Terbit online pada laman web jurnal: **https://ejurnalunsam.id/index.php/jicom/**

JICOM
Jurnal Informatika dan Teknologi Komputer
Vol. 04 No. 01 (2023) 40 - 45 E-ISSN :2774-7115 P-ISSN: 2775-2089

# Implementasi Keamanan Jaringan Metode Port Knocking dan Port Blocking Berbasis Mikrotik PT Securindo Packatama Indonesia

Ade Eksan Nuryakin Habillah[1], Sidik[2]
[1]Program Studi Informatika, Fakultas Teknologi Informasi, Universitas Nusa Mandiri
[1]adeeksannh007@gmail.com*, [2]sdk.sidik1207@gmail.com

***Abstract***

*Network security is important for a company or institution in maintaining data and information security. Often the computer network has problems caused by the negligence of the network manager in building a computer network. Problems that arise can open up opportunities for irresponsible people to hack and damage the running network. For this reason, in order to avoid misuse of computer networks by irresponsible people, it is necessary to increase network security that is more secure and stronger. And in this research, research has been carried out to develop more secure network security by using port knocking and port blocking methods on Mikrotik. In this study, the author will explain the implementation of the port knocking method to provide filter access to the firewall, aiming to provide security for computer access users so that there will be no data or information theft so that data is kept safe. The final result of the study shows that authentication for ports makes the server safe as well as other ports, because port closures are to prevent access attacks from attackers who are not authorized to enter. By using port knocking and port blocking methods, the attacker will try harder to penetrate the system wall on the firewall.*

*Keywords: Port Knocking, Port Blocking, Firewall, Mikrotik Router.*

**Abstrak**

Keamanan jaringan hal penting bagi sebuah perusahaan maupun institusi dalam menjaga keamanan data dan informasi. Sering kali jaringan komputer mengalami masalah yang disebabkan oleh kelalaian pengelola jaringan dalam membangun jaringan komputer. Masalah yang muncul dapat membuka peluang bagi para orang yang tidak bertanggung jawab untuk meretas dan merusak jaringan yang berjalan. Untuk itu supaya tidak terjadi penyalahgunaan jaringan komputer oleh orang yang tidak bertanggung jawab tersebut, maka perlu adanya peningkatan keamanan jaringan yang lebih aman dan kuat. Dan dalam penelitian ini telah dilakukan penelitian untuk mengembangkan keamanan jaringan lebih aman dengan cara menggunakan metode *port knocking dan port blocking* pada mikrotik. Pada penelitian ini, penulis akan menjelaskan implementasi metode *port knocking* untuk memberikan akses *filter* pada *firewall*, bertujuan memberikan keamanan untuk pengguna akses komputer sehingga tidak akan ada pencurian data maupun informasi sehingga data tetap terjaga aman. Hasil akhir penelitian menunjukkan bahwa autentifikasi untuk *port* sehingga membuat server aman dan juga *port* yang lain, karena penutupan *port* untuk mencegah adanya serangan akses dari *attacker* yang tidak berhak untuk mengakses masuk. Dengan menggunakan metode *port knocking* dan *port blocking* akan membuat *attacker* akan berusaha lebih keras untuk menembus dinding sistem pada *firewall*.

Kata kunci: Port Knocking, Port Blocking, Firewall, Mikrotik Router.

## 1. Pendahuluan

Pesatnya perkembangan teknologi modern, penyediaan dalam perolehan informasi memberikan dampak positif, namun tentunya berdampak pada semua bidang, namun juga memiliki sisi negatif, sehingga perlu dilakukan tindakan preventif. Ada faktor yang tidak menyadari menjalankan ancaman jaringan, pencurian data, dan korupsi data. Berbagai metode telah diterapkan dengan menggunakan *firewall* sebagai hambatan kontrol akses [1]. *Firewall* masih tidak efektif karena menutup

Diterima Redaksi : 19-01-2023 | Selesai Revisi : 27-01-2023 | Diterbitkan Online : 01-04-2023

semua akses terlepas dari siapa yang terhubung ke jaringan. Seperti yang anda lihat, ancaman serangan yang sangat mengganggu pengguna semakin meningkat. Keamanan jaringan dan sistem informasi menimbulkan opini apakah menyimpan data, akses informasi dapat aman di masa depan.

PT. Securindo Packatama Indonesia didirikan pada tahun 1979 di Sydney, Australia. Saat ini berkembang menjadi jasa penyedia pengelolaan perparkiran terbesar di Australia dan di Indonesia. Salah satu kunci keberhasilan PT.Securindo Packatama Indonesia selama ini merupakan mengintegrasikan teknologi terkini ke dalam semua aspek pengelolaan parkir, mengintegrasikan seluruh pemilik *real estate* dan pengguna jasa parkir ke dalam satu program dan fasilitas layanan tanpa batasan. Bagitu juga jaringan yang sudah memadai membuat proses pekerjaan lebih cepat dan efektif. Akan tetapi keamanan jaringan di PT Securindo Packatama Indonesia sangat lemah dikarenakan keamanan akses jaringan ke mikrotik masih *firewall* normal dan *port-port* terbuka, ini memudahkan pengguna lain untuk mendapatkan akses yang tidak sah. Dengan demikian, akses dan keamanan *port* sangat penting dalam layanan jaringan dan merupakan bagian integral dari layanan. Masalah keamanan jaringan sering kali disebabkan oleh *port* terbuka yang dapat diakses orang lain dengan bebas.

Dari permasalahan diatas untuk mengamankan sistem jaringan, dengan ditemukannya metode yang mampu untuk menghindari dan menutup kekurangan dari sistem keamanan jaringan yaitu metode *Port Knock* dan *Port Block*. *Port knock* adalah cara konseptual untuk sembunyikan layanan jarak jauh di *firewall*, mengizinkan akses di *port* tersebut dan menemukan layanan hanya setelah klien berhasil mengautentikasi ke *firewall*. Ini membantu pemindai untuk menyembunyikan layanan yang saat ini tersedia di *host* dan bertindak sebagai pertahanan terhadap serangan *zero-day* [2]. Tujuan utamanya adalah untuk melindungi dari serangan yang dapat dieksploitasi melalui pemindaian *port*, membatasi akses pengguna, dan hanya mengizinkan pengguna yang telah menjalankan *Open Port Kncoking* yang memiliki akses penuh untuk membuka dan menutup akses *port* yang dikonfigurasi.

## 2. Metode Penelitian

Metode penelitian yang digunakan untuk menulis skripsi terdiri dari pengumpulan data dan analisa penelitian.

### 2.1. Metode Pengumpulan Data

Adapun tiga metode dalam pengumpulan data yang dapat dilakukan pengumpulan data yaitu:

a. Pengamatan Langsung
   Metode ini dilakukan untuk mendapatkan data atau informasi dengan cara mengamati secara langsung sistem jaringan berjalan yang ada pada PT Securindo Packatama Indonesia.
b. Wawancara
   Untuk mendapatkan informasi yang dibutuhkan maka penulis melakukan wawancara kepada Bapak Fathulloh, S.Kom selaku Staff IT di PT Securindo Packatama Inonesia untuk memperoleh informasi secara langsung mengenai keamanan jaringan yang berjalan dan permasalah yang ditemukan.
c. Studi Pustaka

Penulis memperoleh informasi dan data dari membaca dan mempelajari karya ilmiah, jurnal ilmiah, buku-buku di perpustakaan dan artikel-artikel di internet yang berhubungan dengan judul penyusunan skripsi ini.

### 2.2. Analisa Penelitian

Analisa penelitian yang diperlukan dalam penyusunan skripsi ini adalah sebagai berikut:

a. Analisa Kebutuhan
   Dalam memaksimalkan hasil penelitian untuk penyusunan skripsi ini, dibutuhkan beberapa hardware dan software yang dibutuhkan adalah Winbox, Putty, Vmware.
b. Desain
   Desain jaringan yang digunakan pada skripsi ini menggunakan software GNS3, desain jaringan yang menghubungkan jaringan komputer pada PT Securindo Packatama Indonesia dengan jaringan komputer yang berada pada jaringan di kantor cabang. Akan tetapi menjadi fokus pada pembahasan skripsi ini adalah keamanan jaringan pada PT Securindo Packatama Indonesia.
c. Testing
   Pengujian keamanan jaringan pada PT Securindo Packatama Indonesia meningkatkan keamanan jaringan menggunakan metode *port knocking dan port blocking* yang dikonfigurasi dalam mikrotik. Jika *user* ingin meremote mikrotik maka harus terlebih dahulu *open port knocking* barulah *user* dapat mengakses mikrotik, bila *user* tidak melakukan *open port knocking* maka *user* tersebut akan ditolak dan di *address list* pada *firewall* dianggap sebagai penyusup.
d. Implementasi
   Sistem keamanan jaringan menggunakan *port knocking* dan *port blocking* sudah di implementasikan di PT Securindo Packatama Indonesia, dan akan disimulasikan lagi menggunakan winbox.

### 2.3. Konsep Penunjang Usulan

a. Winbox
   Winbox merupakan aplikasi mode GUI untuk meremote dan mengkonfigurasi Mikrotik RouterOS [3]. Aplikasi *default* dari Mikrotik

untuk melakukan administrasi *routerboard*, semua fungsi dari router bisa diatur dengan aplikasi winbox, aplikasi ini cukup mudah dipahami dan ringan dengan ukuran 522kb dapat di download langsung dihalaman website Mikrotik.com.

b. Port Knocking dan Port Blocking
*Port knocking* merupakan bentuk komunikasi *host-to-host* dimana informasi tersalur melalui *port* yang tertutup. *Port knocking* dapat didefinisikan sebagai metode komunikasi antara dua komputer dimana informasi dikirim ke *port* dalam urutan tertentu. Dalam konstruksi konfigurasi ini bisa disebut pukulan ketukan (*knock*). Dengan kata lain, komputer tidak memiliki *port* komunikasi yang terbuka dan dapat diakses secara bebas, tetapi perangkat tetap dapat diakses dari luar dengan metode *port knocking* [4]. *Port blocking* merupakan metode tambahan untuk memperkuat keamanan pada port winbox dan www.

c. Vmware Workstation
Vmware Workstation adalah aplikasi *desktop virtualization*, tata cara penggunaannya seperti VirtualBox, dapat digunakan baik di windows maupun linux [5]. Untuk pengguna Mac, nama aplikasinya adalah Vmware Fusion, Vmware Workstation ataupun Vmware Fusion menggunakan mekanisme *hosted virtualization*, jadi harus ada sistem operasi windows atau linux yang menjadi *base* OS.

d. Topologi Jaringan
Topologi jaringan menggambarkan koneksi antar tiap titik (perangkat) dalam jaringan internet baik secara fisik atau logis [6]. Topologi paling sederhana dari jaringan internet adalah koneksi *peer-to-peer* yang hanya menghubungkan dua buah perangkat dengan koneksi secara langsung baik menggunakan kabel UTP atau secara nirkabel. Topologi star menghubungkan setiap komputer dengan sebuah hub atau hub, biasanya hub atau hub berupa hub atau switch, dan kabel UTP versi 5 biasa digunakan pada topologi star.

### 2.4. Perangkat Lunak Jaringan

1. Mikrotik RouterOS
Mikrotik RouterOS adalah sistem operasi dan perangkat lunak yang dapat digunakan untuk mengubah komputer menjadi router jaringan yang andal, yang mencakup berbagai fitur yang dirancang untuk jaringan IP dan nirkabel, untuk digunakan oleh ISP dan penyedia layanan akses [3].
2. Router
RouterOS merupakan sistem operasi yang dapat menjadikan PC biasa memiliki fungsi sebagai router dengan fitur yang lengkap [7]. RouterOS di install ke dalam sistem operasi tersendiri dan tidak tergantung pada sistem lainnya, misalkan windows dan linux.

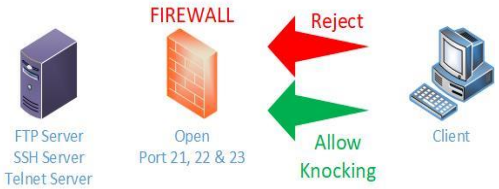
### 2.5. Keamanan Jaringan

Jaringan komputer memberikan kemudahan dalam memberikan perlindungan terhadapa data. Walaupun data yang ada didalam komputer itu masih dapat diakses oleh komputer lain, itu tetap dapat membatasi hak akses orang lain ke dalam data tersebut. Selain itu, juga dapat memusatkan setiap komputer yang terhubung ke dalam jaringan [8].

## 3. Hasil dan Pembahasan

Berdasarkan analisis penelitian bertujuan mendapatkan solusi pemecahan masalah dan menghasilkan suatu desain rancangan keamanan jaringan. Dalam percobaan ini melalui tiga tahap yang dilakukan yaitu: membuat desain rancangan keamanan jaringan, *setting* mikrotik dengan metode *port knocking* dan *port blocking*, dan pengujian awal dan pengujian akhir.

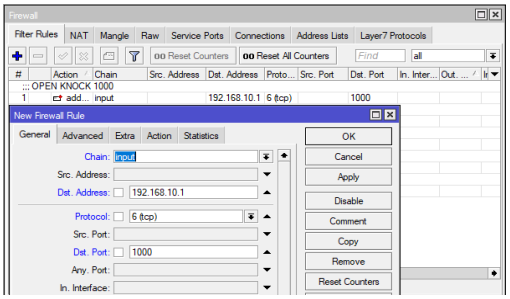
### 3.1. Desain Rancangan Keamanan Jaringan




Gambar 1. Rancangan Usulan

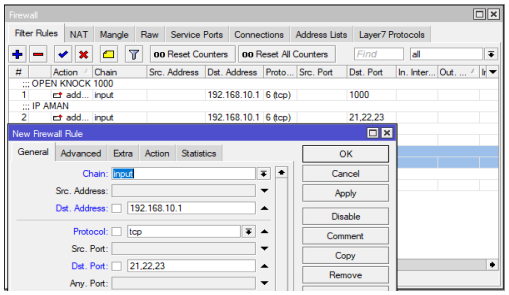
Pada rancangan ini, penulis membuat dan mengimplementasikan keamanan jaringan tambahan dengan metode *port knocking* dan *port blocking*. *Port knocking* dan *port blocking* merupakan sistem keamanan yang bertujuan melindungi dari serangan exploit dengan melakukan pemindaian *port* dan membatasi akses pengguna. Dengan demikian hanya *user* yang sudah melakukan *open port knocking* terlebih dahulu, baru bisa mengaksese secara penuh untuk membuka dan menutup akses *port*. pada perangkat router RB951Ui-2nD, penulis akan melakukan konfigurasi pada software winbox.

### 3.2. Setting Mikrotik dengan Metode Port Knocking dan Port Blocking



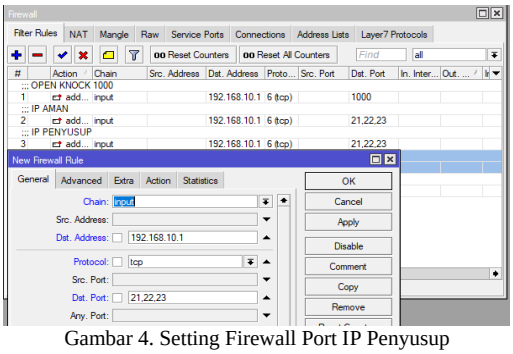

Gambar 2. Setting Firewall Port Knocking

Konfigurasi *port knocking* 1000 > pilih *menu* IP > *Firewall* > Add(+) > di *General* status *Chain* diubah menjadi *input* > masukan IP *Address* di *Dst. Address* 192.168.10.1 > *Protocol* pilih (tcp) > buat *port* unik anda di *Dst. Port* (1000) > di *Action* ubah *Action* menjadi > *add src to address list* > buat keterangan di *Address List Port Knock* 1000 lalu berikan *timeout* nya 00:05:00 (5 menit) klik *apply*, ok.



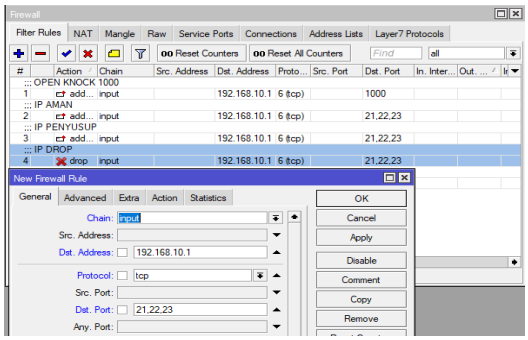

Gambar 3. Setting Firewall Port IP Aman

Konfigurasi *port* IP aman > pilih kembali Add(+) > di *General* status *Chain* diubah menjadi *input* > masukan IP *Address* di *Dst. Address* 192.168.10.1 > *Protocol* pilih (tcp) > di *Dst. Port* pilih *port* mana saja yang ingin diamankan ftp, ssh,telnet (21,22,23) > di *Advenced* pada *Src. Address List* pilih *Port Knock* 1000 > di *Action* ubah *Action* menjadi > *add src to address list* > buat keterangan di *Address List* IP Aman klik *apply*, ok.



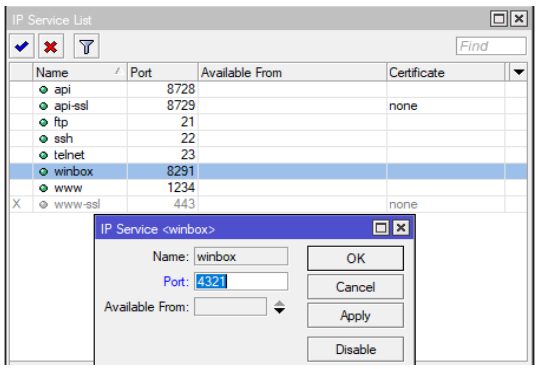

Gambar 4. Setting Firewall Port IP Penyusup

Konfigurasi *port* IP penyusup > pilih kembali Add(+) > di *General* status *Chain* diubah menjadi *input* > masukan IP *Address* di *Dst. Address* 192.168.10.1 > *Protocol* pilih (tcp) > di *Dst. Port* pilih *port* mana saja yang ingin diamankan ftp,ssh,telnet (21,22,23) > di *Advenced* pada *Src. Address List* pilih *Port Knock* 1000 > lalu klik simbol kotak menunjukan tanda (!) artinya ini bukan yang melakukan *port knock* 1000 > di *Action* ubah *Action* menjadi > *add src to address list* > buat keterangan di *Address List* IP Penyusup lalu berikan *timeout* nya 00:05:00 (5 menit) klik *apply*, ok.



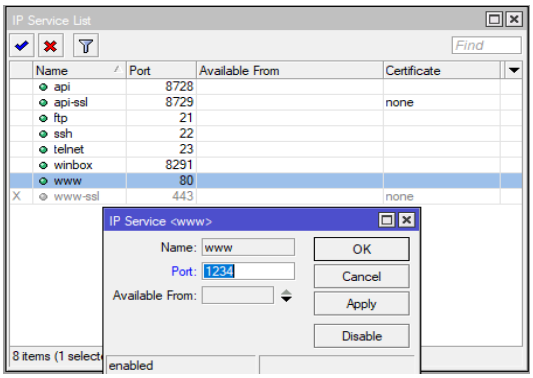

Gambar 5. Setting Firewall IP Drop

Konfigurasi *port* IP drop > pilih kembali Add(+) > di *General* status *Chain* diubah menjadi *input* > masukan IP *Address* di *Dst. Address* 192.168.10.1 > *Protocol* pilih (tcp) > di *Dst. Port* pilih port mana saja yang ingin diamankan ftp,ssh,telnet (21,22,23) > di *Advenced* pada *Src. Address List* pilih IP Aman > lalu klik simbol kotak menunjukan tanda (!) artinya ini bukan IP Aman maka akan di *Drop* IP nya > di *Action* ubah *Action* menjadi *drop* klik *apply*, ok.




Gambar 6. Blokir Port Winbox

Konfigurasi *port* winbox > pilih IP > pilih *Services* > klik dua kali pada winbox > ubah *Port* 8291 menjadi *Port* 4321 klik *apply*, ok.

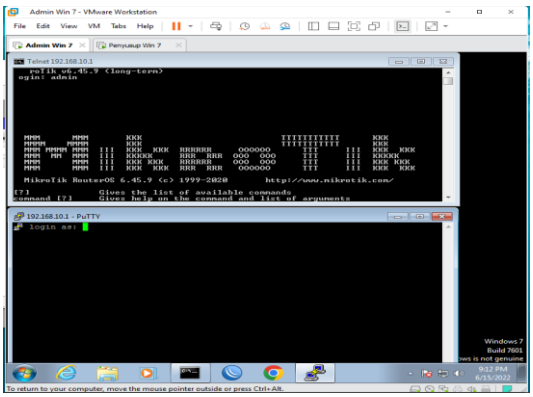



Gambar 7. Blokir Port WWW

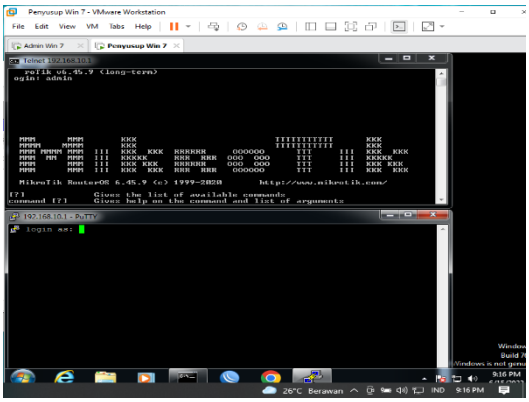
Konfigurasi *port* www > pilih IP > pilih *services* > klik dua kali pada www > ubah *Port* 80 menjadi *Port* 4321 klik *apply*, ok.

### 3.3. Pengujian Awal

Dalam pengujian awal pada simulasi ini belum diterapkan rancangan usulan yang diberikan kepada PT Securindo Packatama Indonesia cabang Tanah Abang yaitu sebelum adanya penambahan keamanan jaringan metode *port knocking* dan *port blocking*, berikut pengujian awal yaitu:

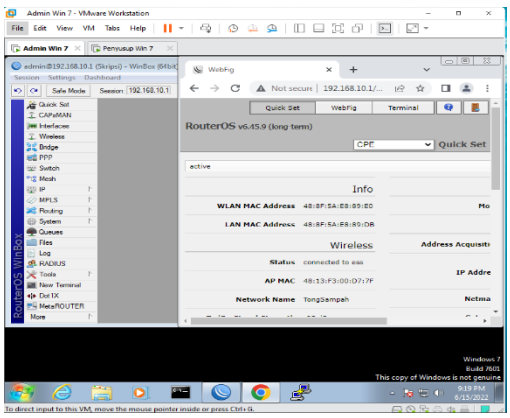


Gambar 8. Pengujian Awal Port

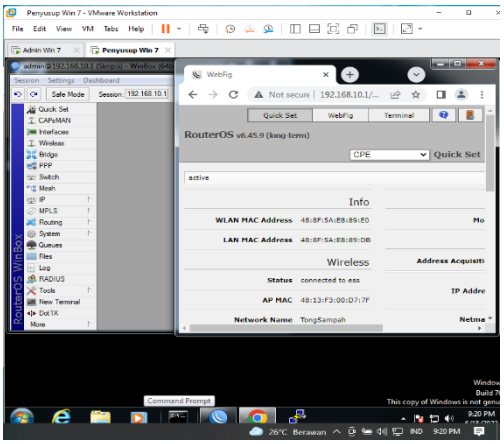


Gambar 9. Pengujian Awal Port Telnet PC Penyusup

Tahap pertama memperlihatkan kondisi *port* telnet dan *port* SSH pada pengujian PC admin dan PC penyusup sebelum diterapkan metode *port knocking* dan *port blocking* keduanya dapat mengakses secara bebas.



Gambar 10. Pengujian Port winbox dan www PC Admin

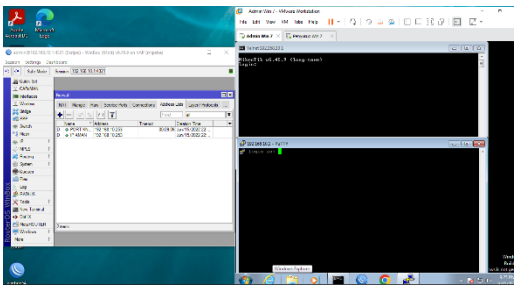


Gambar 11. Pengujian Port winbox dan www PC Penyusup

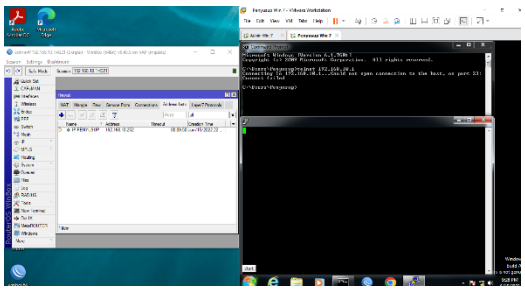
Tahap kedua memperlihatkan kondisi *port* winbox dan *port* www pada pengujian PC admin dan PC penyusup sebelum adanya perubahan angka *port* pada *port* winbox dan www maka dapat diakses.

### 3.4. Pengujian Akhir

Hasil dari pengujian akhir telah menerapkan rancangan keamanan jaringan usulan yang dibuat dan diterapkan pada PT Securindo Packatama Indonesia yaitu dengan ditambahkannya keamanan jaringan yang baru menggunakan metode *port knocking* dan *port blocking*, berikut hasil pengujian akhir yaitu:



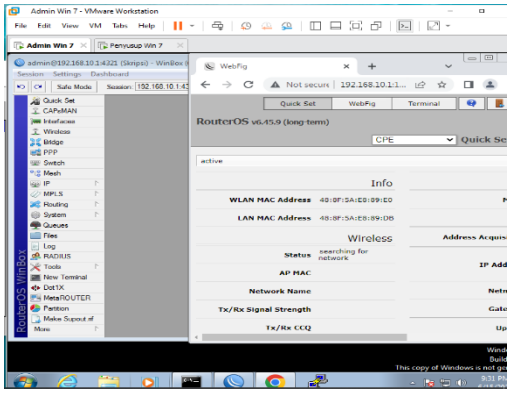
Gambar 12. Hasil Port telnet dan Port SSH PC Admin



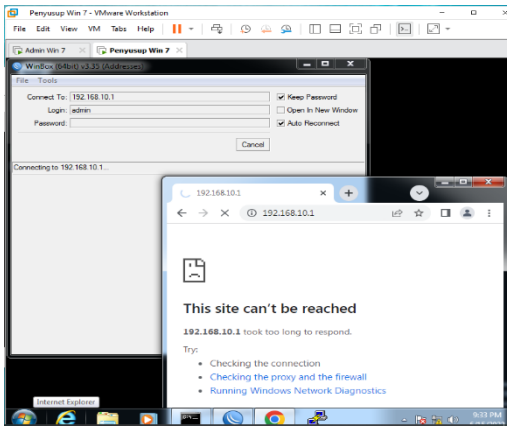
Gambar 13. Hasil Port telnet dan Port SSH PC Penyusup

Tahap pertama memperlihatkan hasilnya dimana kondisi *port* telnet dan *port* SSH pada pengujian PC admin dan PC penyusup sesudah diterapkannya metode *port knocking* dan *port blocking*, hanya PC Admin yang bisa melakukan *open knocking* karena sebelumnya sudah *open port knock* 1000 maka bisa mengakses

secara penuh sedangkan PC Penyusup tidak bisa mengakses.



Gambar 14. Hasil Port winbox dan www PC Admin




Gambar 15. Hasil Port winbox dan www PC Penyusup

Tahap kedua memperlihatkan hasilnya dimana kondisi *port* winbox dan *port* ww pada pengujian PC Admin dan PC Penyusup sesudah adanya perubahan angka *port* pada *port* winbox dan www maka hanya PC Admin yang dapat melakukan remote secara penuh karena PC Admin mengetahui perubahan yang terjadi pada angka *port* tersebut sedangkan PC Penyusup tidak mengetahui perubahan pada angka *port* winbox dan www maka tidak bisa meremotenya.

## 4. Kesimpulan

Berdasarkan hasil pembahasan dan penelitian analisa Local Area Network pada PT Securindo Packatama Indonesia cabang Tanah Abang yang telah diuraikan, maka penulis dapat mengambil beberapa kesimpulan yaitu:

1. Menerapkan keamanan jaringan dengan menggunakan metode *port knocking* dan *port blocking* untuk meningkatkan keamanan jaringan, terutama pada *port* yang dibuka sebelumnya yang tidak memiliki keamanan dan dapat mencegah orang yang tidak berwenang untuk mengaksesnya.
2. Diterapkannya *port blocking* pada *port* winbox dan *port* www bertujuan untuk memperkuat terjadi penyalahgunaan konfigurasi nikrotik melewati winbox maupun melewati webfig pada orang yang tidak bertanggung jawab.

Kemudian penulis akan memberikan saran setelah menganalisa keamanan jaringan *Local Area Network* pada PT Securindo Packatama Indonesia yaitu:

1. Staff IT harus dilatih tentang metode *port knocking* dan *port blocking*.
2. Perlu diadakan perawatan secara berskala terhadap keamanan jaringan perusahaan itu sendiri.
3. Keamanan siber dapat dikembangkan kembali menggunakan metode terbaru sesuai dengan kebutuhan.

kesimpulan tidak boleh ada referensi. Kesimpulan berisi fakta yang didapatkan, cukup menjawab permasalahan atau tujuan penelitian (jangan merupakan padaembahasan lagi); Nyatakan kemungkinan aplikasi, implikasi dan spekulasi yang sesuai. Jika diperlukan, berikan saran untuk penelitian selanjutnya.

## Daftar Rujukan

[1] M. Iqbal, A. MT, and H. B. S. M.Kom, "ANALISA DAN SIMULASI KEAMANAN JARINGAN UBUNTU SERVER DENGAN PORT KNOCKING, HONEYPOT, IPTABLES, ICMP," *Cyber Secur. dan Forensik Digit.*, vol. 3, no. 1, pp. 27–32, Jul. 2020, doi: 10.14421/CSECURITY.2020.3.1.1933.

[2] A. Amarudin and F. Ulum, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking," *J. Teknoinfo*, vol. 12, no. 2, pp. 72–75, Jul. 2018, doi: 10.33365/JTI.V12I2.121.

[3] S. K. M. P. Untung Suprihadi and M. S. Indonesia, *Tutorial Jaringan Handal Dengan Mikrotik Dan Cisco*. Media Sains Indonesia, 2021.

[4] T. M. Diansyah, "ANALISIS IMPLEMENTASI DYNAMIC PORT KNOCKING PADA SERANGAN DOS | Majalah Ilmiah Teknik." http://siakad.univamedan.ac.id/ojs/index.php/mit/article/view/172 (accessed Apr. 04, 2022).

[5] M. Sugianto, M. R. Utomo, and F. Mukharom, *Panduan Dasar VMware vSphere Edisi 2019: Virtualisasi Server Handal Menggunakan VMware vSphere 6.7*. Excellent Publishing, 2019.

[6] A. P. Juledi *et al.*, *Internetworking dan TCP/IP*. Yayasan Kita Menulis, 2021.

[7] S. P. M. M. Ilham Ilahi, *ADMINISTRASI INFRASTRUKTUR JARINGAN*. XP Solution Surabaya, 2020.

[8] M. Badru and Akmaludin, "IMPLEMENTASI AUTOMATIC FAILOVER MENGGUNAKAN ROUTER MIKROTIK UNTUK OPTIMALISASI JARINGAN," 2019. https://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/view/1009/1076 (accessed Apr. 20, 2022).