikrotik Dengan Kombinasi (Semarang University Network Monitoring Using the Dude Mikrotik With Combination of Telegram Application Notifications)," vol. 7, no. 6, p. 2019, 2019.

[3] N. Fernando, Humaira, and E. Asri, "Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang," *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 4, pp. 121–126, 2020, doi: 10.30630/jitsi.1.4.17.

[4] K. E. Pramudita, "Brute Force Attack dan Penerapannya pada Password Cracking," no. 2011, p. 6, 2011.

[5] D. K. Hakim and S. A. Nugroho, "Implementasi Telegram Bot untuk Monitoring Mikrotik Router," *Sainteks*, vol. 16, no. 2, pp. 151–157, 2020, doi: 10.30595/st.v16i2.7132.

[6] D. Tri Atmaja, E. Budhy Prasetya, and P. Edi Kresnha, "Notifikasi Adanya Serangan Pada Jaringan Komputer Dengan Mengirim Pesan Melalui Aplikasi Telegram Dan Kontrol Server," *J. Univ. Muhammadiyah Jakarta*, pp. 1–8, 2018.

[7] R. Juniyantara Putra, N. Putra Sastra, and D. M. Wiharta, "Pengembangan Komunikasi Multikanal Untuk Monitoring Infrastruktur Jaringan Berbasis Bot Telegram," *J. SPEKTRUM*, vol. 5, no. 2, p. 152, 2018, doi: 10.24843/spektrum.2018.v05.i02.p19.

[8] B. Rifai, N. Nuryadi, and A. Ripai, "Implementasi Telegram Notification Alert Pada Network Monitoring System Dengan Nagios," *J. Mantik Penusa*, vol. 3, no. 3, pp. 54–60, 2019, [Online]. Available: http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/659.

[9] A. Dan, P. Manajemen, D. Menggunakan, M. Rb, and P. P. P. M. A. Jambi, "' Analisis Dan Pengembangan Manajemen Jaringan Dengan Menggunakan Mikrotik Rb750 Pada Ppm Al-Hidayah Jambi ,'" vol. 5, no. 1, 2020.

[10] S. Monitoring, "Sistem Monitoring Jaringan Load balancing Dengan Metode Equal Cost Multipath (ECMP) Menggunakan Media Telegram," vol. 4, pp. 18–33, 2019.