PENGUJIAN CELAH KEAMANAN JARINGAN KOMPUTER PT. JIONA SEJATI DENGAN NETWORK PENETRATION TESTING

Sony Firsky Maulana[1], Hendi Suhendi[2]

[1]Universitas Adhirajasa Reswara Sanjaya
Jl. Terusan Sekolah No. 1-2 Bandung, (022) 7100124
e-mail: vikingmahameru@gmail.com

[2]Universitas Adhirajasa Reswara Sanjaya
Jl. Terusan Sekolah No. 1-2 Bandung, (022) 7100124
e-mail: hendi2708@ars.ac.id

Abstrak

Perkembangan teknologi di era saat ini semakin berkembang pesat, sama halnya dengan perkembangan jaringan komputer. Dengan peran teknologi, penyampaian informasi menjadi semakin cepat, berkomunikasi tanpa dibatasi oleh jarak, ruang dan waktu. Adanya perkembangan teknologi tersebut, keamanan merupakan aspek yang perlu diwaspadai oleh setiap pihak yang memiliki skema terpusat, karena pembobolan, manipulasi, maupun kehilangan data dapat terjadi jika dilakukan oleh para hacker yang memang berniat mengambil data sensitif dari sebuah perusahaan. Perusahaan PT. JIONA SEJATI merupakan perusahaan yang bergerak dibidang kontruksi mekanikal dan elektrikal yang mempunyai data legalitas disimpan didalam komputer. Dengan adanya ketersediaan jaringan, baik melalui jaringan WLAN maupun LAN, maka perlu diperhatikan keamanannya dari para hacker. Dengan hanya menggunakan keamanan standar serta tidak adanya keamanan jaringan internet pada router maka pengguna umum dapat dengan mudah terhubung kedalam jaringan PT. JIONA SEJATI. Setelah dilakukan Analisa terhadap jaringan, arsitekrut jaringan, keamanan jaringan serta spesifikasi hardware dan software. Maka penambahan Mikrotik Routerboard untuk menunjang keamanan jaringan pada jaringan yang ada sangatlah berguna. Disamping mempunyai berbagai fitur keamanan, Mikrotik Routerboard juga digunakan untuk memanajemen jaringan agar tidak terjadi monopoli bandwidth antara divisi administrasi dengan divisi operasional. Sehingga penggunaan jaringan internet menjadi lebih aman dan juga lebih stabil.

Kata Kunci: Keamanan Jaringan, *Mikrotik Routerboard*, *Hacker*

Abstrack

The development of technology in the current era is growing rapidly, as is the development of computer networks. With the role of technology, information delivery becomes faster, communicating without being limited by distance, space and time. With these technological developments, security is an aspect that every party with a centralized scheme needs to watch out for, because breaches, manipulations or data loss can occur if hackers intend to take sensitive data from a company. The company PT. JIONA SEJATI is a company engaged in mechanical and electrical construction that has legality data stored on a computer. With the availability of networks, either through WLAN or LAN networks, it is necessary to pay attention to security from hackers. By only using standard security and the absence of internet network security on the router, general users can easily connect to the PT. TRUE JIONA. After analyzing the network, network architecture, network security and hardware and software specifications. So the addition of a Mikrotik Routerboard to support network security on an existing network is very useful. Besides having various security features, Mikrotik Routerboard is also used for network management so there is no monopoly on bandwidth between the administrative and operational divisions. So that the use of the internet network becomes safer and more stable.

Keyword: *Network Security*, *Mikrotik Routerboard*, *Hacker*

1. Pendahuluan

Perkembangan teknologi di era saat ini semakin berkembang pesat, sama halnya dengan perkembangan jaringan komputer. Dengan peran teknologi dapat menyampaikan informasi semakain cepat, berkomunikasi tanpa dibatasi oleh jarak, ruang dan waktu. Secara umum jaringan komputer adalah komputer yang saling terhubung satu sama lain secara global, dengan jaringan komputer kita dapat melakukan pertukaran data (Verawardina, 2018).

Adanya perkembangan teknologi tersebut, keamanan merupakan aspek yang perlu diwaspadai oleh setiap pihak yang memiliki skema sistem terpusat, karena pembobolan, manipulasi, maupun kehilangan data dapat terjadi jika dilakukan oleh para *hacker* yang memang berniat mengambil data sensitif dari sebuah perusahaan. Tidak adanya keamanan pada sistem menyebabkan banyak para hacker dengan mudah dapat mengambil alih sistem yang dibangun. Hal ini menimbulkan keterbukaan untuk mengakses data pribadi maupun data penting sebuah perusahaan atau lembaga yang seharusnya tidak diketahui oleh orang lain (W et al., 2016). Langkah awal yang harus dikembangkan untuk dapat mengurangi kerugian yang diakibatkan oleh para *hacker* adalah melakukan evaluasi terhadap keamanan jaringan yang ada. Hal ini bertujuan untuk mengurangi resiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada perusahaan.

Perusahaan PT. JIONA SEJATI merupakan perusahaan yang bergerak dibidang kontruksi mekanikal dan elektrikal dan mempunyai data legalitas yang banyak disimpan didalam komputer. Dengan adanya ketersediaan jaringan, baik melalui jaringan WLAN maupun LAN, maka perlu diperhatikan keterkaitannya dengan jaringan dari para *Hacker*. Masalah yang ditemukan pada PT.JIONA SEJATI diataranya yaitu mudahnya para pengguna umum terhubung dengan jaringan sehingga data yang disimpan dapat diambil dengan mudah. Permasalah lain yang ditemukan adalah sebagian besar karyawan.

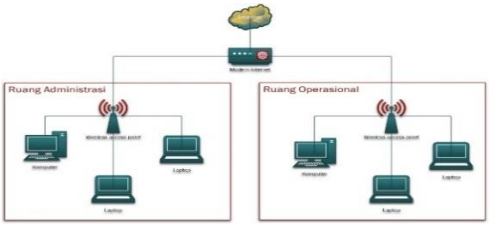
Sebagian besar orang di perusahaan PT. JIONA SEJATI akan merasa bingung saat diminta untuk melakukan evaluasi keamanan jaringan yang ada. Hal ini dikarenakan banyak orang awam untuk melakukan evaluasi jaringan. Solusi yang dapat diusulkan yaitu dengan melakukan pengujian terhadap jaringan yaitu melakukan simulasi bentuk-bentuk serangan terhadap jaringan atau biasa yang dikenal dengan Penetration Testing (Pujiarto et al., 2013).

Penelitian mengenai Penetration testing ini pernah dilakukan oleh (Bayu et al., 2017) dengan judul “Analisa keaman jaringan WLAN dengan metode *Penetration testing* (Studi kasus : Laboratorium sisten informasi dan programing teknik informatika UHO)“, selain itu pernah juga dilakukan oleh (Pujiarto et al., 2013) dengan judul “ Evaluasi keamanan *wireless local area network* menggunakan metode *penetration testing* (Kasus : Universitas Muhammadiyah Magelang) “, juga diteliti oleh (Hussain et al., 2017) dengan judul “*Penetration Testing In System Administration*“, berdasarkan penelitian sebelumnya belum pernah dilakukan di PT.JIONA SEJATI, sehingga penulis mengusulkan penelitian ini untuk diterapkan di PT.JIONA SEJATI.

2. Metode Penelitian

Penulis melakukan penelitian dengan menganalisa jaringan yang sudah berjalan. Sehingga penulis mendapatkan hasil Analisa berupa jenis jaringan yang digunakan, topologi jaringan yang diterapkan , penggunaan perangkat penunjang jaringan serta keamanan jaringan yang diterapkan.

Gambar 1. Jaringan komputer PT. JIONA SEJATI



Melihat gambar jaringan yang ada pada PT.JIONA SEJATI memang tergolong sangat mudah dan simple. Hanya terdapat perangkat modem internet dan 2 buah *wireless acces point*. Dikarenakan pada semua komputer menggunakan perangkat *Wi-fi Reciever*, maka semua akses jaringan yang disalurkan hanya menggunakan jaringan nirkabel. Agar mendapatkan koneksi yang maksimal maka jaringan internet disalurkan menggunakan 2 *Wireless acces point*, yang masing-masing disimpan pada ruang administrasi dan ruang operasional.

3. Hasil dan Pembahasan

Jaringan komputer merupakan salah satu hal terpenting untuk setiap perusahaan yang menerapkan teknologi komputer sebagai sarana kerja bagi setiap karyawan. Pengertian jaringan komputer menurut (Bayu et al., 2017) adalah suatu kumpulan atau beberapa komputer yang dihubungkan sehingga dapat berkomunikasi, termasuk juga printer dan peralatan lainnya yang saling terhubung. Data atau informasi ditransfer melalui kabel maupun *wireless* sehingga orang yang menggunakan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama dan bersama-sama menggunakan *hardware - hardware* yang terhubung dengan jaringan.

Jaringan komputer dapat melemah atau kurang optimal ketika jaringan komputer tersebut di serang oleh penyusup atau *hacker* dan *cracker* untuk kepentingan atau keuntungan pihak lain. Penyusup adalah hacker atau cracker yang selalu mencoba untuk mendapatkan akses dari sebuah sistem keamanan, instrusi sistem yang terjadi ketika orang yang tidak berhak mencoba untuk mendapatkan akses atau mengganggu operasi normal dari sistem informasi (Parningotan, 2018).

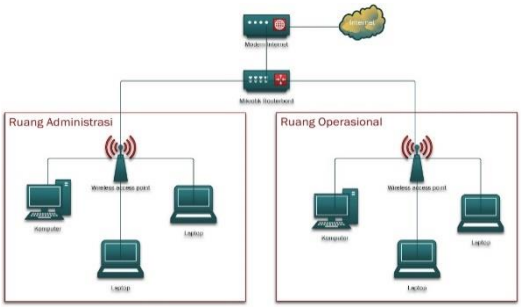
Penetration testing adalah metode evaluasi keamanan pada sistem komputer atau jaringan dengan mengidentifikasikan kelemahan, *vulnerabilities* dan *the absence of patches*. Identifikasi berupa celah keamanan, konfigurasi firewall dan wireless point. Simulasi dan identifikasi dilakukan dalam jaringan internal maupun jarak jauh. Tujuannya adalah menentukan dan mengetahui macam-macam serangan yang mungkin dilakukan pada sistem serta akibat yang bisa terjadi karena adanya kelemahan keamanan pada sistem komputer atau jaringan yang dimiliki (W et al., 2016). Uji penetrasi adalah serangkaian kegiatan yang dilakukan untuk mengidentifikasi dan mengeksploitasi kerentanan keamanan. Ini membantu mengkonfirmasi efektivitas atau ketidakefektifan langkah-langkah keamanan yang telah dilaksanakan (Tarigan et al., 2017). Uji penetrasi juga dapat membantu perusahaan untuk mengukur dampak dan kemungkinan kerentanan. Hal ini akan memungkinkan perusahaan untuk memprioritaskan dan menerapkan langkah-langkah korektif untuk kerentanan yang telah diketahui dan dilaporkan (Tarigan et al., 2017).

Mikrotik adalah perangkat jaringan komputer yang berupa *Hardware* dan *Software* yang dapat difungsikan sebagai *Router*, sebagai alat *Filtering*, *Switching* maupun lainnya. Adapun *hardware* Mikrotik bisa berupa Router PC (yang di install pada PC) maupun berupa Router Board (sudah dibangun langsung dari perusahaan Mikrotik). Sedangkan *software* Mikrotik atau dikenal dengan nama *Router* OS yang terkenal saat ini adalah RB1100 (Amarudin, 2018).

3.1. Manajemen Jaringan Usulan

Manajemen jaringan usulan merupakan gagasan yang dirancang penulis untuk mengatasi masalah yang terjadi pada jaringan komputer yang terpasang saat ini di PT.JIONA SEJATI, dalam hal ini pembuatan sistem manajemen *Bandhwidth* dan juga pemanfaatkan fitur yang ada pada Mikrotik *Routerboard* yang akan berpengaruh terhadap sistem keamanan jaringan. Pada tahap ini permasalahan yang terdapat pada point pertama yang terdapat di analisa permasalahan diatas akan teratasi, dengan mengatur penggunaan bandwitdth pada setiap divisi.

Gambar 2. Jaringan komputer usulan



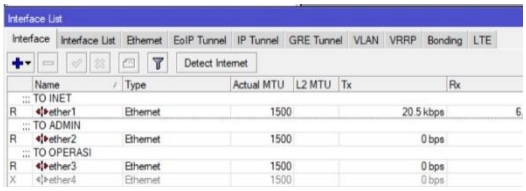
3.2. Implementasi Keamanan Jaringan

Rancang Aplikasi jaringan dibuat dengan menggunakan MikroTik *Routerboard* dengan RouterOS versi 6.45.8 sebagai *router* yang mengatur Mark Routing melalui satu buah ISP berkecepatan 100Mbps.

A. Konfigurasi *Router*

1. Konfigurasi *Interface*

Konfigurasi Interface dilakukan bertujuan agar interface dapat lebih mudah dikenali, konfigurasi interface dapat dilihat pada gambar dibawah ini:



Gambar 3. Tampilan *Interface Router* PT. JIONA SEJATI

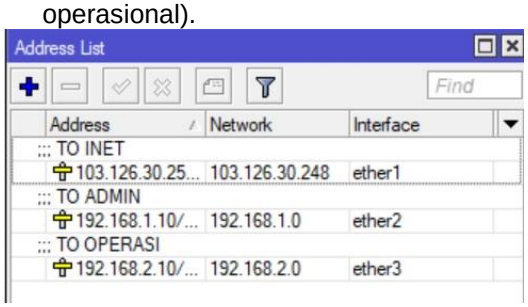
Berikut perintah yang dilakukan untuk konfugaris *interface*:

```
[admin@RO-JIONA] > interface ethernet comment ether1 comment="INET"
[admin@RO-JIONA] > interface ethernet comment ether2 comment="TO ADMIN"
[admin@RO-JIONA] > interface ethernet comment ether3 comment="TO OPERASI"
[admin@RO-JIONA] >
```

Gambar 4. Konfigurasi *Interface Router* PT. JIONA SEJATI

2. Konfigurasi *IP Address*

Konfigurasi *IP Address* pada *Router* PT. JIONA SEJATI adalah menambahkan IP 192.168.100.254/24 pada ether1 (sebagai penghubung antara Router dengan modem internet), IP 192.168.1.10/24 pada ether2 (sebagai penghubung antara *Router* dengan *Access Point* 1 pada ruangan administrasi), dan menambahkan IP 192.168.2.10/24 pada *ether3* (sebagai penghubung antara *Router* dengan *Access Point* 2 pada ruangan operasional).



Gambar 5. Tampilan *IP-Address* PT. JIONA SEJATI

```
[admin@RO-JIONA] > ip address add address=192.168.100.254/24 interface=ether1
[admin@RO-JIONA] > ip address add address=192.168.1.10/24 interface=ether2
[admin@RO-JIONA] > ip address add address=192.168.2.10/24 interface=ether3
[admin@RO-JIONA] >
```

Gambar 6. Tampilan *IP-Address* PT. JIONA SEJATI

3. Konfigurasi *DHCP-Server*

Konfigurasi *DHCP-Server* dilakukan untuk memberikan IP secara otomatis kepada setiap komputer yang ada pada jaringan PT. JIONA SEJATI, konfigurasi dilakukan melalui perintah script berikut:

```
[admin@RO-JIONA] > /ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether2
Select network for DHCP addresses

dhcp address space: 192.168.1.0/24
Select gateway for given network

gateway for dhcp network: 192.168.1.10
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.1.1-192.168.1.9,192.168.1.11-192.168.
.254
Select DNS servers

dns servers: 8.8.8.8,8.8.4.4
Select lease time

lease time: 10m
```

Gambar 7. Konfigurasi *DHCP-Server ether2* PT. JIONA SEJATI

```
[admin@RO-JIONA] > /ip dhcp-server setup
Select interface to run DHCP server on

dhcp server interface: ether3
Select network for DHCP addresses

dhcp address space: 192.168.2.0/24
Select gateway for given network

gateway for dhcp network: 192.168.2.10
Select pool of ip addresses given out by DHCP server

addresses to give out: 192.168.2.1-192.168.2.9,192.168.2.11-192.168.2.254
Select DNS servers

dns servers: 8.8.8.8,8.8.4.4
Select lease time

lease time: 10m
```

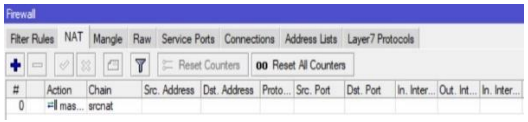
Gambar 8. Konfigurasi *DHCP-Server ether3* PT. JIONA SEJATI

4. Konfigurasi *Firewall* NAT

Konfigurasi Firewall NAT diperlukan agar komputer yang berada pada jaringan PT. JIONA SEJATI mendapatkan akses internet, konfigurasi Firewall NAT dilakukan melalui perintah script berikut:

```
[admin@RO-JIONA] >
[admin@RO-JIONA] > /ip firewall nat add action=masquerade chain=srcna
t
```

Gambar 9. Konfigurasi *Firewall* NAT PT. JIONA SEJATI

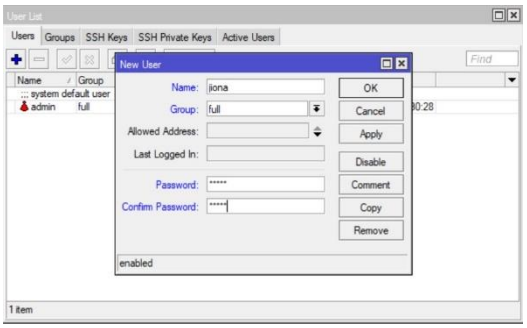


Gambar 10. Tampilan *Firewall* NAT PT. JIONA SEJATI

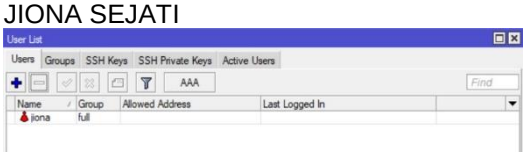
5. Konfigurasi Keamanan *Router*

Konfigurasi keamanan *Router* dilakukan untuk mengamankan *Router* dari pihak lain yang tidak diberikan akses untuk masuk kedalam jaringan yang ada. Konfigurasi ini meliputi beberapa pengamanan yang cukup baik, berikut beberapa konfigurasinya:

a) Merubah *User* Admin *Default*
Menonaktifkan *User* Admin *Default* yang ada dan menambahkan User baru, seperti yang terlihat pada gambar berikut:

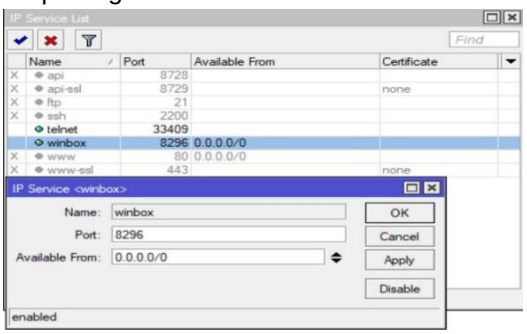


Gambar 11. Konfigurasi *User admin* PT. JIONA SEJATI



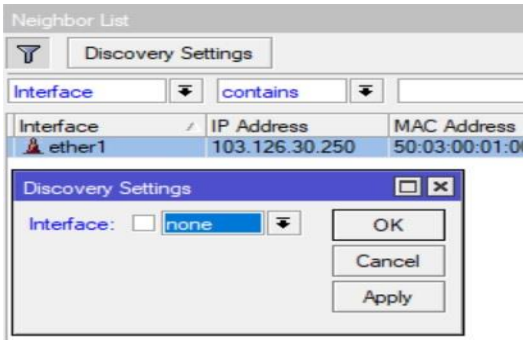
Gambar 12. Tampilan *User admin* PT. JIONA SEJATI

b) Menonaktifkan *Service*
Menu *service* terdapat pada IP > *Service*, setelah terbuka maka matikan *service* yang tidak diperlukan yang dimaksudkan untuk memperkecil akses masuk terhadap mikrotik dan rubah *Port* Winbox serta Web seperti yang terlihat pada gambar berikut:



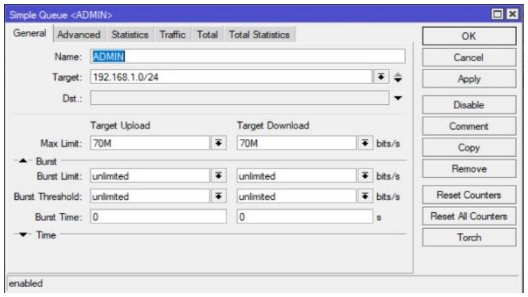
Gambar 13. Konfigurasi *Service* PT. JIONA SEJATI

c) Menonaktifkan *Neighbors Discovery*
Menu *Neighbors Discovery* terdapat pada IP > *Neighbors*, setelah terbuka matikan semua *Neighbors Discovery* dengan memilih *interface=none* seperti yang terlihat pada gambar berikut:

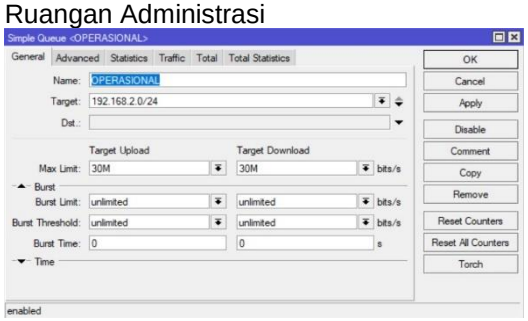


Gambar 14. Mematikan *Neighbor List Router* PT. JIONA SEJATI

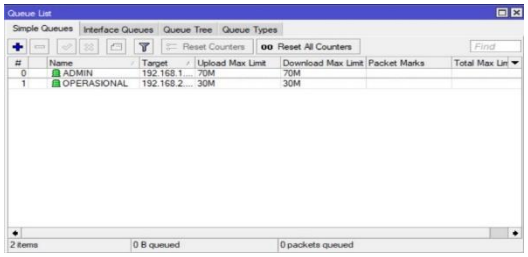
B. Manajemen jaringan
Dikarenakan kantor PT. JIONA SEJATI berlangganan pada salah satu *Internet Service Provider* dengan kecepatan yang besar yaitu 100Mbps, disini saya hanya membagi dua bagian yaitu 70Mbps untuk ruangan administrasi dan 30Mbps untuk ruangan operasional, dengan tujuan mencegah terjadinya monopoli penggunaan *bandwidth* antara ruangan administrasi dengan ruangan operasional, disini saya menggunakan *simple queue* untuk konfigurasi manajemen *bandwidth* tersebut. Untuk konfigurasi dapat dilihat pada gambar berikut:



Gambar 15. Konfigurasi *Simple Queue* Ruangan Administrasi



Gambar 16. Konfigurasi *Simple Queue* Ruangan Operasional

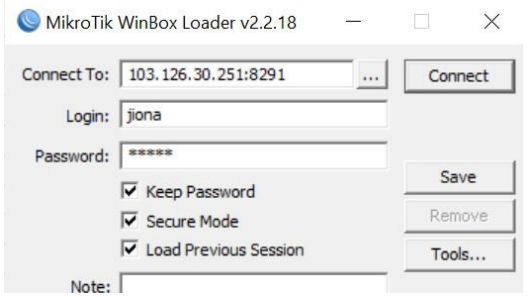


Gambar 17. Tampilan *Simple Queues* PT. JIONA SEJATI

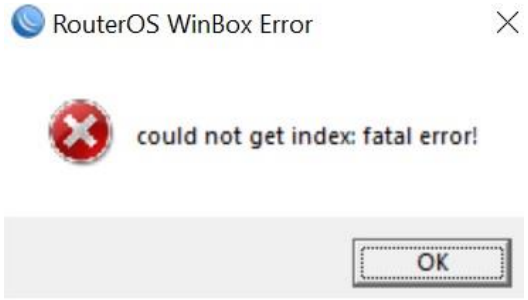
3.3. Pengujian Jaringan

Pengujian jaringan komputer dilakukan dengan mencoba akses masuk ke Mikrotik dengan menggunakan port default Winbox maupun port default Telnet dengan menggunakan aplikasi Putty.

1. *Login* menggunakan *port default* winbox



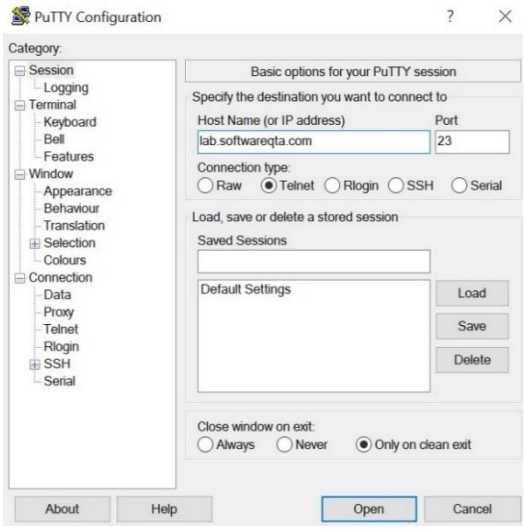
Gambar 18. Tampilan *Login* menggunakan *port default winbox*



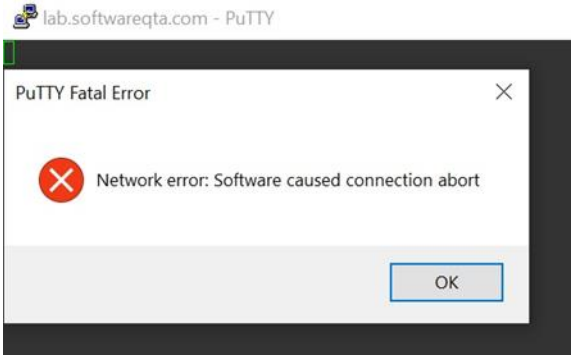
Gambar 19. Tampilan *Error Login* menggunakan *port default winbox*

Pada gambar diatas terlihat bahwa setelah *port default winbox* dirubah maka pengguna lain yang akan mengakses dengan menggunakan p*ort default winbox*, tidak akan bisa masuk meskipun *user* dan *password* login sudah benar.

2. *Login* menggunakan *port default* Telnet



Gambar 20. Tampilan *Login* menggunakan *port default* telnet



Gambar 21. Tampilan *Error Login* menggunakan *port default* telnet

Pada gambar diatas terlihat bahwa setelah port default telnet dirubah maka pengguna lain yang akan mengakses dengan menggunakan port default telnet, tidak akan bisa masuk meskipun user dan password login sudah benar.

4. Kesimpulan

Setelah penulis melakukan analisa jaringan yang ada serta mengimplementasikan solusi yang diberikan, maka kesimpulan yang dapat diambil sebagai berikut:

1. Penambahan Mikrotik Routerboard pada jaringan internet memudahkan dalam pengontrolan jaringan yang ada.
2. Penggunaan fitur security jaringan yang ada pada Mikrotik Routerboard dengan merubah user admin default, menonaktifkan service yang tidak diperlukan, merubah port winbox serta port web dan menonaktifkan neighbor's

discovery sudah cukup aman bagi jaringan internet PT. JIONA SEJATI.

3. Penggunaan management bandwidth dengan memanfaatkan fitur simple queue yang ada pada Mikrotik Routerboard membuat pembagian jaringan antara divisi administrasi dan divisi operasional membuat penerimaan jaringan internet antara masing-masing divisi tidak saling mengganggu.

Referensi

Amarudin, U. F. (2018). *Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking _ Amarudin _ Jurnal Teknoinfo.pdf*.

Bayu, I. K., Yamin, M., & Aksara, L. F. (2017). Analisa Keamanan Jaringan Wlan Dengan Metode Penetration Testing (Studi Kasus: Laboratorium Sistem Informasi dan Programming Teknik Informatika UHO. *SemanTIK*, *3*(2), 69–78.

Hussain, M. Z., Hasan, M. Z., Taimoor, M., Chughtai, A., Taimoor, M., & Chughtai, A. (2017). Penetration Testing In System Administration. *International Journal of Scientific & Technology Research*, *6*(6), 275–278. http://www.ijstr.org/final-print/june2017/Penetration-Testing-In-System-Administration.pdf

Parningotan, P. (2018). Analisis Network Security Snort Menggunakan Metode Intrusion Detection System (Ids) Untuk Optimasi Keamanan Jaringan Komputer. *JURSIMA Jurnal*, *6*(1).

Pujiarto, B., Utami, E., & Sudarmawan, S. (2013). Evaluasi Keamanan Wireless Local Area Network Menggunakan Metode Penetration Testing (Kasus : Universitas Muhammadiyah Magelang). *Data Manajemen Dan Teknologi Informasi (DASI)*, *14*(2), 16.

Tarigan, B. V., Kusyanti, A., & Yahya, W. (2017). Analisis Perbandingan Penetration Testing Tool Untuk Aplikasi Web. *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *1*(3), 206–214.

Verawardina, U. (2018). *Analisis Perbedaan Peformance dan Quality Of Service (Qos) Antara Eigrp dengan Ospf (Studi Kasus Menggunakan 6 Router Melalui GNS 3 dan Wireshark)*. *2*(1), 10–19.

W, Y., Riadi, I., & Yudhana, A. (2016). Analisis Keamanan Webserver Menggunakan Metode Penetrasi Testing. *Annual Research Seminar*, *2*(1), 300–304.