Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

RANCANG BANGUN SISTEM KEAMANAN JARINGAN MIKROTIK MENGGUNAKAN FIREWALL FILTERING DAN PORT KNOCKING DENGAN NOTIFIKASI TELEGRAM PADA EVENT VIRTUAL

Febri[1], Ellbert Hutabri[2]

[1]Mahasiswa Program Stud Teknik Informatika, Universitas Putera Batam
[2] Dosen Program Studi Teknik Informatika, Universitas Putera Batam
email: pb190210090@upbatam.ac.id

ABSTRACT

Network security is a very important aspect in maintaining information security. In network management using proxy devices, use of firewall filtering and port knocking in an effort to increase security and control network access and hide services that are not needed. In addition to obtaining information on suspicious network activity in real-time with telegram notifications. The method used includes analysis of network security needs, system architecture design, firewall filtering and port knocking configurations on the proxy and integration with the telegram API to send notifications. The results of this study show that using firewall filtering and port knocking on Mikrotik can effectively improve network security by limiting unauthorized access and reducing the risk of attacks from outside. The system is also capable of providing notifications via telegram when suspicious activity is detected, thus enabling a network administrator to respond quickly to these threats

Keywords: *Computer Networks, Firewall Filtering, Mikrotik Routers, Telegram*

PENDAHULUAN

Dengan perkembangan jaringan yang yang ada pada saat ini tentunya ancaman keamanan jaringan juga akan beragam seperti ancaman keamanan jaringan *port scanning, brute force* dan DDoS *(Distributed Denial Of Service)* (Saputro et al., 2020). *Event virtual* merupakan sebuah acara yang dilakukan secara *online* melalui sebuah perangkat elektronik yang terhubung ke internet. maka diperlukan sebuah keamanan lebih supaya sebuah *event* dapat berjalan dengan lancer yaitu seseorang yang bertanggung jawab dalam *memonitoring* dan menjamin sebuah acara dapat berjalan sebagaimana mestinya. Dalam mengantisipasi ancaman terhadap keamanan jaringan maka diperlukanlah sebuah tindakan dalam upaya mencegah terjadinya pencurian data, percobaan memasuki sebuah sistem oleh pihak yang tidak sah dalam hak akses dimana proses mekanisme jaringan membutuhkan router mikrotik dalam memanagement jaringan dengan tujuan jaringan dapat digunakan secara efektif tanpa gangguan.

Fungsi utama router mikrotik dalam penelitian ini untuk memberikan kemudahan bagi seorang *administrator* jaringan dalam *memonitoring,*

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

mengkonfigurasi, dan melakukan *troubleshooting* jaringan. Penelitian ini bertujuan untuk melakukan perancangan dan mengimplementasikan sistem keamanan jaringan menggunakan *firewall filtering* dan *port knocking* pada perangkat mikrotik dengan fitur tambahan berupa *notifikasi* melalui telegram, dengan adanya fitur tambahan dari aplikasi telegram diharapkan dapat mengurangi resiko serangan dari luar dan sistem juga dapat memberikan notifikasi melalui telegram jika terdeteksi adanya aktivitas yang mencurigakan.

KAJIAN TEORI

Penelitian ini memiliki beberapa referensi dalam melakukan peneliti ini yang berkaitan dengan perancangan keamanan jaringan diantaranya jurnal penelitian (Fernando et al., 2020) yang berjudul "Monitoring jaringan dan notifikasi dengan telegram pada dinas komunikasi dan informatika kota padang" menjelaskan implementasi dan monitoring keamanan jaringan dengan cacti dan menggunakan notifikasi pada telegram dengan adanya notifikasi pada telegram seorang *administrator* jaringan tidak lagi perlu untuk mengecek keamanan jaringan secara manual supaya *monitoring* jaringan cacti berjalan dengan baik maka kualitas jaringan internet juga diperbaiki supaya pemberitahuan ancaman terhadap sistem keamanan jaringan dapat tersampaikan kepada administrator. aplikasi telegram memiliki ip private yang dapat diakses hanya pada jaringan lokal yang sama sedangkan untuk memonitoring keamanan jaringan menggunakan telegram dapat dilakukan dimana saja. Jurnal penelitian (Mulyanto et al., 2021) yang berjudul implementasi port knocking untuk keamanan jaringan smkn 1 sumbawa besar mejelaskan bahwa serangan terhadap keamanan jaringan dapat dilakukan melalui celah celah pada jaringan komputer salah satunya melalui port yang terbuka yang dapat memberikan akses bagi pihak pihak yang tidak berhak dalam mengaksesnya dimana peneliti mencoba untuk memasukan *ip address* router melalui port 80 (browser atau http), port 22 (ssh) dan port 23 untuk telnet yang mana akan menampilkan interface login ke router.

2.1 jaringan

Jaringan adalah kumpulan perangkat komputer yang terhubung untuk berbagi sumber daya dan berkomunikasi satu sama lain. Jaringan memungkinkan perangkat seperti komputer, printer, server, dan perangkat lain untuk berkomunikasi satu sama lain dan berbagi informasi (Haeruddin, 2021).

Jaringan komputer menurut (Amarudin, 2018) merupakan gabungan dari teknologi telekomunikasi dengan teknologi komputer yang akan menghasilkan suatu pengolahan data.

Jaringan komputer juga dapat diartikan sebagai bentuk pertukaran data/informasi yang dikirimkan oleh pengirim *(transmitter)* dapat sampai ke penerima *(receiver)* dengan tepat dan akurat(Mulyanto et al., 2021).

Menurut (Samsumar & Hadi, 2018) jenis jaringan dan daerah jangkauannya dikelompokkan sebagai berikut:

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Local Area Network (LAN)

Jaringan *local area network* merupakan sebuah jaringan yang daerah area cangkupannya terbatas seperti ruangan, gedung, atau kampus kecil.

Wide Area Network (WAN)

Jaringan yang daerah area cangkupanya lebih luas seperti antar kota atau negara. Jaringan WAN adalah jaringan yang menghubungkan jaringan lan lokal yang tersebar geografis dan biasanya menggunakan infrastruktur seperti telephon, serat optic atau koneksi satelit.

Metropolitan Area Network (MAN)

Jaringan ini mencangkup area yang lebih luas dari LAN, seperti kota atau wilayah metropolitan.

2.2 jenis serangan keamanan jaringan

jenis serangan yang sering terjadi pada keamanan jaringan diantaranya sebagai berikut :

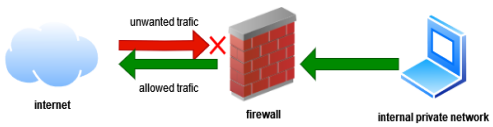
1. Serangan DDoS: Serangan Distribusi Layanan (DDoS) bertujuan untuk membuat jaringan atau layanan tidak tersedia dengan membanjiri lalu lintas jaringan atau sumber daya dengan serangan dari banyak perangkat yang terdistribusi.(Gregorius Hendita Artha Kusuma, 2022) Hal ini dapat mengakibatkan gangguan berat pada operasi jaringan.
2. *Brute force* adalah metode serangan yang mencoba semua kombinasi mungkin secara berurutan untuk memecahkan kata sandi atau mengakses suatu sistem yang dilindungi(Mulyanto et al., 2022)
3. *Port Forwading* adalah proses penjelajahan sistem atau jaringan untuk mengidentifikasi port yang aktif atau terbuka pada perangkat tujuan(Mulyanto et al., 2022)

2.3 Mikrotik

MikroTik RouterOS dan perangkat kerasnya banyak digunakan oleh ISP *(Internet Service Provider),* penyedia layanan Wi-Fi, perusahaan, institusi pendidikan, dan bahkan oleh pengguna rumahan yang memiliki kebutuhan jaringan yang kompleks (Samsumar & Hadi, 2018)

2.4 Firewall Filtering

Tujuan utama dari firewall filtering adalah melindungi jaringan dari ancaman eksternal dan mencegah akses yang tidak sah atau tidak diinginkan ke sistem atau data yang ada di dalam jaringan.(Rizal et al., 2020).



Gambar 1. Cara kerja Firewall
Sumber: (Data Penelitian, 2023)

Terdapat beberapa langkah kerja firewall sebagai berikut(Rizal et al., 2020)

1. Pengecekan paket : ketika ada sebuah paket yang masuk ataupun keluar maka *firewall* akan memeriksanya terlebih dahulu.
2. Evaluasi paket : setelah paket diterima maka *firewall* akan mengevaluasi paket tersebut.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

3. Pengambilan keputusan: setelah dievaluasi *firewall* akan memberikan keputusan apakah paket tersebut akan di lanjut atau dikembalikan
4. *Logging* dan *Monitoring* : selama proses *filtering, firewall* juga akan mencatat informasi paket yang diterima

2.5 Port knocking

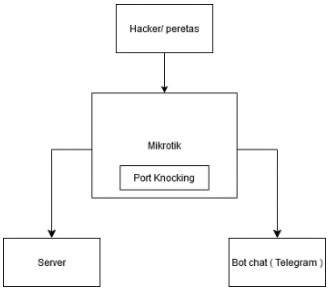
Merupakan sebuah metode sistem *autentifikasi* yang dibuat khusus untuk jaringan. *Port knocking* juga dapat dikatakan sebuah metode yang digunakan untuk menyembunyikan port yang terbuka pada sebuah sistem atau jaringan. (Mulyanto et al., 2021)

2.6 Telegram Bot

Telegram bot merupakan program komputer yang menjalankan tugas-tugas otomatis di aplikasi Telegram.(Fernando et al., 2020) Bot ini berinteraksi dengan pengguna melalui pesan, memberikan respon, menyediakan informasi, menjalankan perintah, atau melakukan tugas lainnya sesuai dengan fungsionalitas yang telah ditentukan(Sastrawangsa, 2017)

2.7 Kerangka Berpikir

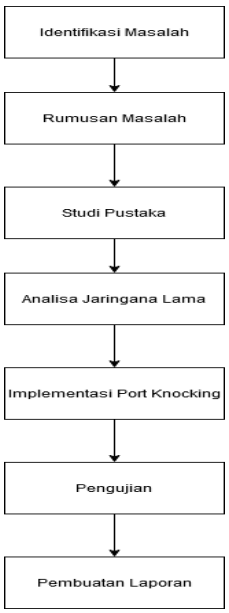
Gambaran ketika ada seseorang yang hendak mencoba untuk memasuki sebuah sistem keamanan jaringan dengan cara yang tidak sah dan alur penerimaan notifikasi ke server dan aplikasi telegram.



Gambar 2. Kerangka pemikiran
Sumber: (Data Penelitian, 2023)

METODE PENELITIAN

Dalam penelitian ini peneliti menggunakan analisis kualitatif yang bersifat kualitatif. Dikarenakan dalam penelitian ini menggambarkan suatu objek yang diteliti. Adapun tahapan dalam analisa dan perancangan keamanan jaringan sebagai berikut:



Gambar 3. Tahapan Metode Penelitian
Sumber: (Data Penelitian, 2023)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

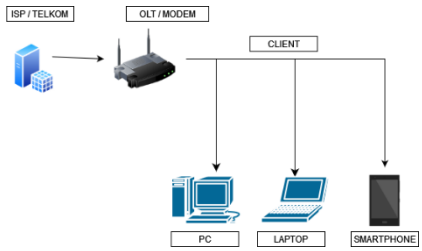
Jurnal Comasie

ISSN (Online) 2715-6265

Metode yang digunakan dalam penelitian ini yakni dengan menggunakan cara pendekatan observasi dan wawancara yang mana peneliti langsung mendatangi tempat yang akan menjadi objek penelitian dan dapat diambil kesimpulan.

3.1 Rancangan Jaringan yang sedang Berjalan

Berdasarkan hasil observasi dan wawancara yang dilakukan pada PT.Shanaya Creativo Innovation peneliti memperoleh informasi bahwa keamanan jaringan diperusahaan ini masih bergantung pada perangkat komputer saja dalam memonitoring keamanan jaringan. Adapun analisis jaringan lamanya sebagai berikut :

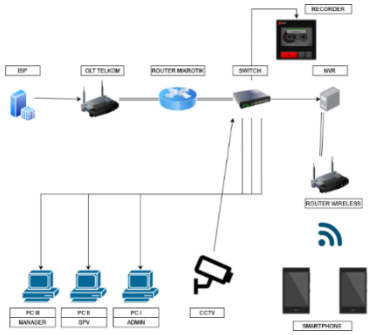


Gambar 4. Rancangan Jaringan Lama
Sumber: (Data Penelitian, 2023)

Kelemahan pada rancangan jaringan yang sedang berjalan:

1. Jaringan yang sedang berjalan belum menggunakan mikrotik dalam konfigurasi jaringan
2. .hanya mengandalkan layanan dari ISP *(Internet service Provider)*

3.2 Rancangan Jaringan yang Diusulkan



Gambar 5. Rancangan Jaringan Baru
Sumber: (Data Penelitian, 2023)

Berdasarkan gambaran diata dapat dijelaskan dengan menambahkan sebuah perangkat mikrotik untuk dapat memantau lalu lintas jaringan serta menambahkan sebuah smartphone yang telah terinstal sebuah aplikasi telegram yang berguna untuk memberikan sebuah pesan peringatan jika terjadi sebuah ancaman serangan terhadap jaringan.

3.3 Tahapan rencana implementasi

1. menyiapkan perangkat mikrotik yang akan digunakan untuk konfigurasi jaringan
2. terdapat beberapa tahapan dalam mengkonfigurasi mikrotik diantaranya
   a. melakukan konfigurasi dasar pada mikrotik dengan membuat dhcp *client* dan dhcp *server* dan melakukan NAT *(Network Addressing Translation)* agar *client* nantinya mendapatkan akses internet.
   b. membuat kebijakan tentang keamanan yang nantinya akan diterapkan pada firewall mikrotik.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

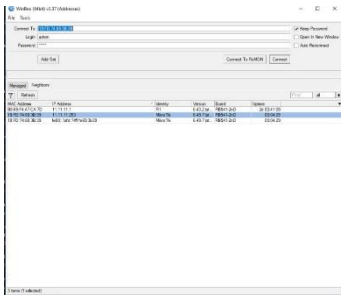
ISSN (Online) 2715-6265

c. membuat aturan pembatasan hak akses serta pemblokiran bagi pihak yang tidak berhak dalam mengaksesnya.
d. membuat aturan pada firewall menjadi dinamis supaya dapat membuka port tertentu yang dapat diakses.

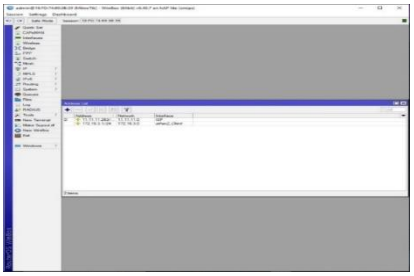
3. Integrasi notifikasi telegram

HASIL DAN PEMBAHASAN

Dalam melakukan konfigurasi dan memantau lalu lintas jaringan dikarenakan aplikasi ini dapat memberikan kemudahan bagi peneliti dalam mengkonfigurasi jaringan secara statis maupun dinamis Untuk mikrotik, terlebih dahulu pengguna menginstall aplikasi *winbox*



Gambar 6. Tampilan Awal *Winbox*
Sumber: (Data Penelitian, 2023)



Gambar 7. Home Tool *Winbox*
Sumber: (Data Penelitian, 2023)

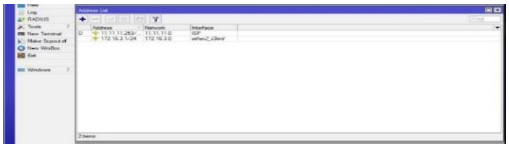
Tabel 1. Pengalamatan IP

IP Address	Device	Subnet	Internet	Note
11.11.11.2/24	Router Mikrotik	255.255.255.0	NAT	Ether 1
172.16.3.1	Router Mikrotik	255.255.255.0	NAT	Ether 2/Gateway
172.16.3.2-254	Client	255.255.255.0		Host:254
172.16.3.2-254	Laptop & Smartphone	255.255.255.0		Wlan 1 Bridge

Sumber: (Data Penelitian, 2023)

4.1 Konfigurasi Alamat ip

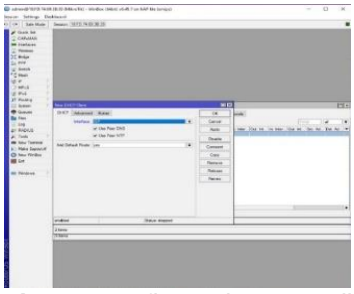
Pada konfigurasi alamat ip peneliti memasukan ip *address* 11.11.11.2/24 sesuai dengan tabel ip diatas



Gambar 8. Konfigurasi Alamat Ip
Sumber: (Data Penelitian, 2023)

4.2 Konfigurasi DHCP Client

Tujuan dari *DHCP Client* pada MikroTik adalah untuk mengkonfigurasi secara otomatis alamat IP dan pengaturan jaringan lainnya pada perangkat *MikroTik*



Gambar 9. Konfigurasi DHCP Client
Sumber: (Data Penelitian, 2023)

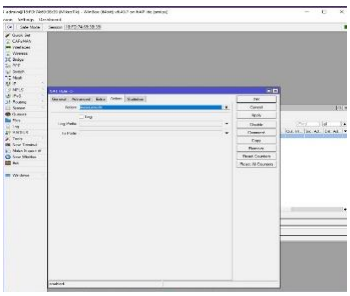
Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

4.3 Konfigurasi NAT

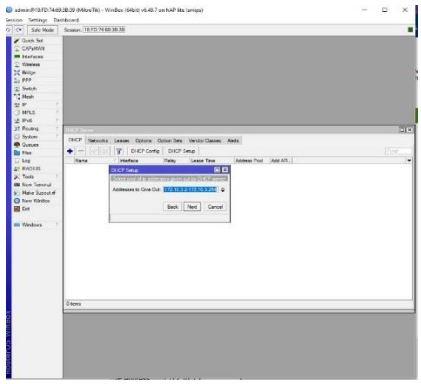
Selanjutnya melakukan setingan pada Nat agar jaringan lokal mendapatkan akses internet. Tahapan langkah-langkahnya dengan cara klik IP → *Firewall* → NAT → *General* (*chain-srcnat*) → *action* → *masquerade*



Gambar 10. Konfigurasi NAT
Sumber: (Data Penelitian, 2023)

4.4 Konfigurasi DHCP Server

Tahapan yang dilakukan dalam mengkonfigurasi DHCP server adalah dengan cara mengklik Ip → *DHCP Server* → Pilih *Interface* eth 2 → Masukan *DHCP Address space* 172.16.3.0/ 24 → Masukan *gateway* 172.16.3.1 → *Address to give out* (172.16.3.2-254)



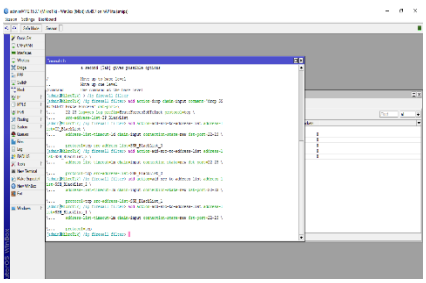
Gambar 11. Konfigurasi DHCP Server
Sumber: (Data Penelitian, 2023)

4.5 Konfigurasi Firewall Rule Pada mikrotik

Pada konfigurasi ini melakukan *firewall rule* pada mikrotik dengan tujuan mengidentifikasi jenis serangan pada jaringan. Adapun rule yang akan di konfigurasi pada mikrotik adalah

4.5.1 Brute force SSH dan telnet

Pada *rule brute force* SSH dan telnet proses ini akan melewati port 22 untuk SSH dan 23 untuk telnet. Untuk mengetahui jenis serangan yang terjadi maka pada router *winbox administrator* jaringan akan mengkonfigurasi *firewall rule* yang mana nantinya dapat mengetahui jenis serangan yang sedang terjadi.



Gambar 12. Konfigurasi Brute force SSH dan Telnet
Sumber: (Data Penelitian, 2023)

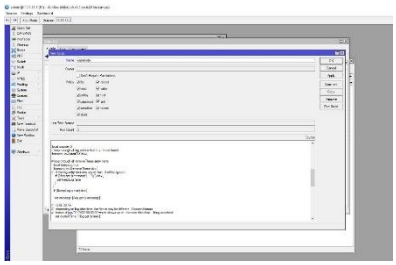
4.6 Konfigurasi Log Mikrotik

Pada tahapan ini melakukan konfigurasi pada router mikrotik melalui *winbox* agar ketika terjadi serangan router mengirimkan pesan ke telegram melalui *botID* dan *chatID* pada API telegram. Pada *System-Script* masukan *source code*. ketika terjadi suatu serangan maka aplikasi telegram akan selalu mendapatkan notifikasi pemberitahuan yang mana ini tujuan ketika pengguna melakukan konfigurasi pada *log mikrotik.*

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

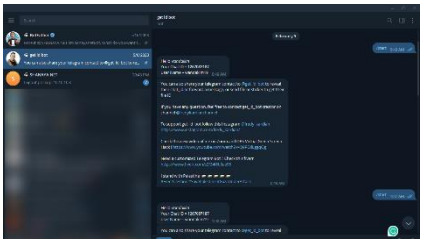
ISSN (Online) 2715-6265



Gambar 13. Konfigurasi Log Mikrotik
Sumber: (Data Penelitian, 2023)

4.7 Konfigurasi Telegram

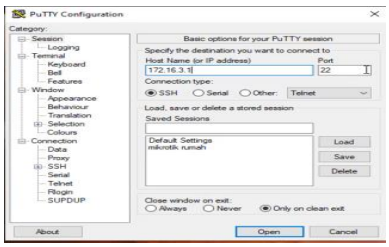
Melakukan konfigurasi *chabot* ke telegram untuk mendapatkan *Bot ID* dan nomor ID dan token yang akan digunakan untuk konfigurasi pada *winbox* yang mana nantinya pengguna dapat melihat serta memantau keamanan jaringan melalui aplikasi telegram.



Gambar 14. *Chat Id Bot*
Sumber: (Data Penelitian, 2023)

4.8 Pengujian Serangan

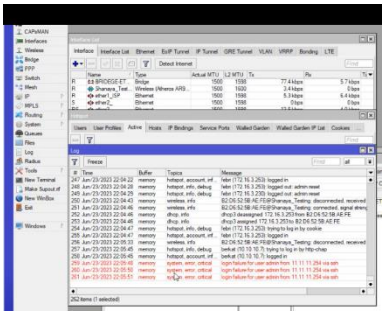
Pada pengujian serangan *Brute Force SSH dan Telnet* penguji menggunakan aplikasi *PUTTY*



Gambar 14. Konfigurasi pada Putty
Sumber: (Data Penelitian, 2023)

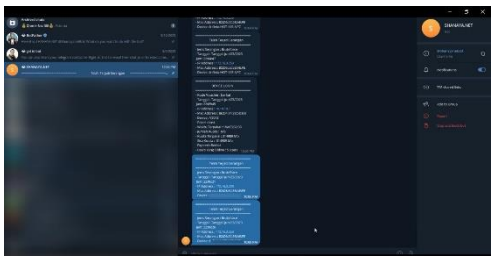
pada langkah berikutnya penguji akan memasukan *username* dan *pasword* yang salah untuk menguji serangan *brute force SSH* dan *telnet* pada *terminal*.

Maka pada *log winbox* terdeteksi sebanyak 3 kali serangan *brute force* dari IP pelaku yaitu 172.16.3.1 melakukan serangan *brute force* yang di tunjukan pada gambar 4.23. Pada *firewall rule* yang di atur adalah apabila pelaku melakukan serangan *brute force ssh* dan *telnet* sebanyak 3 kali maka *IP client* akan diblokir selama 1 hari.



Gambar 15. Pemberitahuan pada Log Winbox
Sumber: (Data Penelitian, 2023)

Ketika terjadi serangan maka akan terdeteksi oleh aplikasi *winbox* dan secara otomatis akan mengirimkan notifikasi ke telegram



Gambar 14. Notifikasi *Telegram Brute force SSH* dan *Telnet*
Sumber: (Data Penelitian, 2023)

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

Kesimpulan

Dari hasil penelitian yang dilakukan di PT. Shanaya Creativo Innovation dan dilakukan perancangan dan diimplementasikan dalam bentuk pengujian maka dapat disimpulkan sebagai berikut :

1. penggunaan router mikrotik dan aplikasi *winbox* dapat memberikan kemudahan bagi seorang *administrator* jaringan dalam mengkonfigurasi dan menjaga keamanan jaringan.
2. dengan menggunakan aplikasi tambahan telegram seorang *administrator* jaringan tidak lagi harus menggunakan komputer atau laptop dalam memantau aktivitas jaringan.

Saran

1. dalam penelitian ini peneliti hanya membahas mengenai cara mengidentifikasi jenis serangannya saja dan belum dengan cara mengatasinya diharapkan untuk peneliti yang hendak meneliti dengan topik yang sama dapat dikembangkan cara mengatasinya juga.
2. dalam penelitian ini peneliti hanya berfokus pada satu jenis serangan saja diharapkan untuk penelitian selanjutnya dapat dikembangkan.

DAFTAR PUSTAKA

Amarudin, A. (2018). Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking. *Jurnal Teknoinfo*, *12*(2), 72. https://doi.org/10.33365/jti.v12i2.121

Fernando, N., Humaira, & Asri, E. (2020). Monitoring Jaringan dan Notifikasi dengan Telegram pada Dinas Komunikasi dan Informatika Kota Padang. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *1*(4), 121–126. https://doi.org/10.30630/jitsi.1.4.17

Gregorius Hendita Artha Kusuma. (2022). Sistem Firewall untuk Pencegahan DDOS ATTACK di Masa Pandemi Covid-19. *Journal of Informatics and Advanced Computing (JIAC)*, *3*(1).

Haeruddin, H. (2021). Analisa dan Implementasi Sistem Keamanan Router Mikrotik dari Serangan Winbox Exploitation, Brute-Force, DoS. *Jurnal Media Informatika Budidarma*, *5*(3), 848. https://doi.org/10.30865/mib.v5i3.2979

Mulyanto, Y., Herfandi, H., & Candra Kirana, R. (2022). ANALISIS KEAMANAN WIRELESS LOCAL AREA NETWORK (WLAN) TERHADAP SERANGAN BRUTE FORCE DENGAN METODE PENETRATION TESTING (Studi kasus:RS H.LMANAMBAI ABDULKADIR). *Jurnal Informatika Teknologi Dan Sains*, *4*(1), 26–35. https://doi.org/10.51401/jinteks.v4i1.1528

Mulyanto, Y., Julkarnain, M., & Afahar, A.

Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

J. (2021). Implementasi Port Knocking Untuk Keamanan Jaringan Smkn 1 Sumbawa Besar. *Jinteks*, *3*(2), 326–335.

Rizal, R., Ruuhwan, R., & Nugraha, K. A. (2020). Implementasi Keamanan Jaringan Menggunakan Metode Port Blocking dan Port Knocking Pada Mikrotik RB-941. *Jurnal ICT : Information Communication & Technology*, *19*(1), 1–8. https://doi.org/10.36054/jict-ikmi.v19i1.119

Samsumar, L. D., & Hadi, S. (2018). Samsumar, L. D., & Hadi, S. (2018). Pengembangan Jaringan Komputer Nirkabel (Wifi) Menggunakan Mikrotik Router (Studi Kasus Pada SMA PGRI Aikmel). *Jurnal METHODIKA*, *4*(1), 1–9.

Saputro, A., Saputro, N., Wijayanto, H., & Informatika, P. S. (2020). Metode Demilitarized Zone Dan Port Knocking Untuk Demilitarized Zone and Port Knocking Methods for Computer. *Metode*, *3*(2), 22–27.

Sastrawangsa, G. (2017). Pemanfaatan Telegram Bot Untuk Automatisasi Layanan Dan Informasi Mahasiswa Dalam Konsep Smart Campus. *Konferensi Nasional Sistem & Informatika*, 773.

	Febri Merupakan Mahasiswa Prodi Teknik Informatika Universitas Putera Batam.
	Ellbert Hutabri Merupakan Dosen Prodi Teknik Informatika Universitas Putera Batam.