Implementasi *Monitoring* Keamanan Jaringan Menggunakan *Port Knocking* Berbasis *Telegram*

Herdi Setiadi[1], Dini Rohmayani[2], Rangga Satria Perdana[3]

[1,2] *Program Studi Teknik Informatika- Politeknik TEDC Bandung*

[3] *Program Studi Sistem Informasi- Universitas Sangga Buana Bandung*

Jl. Politeknik-Pesantren KM2 Cibabat Cimahi Utara – Cimahi Jawa Barat - Indonesia

stdherdis@gmail.com, dinirohmayani@poltektedc.ac.id, rangga.satria@usbypkp.ac.id

Abstrak— Seiring dengan kemajuan teknologi digital, jaringan komputer menjadi lebih rentan terhadap serangan siber seperti *hacking* dan malware. Kelemahan pada sistem keamanan, terutama pada *router*, seperti autentikasi yang lemah dan konfigurasi yang tidak aman, dapat membuat jaringan mudah dieksploitasi. Penelitian ini bertujuan untuk meningkatkan keamanan jaringan dengan menerapkan metode *port knocking* pada *router* MikroTik yang terhubung dengan notifikasi *real-time* melalui Telegram. Penelitian ini menggunakan metode *Network Development Life Cycle (NDLC)* dengan lima tahapan: *Analysis, Design, Simulation Prototyping, Implementation, dan Monitoring*. Uji coba dilakukan di kantor desa Jalatrang, kabupaten Ciamis, di mana ditemukan kelemahan dalam keamanan jaringan, khususnya pada *login router* MikroTik. Metode *port knocking* digunakan untuk menyembunyikan *port* penting dan hanya membukanya setelah urutan "ketukan" yang benar dilakukan. Integrasi dengan Telegram juga memberikan notifikasi *real-time* yang membantu administrator menerima informasi notifikasi lebih cepat. Jenis serangan yang diujikan menggunakan *port scanning*. Hasil pengujian menunjukkan bahwa metode *port knocking* berhasil meningkatkan keamanan jaringan dengan menyembunyikan port seperti winbox dari pemindai, sehingga mengurangi risiko akses yang tidak sah. Penggunaan Telegram terbukti mempermudah pengelolaan dan pemantauan *router* MikroTik. Implementasi *port knocking* berbasis Telegram ini efektif dalam meningkatkan keamanan dan mempermudah pengelolaan jaringan secara keseluruhan.

Kata Kunci*— keamanan jaringan, *port knocking*, *port scanning*, *real-time*, telegram, *NDLC

Abstrack*— *Digital technology advancements have increased the vulnerability of computer networks to cyberattacks such as hacking and malware. Weaknesses in security systems, particularly in routers—such as weak authentication and insecure configurations—can make networks easy to exploit. This study aims to enhance network security by implementing a port knocking method on MikroTik routers, with real-time notifications via telegram. The research employs the Network Development Life Cycle (NDLC) method, which includes five phases: Analysis, Design, Simulation Prototyping, Implementation, and Monitoring. Testing was conducted at the Jalatrang village office in Ciamis Regency, where security vulnerabilities, particularly in MikroTik router logins, were identified. The port knocking method obscures important ports, opening them only after the correct sequence of "knocks" is performed. Integration with Telegram provides real-time notifications, helping administrators receive information more quickly. Port scanning was used to test various attack scenarios. Results indicate that the port knocking method successfully improved network security by concealing ports such as Winbox from scanners, thereby reducing the risk of unauthorized access. The use of telegram facilitated the management and monitoring of MikroTik routers. Implementing port knocking with Telegram-based notifications proves effective in enhancing security and streamlining overall network management.

Keyword*— *Network Security, port knocking, port scanning, real-time, telegram, NDLC.

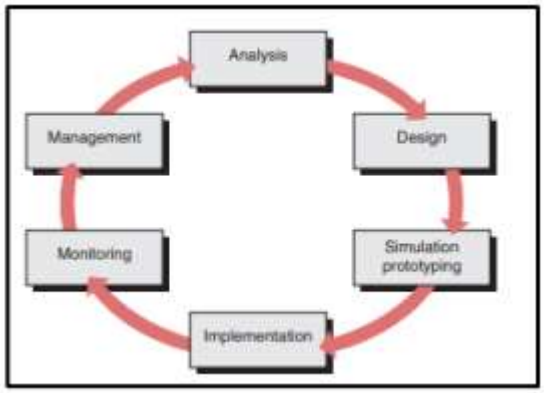
I. PENDAHULUAN

Keamanan jaringan merupakan aspek krusial dalam melindungi informasi dan sistem dari berbagai ancaman siber. Salah satu ancaman yang sering dihadapi adalah serangan *web defacement*, di mana penyerang mengeksploitasi kerentanan pada situs *web* atau *server web* untuk merusak, memodifikasi, atau menghapus konten halaman *web*. Tahun 2022, Badan Siber dan Sandi Negara (BSSN) mencatat sebanyak 2.348 kasus *web defacement* di situs-situs Indonesia, dengan jumlah kasus terbanyak terjadi pada bulan Januari, yaitu sebanyak 416 kasus. Sektor Administrasi Pemerintahan menjadi yang paling banyak terkena serangan, dengan total 885 kasus [1]. Kebutuhan untuk mengimplementasikan langkah-langkah keamanan yang lebih efektif menjadi semakin mendesak. Khususnya di instansi pemerintahan, keamanan jaringan menjadi prioritas utama karena mereka mengelola data sensitif dan informasi penting yang mendukung fungsi-fungsi vital pemerintahan. Keamanan jaringan di instansi pemerintahan sering kali menghadapi tantangan yang kompleks, termasuk perlunya melindungi data pribadi warga, informasi keuangan, serta sistem administrasi internal dari ancaman siber yang terus berkembang. Kelemahan dalam sistem keamanan dapat mengakibatkan pencurian data, kerusakan reputasi, serta gangguan pada layanan publik. Oleh karena itu, instansi pemerintahan harus menerapkan solusi keamanan yang efektif untuk menjaga integritas dan kerahasiaan data mereka. Observasi dan wawancara penulis lakukan di tanggal 10 Juni 2024 hingga 14 Juni 2024 di kantor desa Jalatrang, kecamatan Cipaku, kabupaten Ciamis, ditemukan beberapa kelemahan dalam sistem keamanan dan *monitoring* jaringan di lokasi penelitian. Salah satu kelemahan pada sistem keamanannya

adalah tidak adanya keamanan *firewall* pada autentikasi *login router* MikroTik, yang memberikan peluang bagi peretas untuk mengakses jaringan secara tidak sah. Hal ini pada akhirnya dapat mengancam data, konfigurasi, dan keamanan infrastruktur jaringan secara keseluruhan. Selain itu, tidak adanya sistem *monitoring* jarak jauh membuat *administrator* tidak dapat memantau aktivitas jaringan atau merespon ancaman secara *real-time* yang dapat menyebabkan jaringan rentan terhadap serangan dan gangguan operasional. Penerapan *port knocking* diharapkan menjadi salah satu metode untuk meningkatkan keamanan autentikasi *login router* MikroTik. Integrasi dengan telegram memungkinkan pemantauan jarak jauh dengan notifikasi langsung mengenai aktivitas jaringan dan ancaman, sehingga administrator dapat merespons secara cepat. Kombinasi ini bertujuan memperkuat keamanan jaringan dan meningkatkan kemampuan pemantauan untuk mengurangi risiko serangan dan gangguan operasional. Berdasarkan latar belakang masalah yang telah dipaparkan pada paragraf sebelumnya, penulis tertarik untuk mengambil judul "Implementasi *Monitoring* Keamanan Jaringan Menggunakan *Port Knocking* Berbasis Telegram."

II. METODE PENELITIAN

Metode penelitian yang akan digunakan dalam Tugas Akhir ini adalah *Network Development Life Cycle (NDLC)*. Metode penelitian *NDLC* merupakan sebuah metode yang bergantung pada proses pembangunan sebelumnya seperti perencanaan strategi, daur hidup pemngembangan aplikasi, dan analisis pendistribusian data. Efektivitas dalam pengimplementasian teknologi jaringan akan menghasilkan sistem informasi yang memenuhi tujuan strategis, memungkinkan penerapan pendekatan *top-down*. Berikut ini adalah tahapan dari *NDLC*[2].



Gbr. 1 *NDLC Methodology*

Penelitian ini menggunakan pendekatan *NDLC* dengan lima tahapan: *Analysis, Design, Simulation Prototyping, Implementation, dan Monitoring*. Tahap *Management* tidak dilakukan karena kebijakan institusi membatasi pengujian keamanan jaringan ini. Penelitian ini difokuskan pada tahapan *Analysis, Design, Simulation Prototyping, Implementation, dan Monitoring*. Meskipun tahap *management* tidak dilakukan, hasil pengujian pada tahap kelima diharapkan sudah cukup untuk memberikan gambaran tentang efektivitas dan keandalan sistem yang dikembangkan.

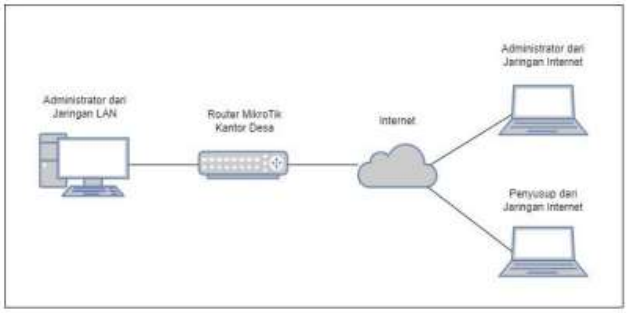
III. HASIL DAN PEMBAHASAN

A. Analisis Sistem yang Sedang Berjalan

Sistem Jaringan yang saat ini diterapkan di lokasi studi kasus menggunakan perangkat MikroTik sebagai *router* utamanya. Tetapi sistem ini belum memiliki konfigurasi *firewall* yang memadai untuk mengatur autentikasi *login user*, sehingga akses ke jaringan cenderung tidak terkontrol dan rentan terhadap ancaman keamanan jaringan. Sistem yang saat ini sedang berjalan tidak dilengkapi dengan *monitoring* dan kontrol *router* secara *real-time*, sehingga *administrator* jaringan tidak dapat memantau aktivitas jaringan secara efektif dan responsif. Kurangnya mekanisme pengawasan ini dapat menjadi penghambat dalam identifikasi dan penanganan masalah jaringan.

B. Topologi yang Sedang Berjalan

Hasil observasi dan wawancara mengenai kebijakan instansi, peraturan mengenai pengalamatan dan topologi jaringan komputer sebagai sumber koneksi internet yang berasal dari pusat merupakan mutlak kewenangan instansi, penulis tidak diperkenankan untuk menampilkan topologi jaringan tersebut dan penulis hanya menampilkan topologi jaringan yang terlibat langsung dengan penelitian ini. Sehingga untuk implementasi *monitoring* keamanan jaringan menggunakan *port knocking* berbasis telegram, diatur sebagaimana yang ditunjukkan pada gambar 2.



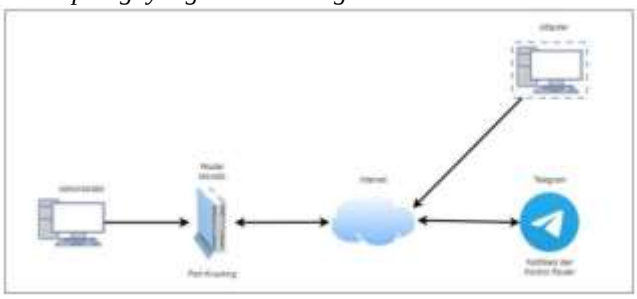
Gbr. 2 Topologi jaringan yang sedang berjalan

1. *Router* MikroTik yang terdapat di kantor desa Jalatrang dengan *IP* publik yang ditetapkan pada port ethernet1 dengan *IP* 202.138.225.xxx dan *IP LAN* pada *port ethernet2* dengan *IP* 192.168.10.1/24. *IP* publik yang ditetapkan pada *router* MikroTik membuat *router* dapat diakses melalui jaringan internet baik oleh *administrator* jaringan yang berwenang maupun penyusup.
2. *Administrator* dari jaringan Internet dapat mengakses *router* MikroTik untuk manajemen jaringan dengan autentikasi *login username* dan *password* tanpa melalui proses *port knocking*.
3. *Administrator* jaringan juga dapat mengakses ke MikroTik dari jaringan *LAN* tanpa harus melakukan *port knocking*.

C. Analisis Sistem yang Akan Dibangun

Sistem jaringan yang akan dibangun melibatkan konfigurasi *port knocking* yang diterapkan pada *firewall* untuk menyembunyikan *port* akses *router*, di mana akses hanya diberikan setelah serangkaian *port knocks* yang berurutan dilakukan. Perubahan *port* pada winbox akan dilakukan untuk menambah keamanan jaringan, *port default* winbox diubah dari 8289 menjadi 8280. Telegram digunakan untuk mengirimkan notifikasi terkait autentikasi *login router*, memberikan informasi mengenai *list user* yang sedang aktif. Sistem jaringan yang akan dibangun dapat memungkinkan *monitoring* dan kontrol *router* MikroTik melalui telegram dengan memanfaatkan *API bot* Telegram untuk mengirimkan laporan *real-time* tentang status jaringan dan menerima perintah dari jarak jauh untuk mengelola *router*. Melalui pendekatan ini, sistem tidak hanya memperkuat keamanan melalui *port knocking* dan notifikasi autentikasi *login router* dengan telegram, tetapi juga menyediakan pemantauan dan kontrol yang lebih efisien.

D. Topologi yang Akan Dibangun

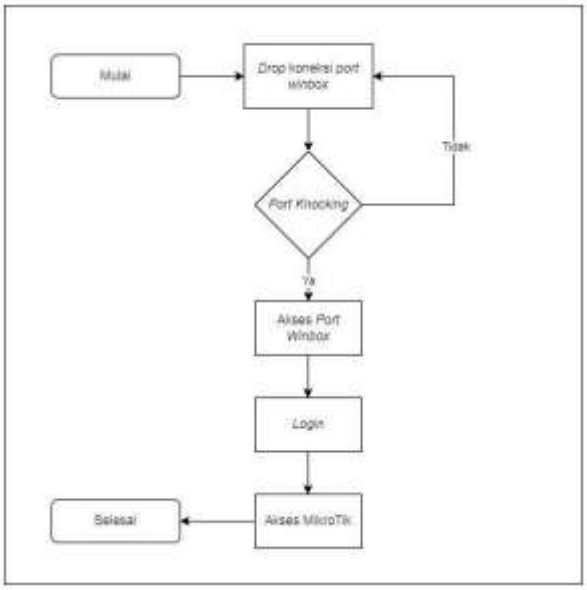


Gbr. 3 Topologi yang akan dibangun

Gambar 3 menjelaskan mengenai topologi yang akan dibangun. *Administrator* harus melakukan *port knocking* ketika akan mengakses *router* MikroTik dan selanjutnya notifikasi *login user* akan dikirimkan ke telegram. *Administrator* dapat melakukan perintah ke *router* untuk pengecekan CPU, ping koneksi dan *enable/disable port knocking* dengan menggunakan *API* telegram.

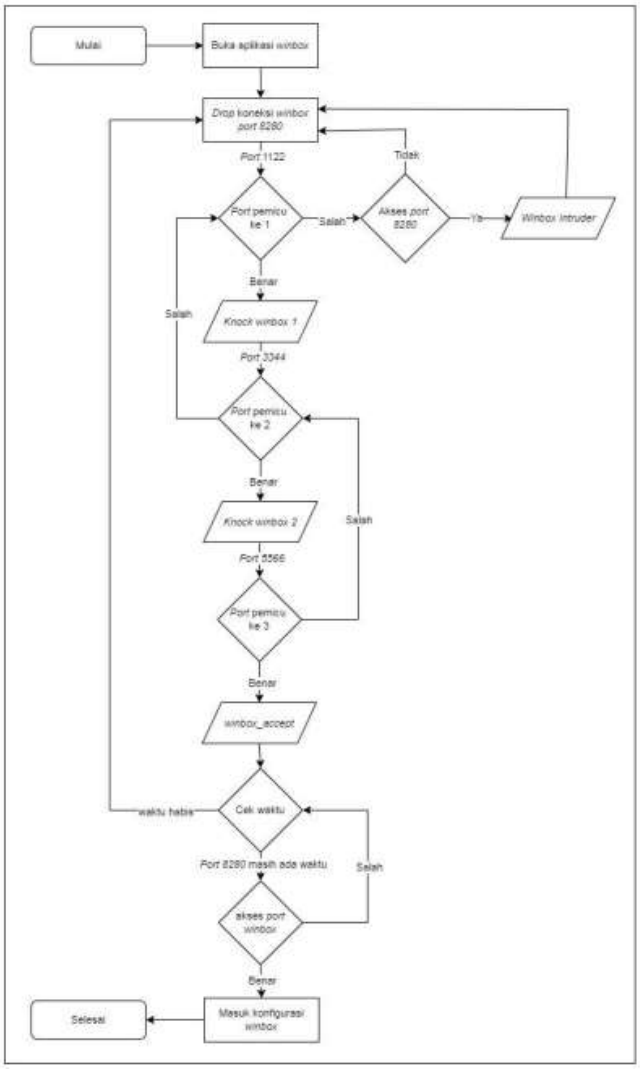
E. Alur akses *router* dengan *port knocking* dan *drop* koneksi

Gambar 4 menggambarkan proses *administrator* dapat mengakses dan *login* ke *router* MikroTik menggunakan *port knocking* melalui jaringan internet dan bagaimana *drop* koneksi dapat berkeja



Gbr. 4 Alur akses *router* dengan *port knocking* dan *drop* koneksi

F. Alur Autentikasi Login ke Port Winbox Dengan Port Knocking

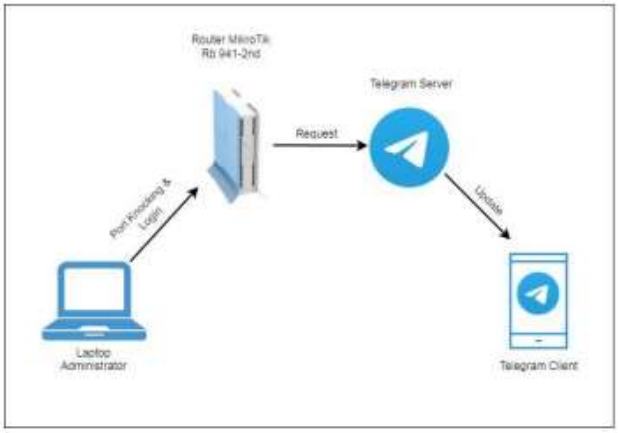


Gbr. 4 Alur autentikasi l*ogin port* winbox dengan p*ort knocking*

Gambar 4 menunjukan bahwa *administrator* jaringan dapat melakukan autentikasi *login* ke *port* winbox *router* MikroTik melalui beberapa tahapan yaitu:

1) *Administrator* jaringan memulai proses dengan membuka *software* winbox.
2) Pengamanan *router* MikroTik dari akses yang tidak sah dilakukan dengan mendrop semua koneksi yang masuk ke *port* Winbox (port 8280) setelah *IP* publik *router* MikroTik ditetapkan.
3) *Administrator* harus mengetuk *port* pemicu ke-1, yaitu port 1122. *IP* administrator akan terdaftar dalam *address list* KNOCK_WINBOX1 selama 10 detik, apabila ketukan *port* pemicu ke-1 berhasil dilakukan. Ketika *administrator* tidak mengetuk *port* pemicu ke-1, koneksi ke *port* winbox akan di-drop.
4) *IP* akan terdaftar dalam *address list* WINBOX_INTRUDER selama 10 detik dan menandakan bahwa *IP* tersebut merupakan penyusup, apabila ada koneksi yang memaksa mengakses *port* winbox yang baru saat koneksi di-drop.
5) Administrator dapat mengetuk *port* pemicu ke-2, yaitu port 3344, apabila administrator berhasil mengetuk *port* pemicu ke-1 dan masih terdaftar dalam *address list* KNOCK_WINBOX1. Ketika ketukan *port* pemicu ke-2 berhasil, *IP administrator* akan terdaftar dalam *address list* KNOCK_WINBOX2 selama 10 detik. Ketika *administrator* tidak mengetuk *port* pemicu ke-2, maka harus mengulang proses dari *port* pemicu ke-1.
6) *Administrator* dapat mengetuk *port* pemicu ke-3, yaitu *port* 5566, apabila *administrator* berhasil mengetuk *port* pemicu ke-2 dan masih terdaftar dalam *address list* KNOCK_WINBOX2. Ketika ketukan *port* pemicu ke-3 berhasil, *IP administrator* akan terdaftar dalam *address list* WINBOX_ACCEPT selama 1 jam, yang artinya permintaan koneksi *administrator* melalui *port* winbox diterima dalam batas waktu tersebut. Apabila *administrator* tidak mengetuk *port* pemicu ke-3, maka harus mengulang proses dari *port* pemicu ke-2.
7) Selama *IP administrator* terdaftar dalam *address list* WINBOX_ACCEPT, *administrator* dapat mengakses *port* winbox yang baru (port 8280) dan melanjutkan dengan proses autentikasi *login* ke *router* MikroTik.
8) Ketika didalam *address list* MikroTik masih tercatat *login user administrator* yang sebelumnya, maka *administrator* yang sudah *logout* dan ingin kembali *login*, tidak perlu melalui proses *port knocking*.

G. Integrasi ke Telegram



Gbr. 5 Integrasi ke telegram

Integrasi dari setiap komponen yang digunakan dalam sistem *port knocking* dan notifikasi *login user* ke telegram seperti yang ditunjukkan pada gambar 5 yaitu sebagai berikut :

1) *Administrator* dapat mengakses *router* MikroTik Rb 941-2nd melalui proses *port knocking* dengan masuk ke *port* pemicu winbox pada *router* MikroTik.
2) *Administrator* dapat mengakses *port* baru pada *router* MikroTik dan melanjutkan *login* dengan *IP address*, *username*, dan *password* yang benar.

3) *Router* MikroTik Rb 941-2nd akan mengirimkan permintaan *(request)* ke telegram *server* berupa informasi *user login*.
4) Permintaan dikirimkan menggunakan metode *send messages* yang diatur pada *script* dan *scheduler* agar *request* tersebut dapat dikirimkan secara terjadwal.
5) *Chat ID* pada telegram digunakan sebagai nomor identitas yang unik untuk mengirimkan pesan ke akun telegram tertentu.
6) Telegram *client*, yang terpasang pada *smartphone*, akan menerima *update* dari telegram *server* berupa pesan notifikasi tentang *login user* MikroTik

Pengujian

A. *Pengujian Port Knocking Winbox Dengan Notifikasi Telegram*

Pengujian *port knocking* winbox dengan notifikasi telegram dimulai dari mengakses ke serangkaian *port* pemicu sampai akses ke *port* yang baru pada winbox yang dilanjutkan dengan proses *login user* ke *router* MikroTik sampai dikirimkannya notifikasi *login user* MikroTik ke telegram. Pengujian ini dilakukan dengan mengakses *router* MikroTik menggunakan winbox dan pengecekan *log* dilakukan pada *webfig*.

B. *Akses Port Winbox Setelah Knocking*

Setelah melalui tahapan ketukan akses port pemicu ke-1 sampai ke-3 winbox hingga pada *IP user* koneksinya diterima, maka *user* dapat mengakses dan *login* ke *port* winbox menggunakan *IP* publik *router* yaitu 10.10.10.1 dengan *port* 8280 serta *login* menggunakan *username* dan *password* yang ditunjukkan pada gambar 6.

Gbr. 6 Akses *port w*inbox setelah *knocking*

C. *Notifikasi Login User MikroTik ke Telegram Port Winbox*

Setelah *user* melalui *port knocking* dan akses serta *login* ke winbox maka pada telegram akan menampilkan peringatan informasi *login user* melalui winbox yang ditunjukkan pada gambar 7.

Gbr. 8 Notifikasi *login user* ke telegram

Tabel hasil pengujian akses *port* winbox dengan menggunakan *port knocking* dapat dilihat pada tabel 1.

Tabel 1 Hasil pengujian akses *port* winbox

Uji Ke	*Port* 1122 (10 s)	*Port* 3344 (10 s)	*Port* 5566 (10 s)	*Allowed AddressList* (1 h)	*Port* 8280	*Intruder*	*Login*	Notif
1	√	x	x	x	x	x	x	x
2	√	√	x	x	x	x	x	x
3	√	√	√	√	x	x	x	x
4	√	√	√	√	√	x	x	x
5	√	√	√	√	√	x	√	√
6	x	x	x	x	√	√	x	x

Keterangan :
√ : dilakukan ketukan *port* atau kondisi yang terjadi.
x : tidak dilakukan ketukan *port* atau kondisi yang tidak terjadi.

D. *Pengujian Port Scanning Sebelum Port Knocking*

Pengujian *port scanning* sebelum konfigurasi *port knocking* adalah pengujian untuk mengetahui *port* yang terbuka pada MikroTik dengan nomor *port* winbox yang sudah diganti (8280). *NMAP/Zenmap* digunakan dalam pengujian *scanning* ini.

Gbr. 8 Pengujian *nmap* sebelum *port knocking*

Pengujian *port scanning* sebelum melakukan *port knocking* ke *port* winbox *router* MikroTik ditunjukkan pada gambar 8. Sebelum melakukan *port knocking* ke *router* MikroTik maka pada *port scanning* menampilkan *port* layanan winbox (*port* 8280) dengan status *open*. Status *open* menunjukan bahwa *port* winbox yang terbuka dapat menjadi potensi risiko serangan jaringan, terutama jika *router* terhubung ke internet atau jaringan publik.

E. Pengujian Port Scanning Setelah Port Knocking

Pengujian *port scanning* setelah konfigurasi *port knocking* ke *port* winbox, *router* MikroTik ditunjukkan pada gambar 9.

Gbr. 9 Pengujian *nmap* setelah *port knocking*

Pengujian *port scanning* setelah melakukan *port knocking* ke *port* winbox *router* MikroTik ditunjukkan pada gambar 9. Setelah melakukan *port knocking* ke *router* MikroTik pada layanan winbox maka *port scanning* akan menampilkan *port* layanan winbox (*port* 8280) dengan status *filtered* atau tertutup. *Port* layanan tersebut dapat memiliki status *filtered* jika sudah melakukan *port knocking* ke *port* winbox

F. Hasil Pengujian Port Scanning

Berikut tabel pengujian hasil *port scanning* sebelum dan setelah dilakukan *port knocking* yang ditunjukkan pada tabel 2.

Tabel 2 Hasil pengujian *port scanning*

Pengujian	Model Pengujian	*Port Winbox*
1	Sebelum konfigurasi *port knocking*	*Open*
2	Setelah konfigurasi *port knocking*	*Filtered*

G. Pengujian Kontrol Router Mikrotik Dengan Integrasi Telegram

Setelah memastikan *script* dan *schedule* pada MikroTik berfungsi sesuai dengan kebutuhan, langkah selanjutnya adalah melakukan pengujian terhadap kontrol *router* MikroTik menggunakan telegram. Pengujian ini bertujuan untuk menilai efektivitas dan keandalan integrasi antara MikroTik dan telegram dalam mengelola dan memantau keamanan jaringan. Pengujian ini akan memungkinkan evaluasi sejauh mana telegram dapat berfungsi sebagai alat yang efisien dan aman untuk mengendalikan fungsi-fungsi penting pada *router* MikroTik.

1) Pengujian perintah "/menu"

Gambar 10 merupakan hasil pengujian perintah /menu pada telegram yang kemudian direspon oleh *router* MikroTik. Perintah diolah di *router* kemudian ditampilkan kembali pada telegram pilihan menu yang tersedia.

Gbr. 10 Pengujian perintah /Menu

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan keseluruhan tahapan perancangan, implementasi dan pengujian dari implementasi *monitoring* keamanan jaringan menggunakan *port knocking* dapat diambil kesimpulan sebagai berikut:

1) Analisis sistem keamanan jaringan dengan metode *port knocking* menunjukkan bahwa metode ini menambah perlindungan dengan menyembunyikan *port* yang tidak aktif dan hanya membukanya saat menerima "ketukan" yang benar. Kelebihan metode ini termasuk peningkatan keamanan terhadap pemindaian *port* dan akses tidak sah. Namun, *port knocking* juga memiliki kekurangan, seperti risiko jika urutan paket mudah ditebak. Selain itu, metode ini memerlukan konfigurasi yang tepat dan pemantauan rutin. Walaupun *port knocking* membantu mengurangi risiko, menggabungkannya dengan metode keamanan lain akan menciptakan sistem yang lebih kuat dan efektif.

2) Implementasi *port knocking* yang terintegrasi dengan notifikasi telegram dan kontrol keamanan *router* MikroTik berhasil meningkatkan keamanan jaringan. *Port knocking* menyembunyikan *port* dari akses yang tidak sah, sementara notifikasi telegram memberikan informasi secara *real* tentang aktivitas jaringan. Kontrol MikroTik yang terhubung dengan telegram memudahkan manajemen keamanan dari jarak jauh. Kombinasi ini efektif dalam melindungi jaringan dan memungkinkan respons cepat terhadap potensi ancaman.

3) *Port knocking* pada *router* MikroTik meningkatkan aspek keamanan jaringan dengan menyembunyikan *port* dari pemindai yang tidak sah. Aspek ini menambah lapisan perlindungan terhadap akses tidak sah. *Port knocking* akan lebih bagus lagi apabila digunakan bersama dengan metode keamanan lain untuk perlindungan data yang lebih optimal.

B. Saran

Setelah melakukan keseluruhan tahapan perancangan, implementasi, pengujian dan penulisan laporan ini maka penulis memiliki beberapa saran bagi pembaca yang ingin mengimplementasikan *port knocking* dengan integrasi telegram pada perangkat jaringan seperti router seperti :

1) Menentukan *port* pemicu dari *port knocking* harus ditentukan nomor *port* yang unik namun mudah diingat agar tidak menyulitkan *administrator* jaringan ketika mengakses *router* MikroTik dari jaringan internet. Selain itu penentuan jumlah *port* pemicu pada *port knocking* juga harus diperhitungkan sesuai kebutuhan dengan memperhatikan kondisi keamanan jaringan *administrator*.

2) *Port knocking* juga dapat mencegah serangan *brute force* jika dilakukan tambahan penyesuaian konfigurasi pada *firewall* MikroTik seperti *block IP* dalam waktu tertentu pada *IP* yang terdeteksi melakukan serangan *brute force*. Namun hal ini perlu dianalisis lebih lanjut kebutuhan dan kondisi jaringan, karena dengan melakukan *block IP* dikhawatirkan akan ada dampak negatif jika dilakukan tanpa analisis.

3) Mengontrol dan memantau *router* MikroTik dengan integrasi telegram dapat dilakukan dengan menambahkan atau membuat perintah baru sesuai kebutuhan.

REFERENSI

[1] csirt (2024). Lanskap Keamanan Siber Indonesia Tahun 2022. https://csirt.perhutani.co.id Retrieved 09 September, 2024, from https://csirt.perhutani.co.id/?p=3183

[2] Iqromullah, R., Khairil, K., & Suryana, E. (2023). Security System Implementation And Monitoring Networks At Sma N 10 City Of Bengkulu. Jurnal Media Computer Science, 2(2), 153–168.

[3] Ariska, D. (2021). Konfigurasi Pemblokiran Situs Menggunakan Static Dns Mikrotik. In *Jurnal Algoritma* (Vol. 14, Issue 11). Politeknik Negeri Sriwijaya.

[4] Asyikin, A. N., Saputera, N., & Yohanes, E. (2013). Sistem Manajemen Hotspot Di Politeknik Negeri Banjarmasin Menggusnakan Mikrotik Router Os. *Poros Teknik*, *5*(1), 31–35.

[5] Christian, Y. (2019). Analisis Sistem Pengamanan Akses Autentikasi Jaringan dengan Metode Port Knocking dan Action Tarpit pada Router Mikrotik. *Telcomatics*, *4*(1), 1–6.

[6] Dwiyatno, S. (2020). Analisis Monitoring Sistem Jaringan Komputer Menggunakan Software Nmap. *Prosisko: Jurnal Pengembangan Riset Dan Observasi Sistem Komputer*, *7*(2), 108–115.

[7] Ernawati, T., Idham Kholid, Dahlan, & Rohmayani, D. (2024). Case Study in Network Security System Using Random Port Knocking Method on The Principles of Availability, Confidentiality and Integrity. *Jurnal Online Informatika*, *9*(1), 41–51.

[8] Fathurrozi, A., & Karimah, F. (2021). Pelayanan Dan Informasi Customer Service Berbasis Bot Telegram Dengan Algoritma Forward Chaining Pada CV. Primguard Indonesia. *Journal of Informatic and Information Security*, *2*(2).