Jurnal Ilmiah Teknologi - Informasi dan Sains (TeknoIS)
Volume 8 Nomor 2 Bulan November 2018 Hal. 25-36
p-ISSN : 2087-3891 dan e-ISSN : 2597-8918

# Pengembangan Notifikasi Email Untuk Keamanan Port Menggunakan Metode *Port Knocking*

**Marina Apriani[1], Arif Harbani[2]**
Program Studi Tenik Informatika
STIKOM Binaniaga Bogor.
Email: arifharbani@gmail.com

***ABSTRACT***

*Port Knocking is a method that is used to close all access to a particular port and a client can access the port when it has successfully performed a series of port beats to several ports that have been set up as trigger ports. This is a problem when the client is not entitled to remote access to the proxy port and is vulnerable to attacks from outside who want to retrieve information from the proxy. Port security on proxy with the port knocking method with the technique of hiding ports is a solution to secure ports from clients that are not allowed to do remote access.*

*The method used includes four stages of work, namely analysis, design, implementation, and testing. The analysis phase is done by observing the problems in the agency and the needs in the implementation process. The design phase is mapping the scope topology in the implementation process. The implementation phase is carried out by performing several work procedures and the testing phase is carried out to carry out several testing procedures so that conclusions arise.*

*Development of port knocking is done by adding email notifications to the router. The addition of notifications aims to provide an early warning to the administrator when there is a client that successfully accesses one of the ports used as a remote access point.*

***Keywords****: port knocking, email notification, port trigger, remote access, mikrotik.*

***ABSTRAK***

*Port Knocking merupakan suatu metode yang digunakan untuk menutup seluruh akses pada port tertentu dan seorang client dapat melakukan akses pada port tersebut ketika telah berhasil melakukan serangkaian ketukan port kepada beberapa port yang telah diatur sebagai port pemicu. Hal itu menjadi masalah ketika clent yang tidak berhak melakukan remote access ke port mikrotik dan rentan terhadap serangan dari luar yang ingin mengambil informasi dari mikrotik. Keamanan port pada mikrotik dengan metode port knocking dengan teknik menyembunyikan port adalah solusi untuk mengamankan port dari client yang tidak diizinkan untuk melakukan remote access.*

*Metode yang digunakan meliputi empat tahap pengerjaan, yaitu analisis, perancangan, implementasi, dan pengujian. Tahap analisis dilakukan pengamatan masalah pada instansi dan kebutuhan dalam proses implementasi. Tahap perancangan dilakukan pemetaan terhadap topologi ruang lingkup dalam proses pengerjaan implementasi. Tahap implementasi dilakukan dengan melakukan beberapa prosedur pengerjaan dan tahap pengujian dilakukan untuk melakukan beberapa prosedur pengujian sehingga memunculkan simpulan.*

*Pengembangan pada port knocking dilakukan dengan menambahkan notifikasi email pada router. Penambahan notifikasi bertujuan untuk memberikan peringatan dini kepada administrator ketika terdapat client yang berhasil melakukan akses pada salah satu port yang digunakan sebagai jalur remote access.*

***Kata Kunci****: port knocking, email notification, port trigger, remote access, mikrotik*

## PENDAHULUAN

*Router* adalah perangkat keras jaringan komputer yang menghubungkan beberapa jaringan yang sama atau berbeda dan juga sebagai alat untuk mengatur keluar dan masuknya suatu data pada jaringan, *router* berada pada lapisan terluar yang terhubung langsung ke jaringan publik. *Router* sering menjadi salah satu target penyerang untuk tujuan mengambil informasi data yang melalui *router*. Hal ini mengakibatkan keamanan *router* rentan terhadap serangan dari luar maupun dalam. Selain itu administrator tidak bisa secara terus menerus memantau *router* yang berada di ruang NOC tempat *router* mikrotik di letakkan.

Permasalahan ini yang mengharuskan pihak administrator jaringan untuk membuat keamanan *router* khususnya *router* mikrotik dengan menutup port mikrotik. *Port* yang terbuka akan mempermudah penyerang mengetahui *port-port* yang mudah diakses dengan menggunakan aplikasi *tool scanner* seperti NMAP-Zenmap, *MiTec Network Scanner*, *SoftPerfect Network Scanner, Network DeepScan, Network Scanner* dan lain-lain. Solusi dari masalah tersebut diperlukan suatu keamanan pada *router* mikrotik agar *port-port* yang terbuka dapat tertutup sehingga sulit diketahui penyerang bahwa *port* tersebut tertutup. Metode yang digunakan adalah *port knocking*. *Port knocking* adalah teknik yang dilakukan untuk membuka akses ke *port* tertentu yang telah diblok oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa protokol TCP, UDP maupun ICMP.

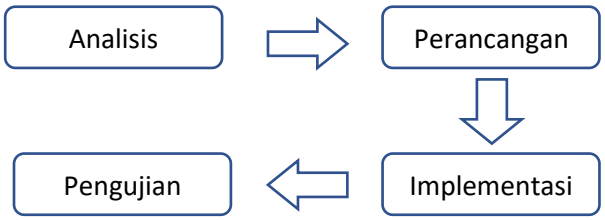
Selain itu untuk mempermudah administrator jaringan dalam memantau *router* yaitu dengan mengirimkan notifikasi langsung ke administrator jaringan apabila ada serangan pada *router* mikrotik. Notifikasi yang digunakan merupakan notifikasi *email.*

Rumusan masalah dalam penelitian ini adalah:
1. Bagaimana pengaruh notifikasi email terhadap proses autentikasi Port Knocking
2. Bagaimana menerapkan keamanan port dengan menggunakan metode *port knocking* dengan notifikasi email ?

Adapun tujuan penelitian ini dimaksudkan untuk:
1. Menjaga keamanan port menggunakan metode *port knocking.*
2. Membatasi penggunaan *remote access* dari *client* yang yang tidak mempunyai hak untuk melakukan *remote access* dan *router* dapat melakukan pengiriman notifikasi *email* yang terkirim langsung kepada pihak administrator ketika terdeteksi adanya serangan

## METODE

Metode yang digunakan dalam pembuatan Keamanan *Port* pada Mikrotik dengan Metode *Port Knocking* terdiri dari 4 tahapan. Metode dapat dilihat pada Gambar 1.




Gambar 1 Metode pengerjaan

**Fase Analisis**

Tahap ini merupakan langkah pemahaman sistem, identifikasi masalah dan kebutuhan sehingga dapat menganalisis rancangan pembuatan sesuai dengan kebutuhan yang ada.

**1. Analisis masalah**

Masalah yang dihadapi adalah banyaknya pengguna perangkat mikrotik yang harus diatur dan dikelola. Banyaknya *username* dan *password* yang digunakan membuat keamanan mikrotik menjadi rentan akan serangan karena penyerangan jenis *brute force* mencoba semua kombinasi *username* dan *password.*

**2. Analisis kebutuhan**

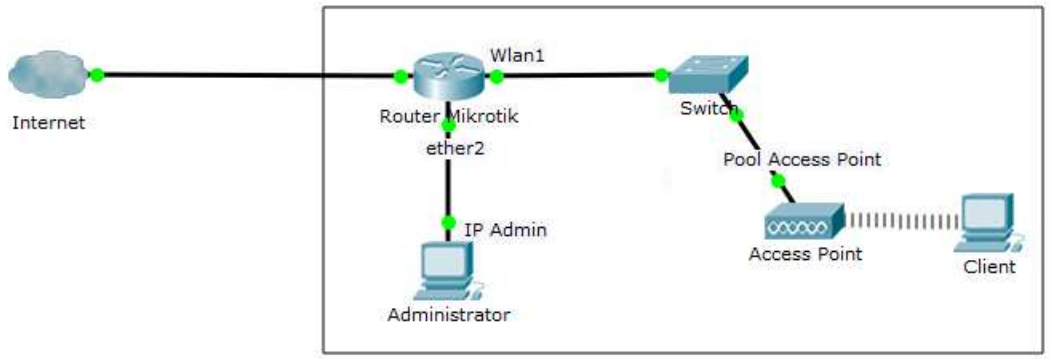
Dalam pembuatan keamanan *port* pada mikrotik dengan *port knocking* dibutuhkan perangkat keras dan perangkat lunak yang merujuk ke Tabel 1.

Tabel 1 Daftar kebutuhan perangkat keras dan perangkat lunak

| Perangkat keras | Spesifikasi | Perangkat lunak | Spesifikasi |
|---|---|---|---|
| Mikrotik *router* | Mikrotik RB951UI-2ND | Winbox | Winbox v3.10 |
| Kabel UTP | Kabel *Straight* | Google Chrome | |
| Laptop | Laptop HP *Notebook* | Putty | |
| RAM | 4 GB | | |

**Fase Perancangan**

Perancangan dilakukan menggunakan jaringan yang sudah ada untuk mengkonfigurasi jaringan mikrotik. Tahap perancangan ini bertujuan untuk memberikan gambaran tentang topologi jaringan sesuai dengan kebutuhan. Topologi yang digunakan hanya mengambil sebagian dari topologi dalam skala laboratorium terlihat pada gambar digunakan hanya yang berada dalam kotak. Topologi jaringan yang dibuat seperti ditunjukkan pada Gambar 2. Sedangkan untuk daftar pengalamatan IP pada topologi jaringan merujuk pada Tabel 2.




Gambar 2. Topologi jaringan

Tabel 2 Daftar pengalamatan IP pada topologi jaringan

| Titik | IP |
|---|---|
| Ether2 | 192.168.88.1/24 |
| Wlan1 | 10.10.10.1/24 |
| IP Admin | 192.168.88.2/24 |
| *Pool Access Point* | 10.10.10.0/24 |

**Fase Implementasi**

**1. Konfigurasi IP *Address***

Pemberian IP dilakukan pada *interface* ether2 dengan alamat 192.168.88.1/24 yang digunakan untuk menghubungkan admin jaringan dengan mikrotik. Selain pemberian IP pada ether2, Pemberian IP juga dilakukan pada *interface* wlan1 dengan alamat 10.10.10.1/24. Pemberian alamat pada wlan1 digunakan sebagai alamat *access point*.

**2. Konfigurasi *Access Point***

Pembuatan *access point wireless* pada mode *access point bridge* dengan pemberian nama *ssid* yaitu wifi. Pembuatan *wireless* tersebut dilanjutkan dengan pembuatan IP *pool* yang mengarah ke IP *address interface* wlan1 yang sudah dikonfigurasi. Pembuatan IP *pool* ini bertujuan agar memberikan *range* IP yang akan didapatkan oleh *client* ketika mengaktifkan atau menggunakan *access point* yang telah dibuat. Pembuatan *range* IP dari 10.10.10.2 sampai dengan 10.10.10.254 yang diberi nama pool1. Pembuatan IP DHCP *server* berfungsi sebagai pemberi IP kepada *client* yang melakukan permintaan IP kepada *interface* yang telah ditunjuk sebagai DHCP *server*. *Interface* yang akan digunakan sebagai *dhcp-server* adalah wlan1 dan pemberian IP diberikan dengan *list* IP yang sudah dikonfigurasi pada *pool*. Penambahan IP *gateway* dari mikrotik bertujuan untuk mengetahui IP mikrotik ketika *client* menggunakan *access point* dengan *network address* 10.10.10.0/24.

**3. Konfigurasi *Firewall Filter Rules***

Konfigurasi utama dalam pembuatan keamanan *port* dengan metode *port knocking* adalah konfigurasi *firewall filter rule* pada mikrotik. *Firewall filter rule* bertujuan sebagai pengatur data yang masuk ataupun yang keluar melalui router sehingga router dapat membuat aturan untuk setiap data apakah data tersebut diterima, diteruskan ataupun dibuang. Pada konfigurasi *port knocking,* penggunaan *firewall filter rule* digunakan untuk menutup semua akses yang masuk pada port *remote access* seperti SSH, telnet, winbox, ataupun *web config* (*webfig). Web config* merupakan sebuah *utility* pada mikrotik yang digunakan untuk melakukan konfigurasi router dengan *web browser.*

Sebelum melakukan *firewall filter rules, default port* yang digunakan pada setiap jenis *remote access* dialihkan pada *port* baru. Hal tersebut dilakukan untuk meningkatkan keamanan setiap *port* sehingga ketika ada seseorang yang ingin melakukan *remote access* dengan tujuan *port default,* maka akses tidak akan bisa dilakukan. Perubahan setiap *port* akses merujuk pada Tabel 3.

Tabel 3 Perubahan *port* akses

| Jenis Akses | *Port default* | *Port* baru |
|---|---|---|
| SSH | 22 | 2224 |
| Telnet | 23 | 2322 |
| Webfig | 80 | 8020 |
| Winbox | 8291 | 8280 |

Ketika semua *port* telah dialihkan pada *port* baru, dibuat sebuah konfigurasi pada *firewall filter rule* untuk memberikan akses izin kepada administrator menuju *router* tanpa harus menggunakan metode *port knocking*. Dalam *rule* tersebut, administrator menggunakan IP statik dengan alamat 192.168.88.2/24. Konfigurasi tersebut seperti ditunjukkan pada Gambar 3.

```
;;; ADMIN IP STATIC

ip firewall filter add chain=input action=accept protocol=tcp src-address=192.168.88.2 dst-address=192.168.88.1 dst-port=8020,2224,2322,8280
```

Gambar 3. Pembuatan *firewall filter rule* untuk administrator

Pembuatan *port knocking rule* pada mikrotik untuk port yang digunakan sebagai *remote access.* Pembuatan *rule*s tersebut bertujuan untuk menutup semua akses pada *port* yang digunakan sebagai *remote access* dan hanya akan bisa dibuka jika seorang *client* mampu melakukan *knocking port* secara berurut.

```
;;; Rule Knocking Port WEBFIG

ip firewall filter add chain=input action=add-src-to-address-list protocol=tcp address-list=WEBFIG1 address-list-timeout=10s dst-port=3333

ip firewall filter add chain=input action=add-src-to-address-list protocol=tcp src-address-list=WEBFIG1 address-list=WEBFIG2 address-list-timeout=10s dst-port=1111

ip firewall filter add chain=input action=add-src-to-address-list protocol=tcp src-address-list=WEBFIG2 address-list=WEBFIG_ACCEPT address-list-timeout=10m dst-port=2222 log=yes

ip firewall filter add chain=input action=drop protocol=tcp src-address-list=!WEBFIG_ACCEPT dst-port=8020
```

Gambar 4. Pembuatan *firewall filter rule port* webfig

Gambar 4 menunjukkan bahwa pembuatan *rule knocking* untuk *port webfig*. Baris pertama menunjukan perintah bahwa *port* pemicu sebagai *port* palsu awal yang digunakan adalah *port* 1111, *port* pemicu selanjutnya 2222, dan *port* pemicu terakhir untuk dapat menuju ke *port webfig* adalah 3333. Ketika berhasil melalui semua *port* pemicu yang ada, maka untuk masuk ke *port* webfig hanya lakukan *request port webfig* yang sudah dialihkan. Peningkatan keamanan *port* dilakukan pada efisiensi waktu yang digunakan. Batas waktu yang melebihi saat melakukan *request port* pemicu maka permintaan tidak akan berhasil dan diulang. Hal ini berlaku juga untuk *port* mikrotik yang lain namun dengan *port* pemicu yang berbeda tiap pintunya, misalnya Telnet, SSH dan Winbox. Port pemicu yang digunakan dalam pembuatan port knocking merujuk pada tabel 4.

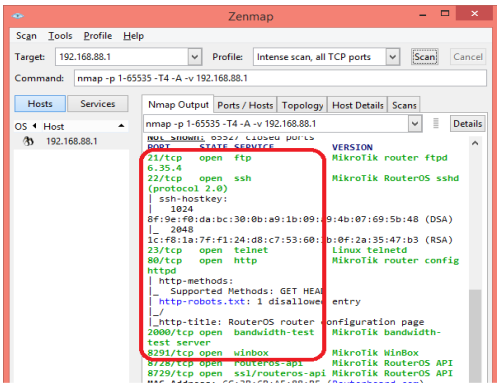
Tabel 4 Daftar *port* pemicu pembuatan *port knocking*

| Jenis Akses | *Port* pemicu 1 | *Port* pemicu 2 | *Port* pemicu 3 | *Port* baru |
|---|---|---|---|---|
| SSH | 4444 | 6060 | 5555 | 2224 |
| Telnet | 1234 | 5678 | 1298 | 2322 |
| Webfig | 3333 | 1111 | 2222 | 8020 |
| Winbox | 1122 | 5566 | 3344 | 8280 |

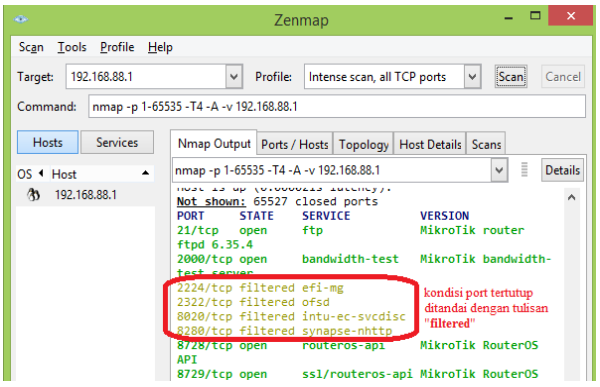
**Fase Pengujian**

**1. Pengujian *port scanning***

Pengujian ini dilakukan dengan menggunakan salah satu aplikasi *tool scanner* yaitu Zenmap. Hal ini dilakukan untuk mengetahui kondisi *port* mikrotik sebelum dan sesudah pemasangan *port knocking*. IP *address* dari *interface* ether2 yaitu 192.168.88.1 dimasukan kedalam *tool box* target pada Zenmap. IP tersebut akan dilakukan *scanning* pada *port* mikrotik. Hasilnya menunjukan pada Gambar 5 status atau kondisi semua *port* mikrotik dalam keadaan terbuka karena mikrotik belum dilakukan pemasangan *port knocking*.




Gambar 5. *Scanning port* sebelum pemasangan *port knocking*

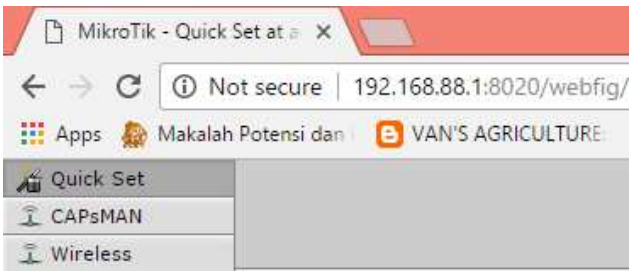



Gambar 6. *Scanning port* sesudah pemasangan port *knocking*

Namun sebaliknya pada Gambar 6 menunjukan kondisi semua *port* mikrotik dalam keadaan tertutup dengan tulisan *"filtered*" dan nama dari *port* mikrotik tersebut tidak dapat dikenali. Hal tersebut dikarenakan sebelumnya *port default* mikrotik sudah dialihkan ke *port* baru. Kondisi semua *port* dalam keadaan tertutup karena sudah dilakukan pemasangan *port knocking* pada *router* mikrotik.

**2. Akses *router* dengan alamat admin**

Pengujian ini dilakukan dengan menggunakan alamat admin. Admin bisa langsung masuk ke *port* mikrotik yang dituju tanpa melakukan *knocking port*. Gambar 7 menunjukkan bahwa admin bisa langsung masuk ke *port webfig* tanpa melakukan *knocking* atau tanpa membuka *port* pemicu terlebih dahulu hanya dengan membuka *port webfig* yang sudah dialihkan.




Gambar 7. Admin membuka webfig

**3. Pengujian *client* akses tanpa melakukan *knocking***

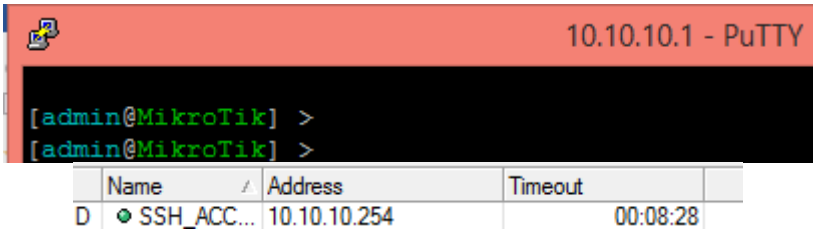
Pengujian ini dilakukan dengan *client* yang melakukan koneksi ke *access point* yang sudah dibuat. Dengan cara seperti itu, *client* dapat melakukan koneksi mikrotik menggunakan IP *gateway* dari *access point*. Pengujian ini dilakukan dengan cara *client* melakukan akses mikrotik tanpa melakukan *knocking* ke *port* pemicu. Gambar 8 menunjukkan bahwa pada awal gambar *client* tidak bisa

membuka *port* winbox tersebut dengan menggunakan *port default*. Sedangkan gambar yang berada di sebelahnya menunjukkan bahwa meskipun *client* mengetahui *port* winbox yang telah dialihkan dari *port default,* namun tetap *client* tidak berhasil membuka *port* winbox. Hal ini disebabkan *client* tidak melakukan *knocking port* ke *port* pemicu sehingga akses pun tidak bisa dilakukan.


Gambar 8. *Client* gagal masuk *port* winbox

**4. Pengujian client akses dengan melakukan knocking**

Pengujian ini dilakukan dengan *client* yang melakukan *knocking* ke *port* pemicu terlebih dahulu lalu masuk ke *port* SSH yang sudah dialihkan dari *port default*. Gambar 9 menunjukkan bahwa *client* berhasil membuka *port* SSH dengan melakukan *knocking* ke *port* pemicu yang telah dibuat untuk *port* SSH. Namun seperti penjelasan sebelumnya bahwa untuk menambah keamanan mikrotik dilakukan pembatasan waktu akses yang telah dibuat pada *firewall filter rule.* Ketika batas waktu yang ditentukan telah habis maka *client* tidak dapat melakukan akses ke *port* SSH, melainkan harus melakukan *knocking port* ke *port* pemicu lagi terlebih dahulu.




Gambar 9. *Client* Berhasil masuk dengan *knocking*

## HASIL DAN PEMBAHASAN

## METODE PENGEMBANGAN

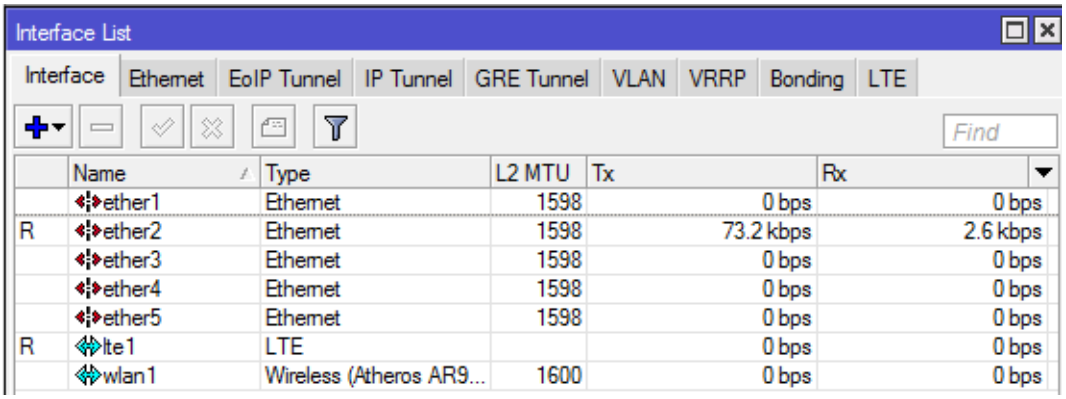
### Fase Perancangan

Untuk menerapkan notifikasi *email* maka dibuat penerapan topologi. Gambar 2 memperlihatkan topologi yang akan dibangun untuk implementasi *port knocking* dengan notifikasi *email*. Topologi pada pengembangan ini menggunakan akses internet untuk masuk ke dalam *email*. Pemberian IP *address* untuk topologi dibawah merujuk pada Tabel 2.

### Fase Implementasi

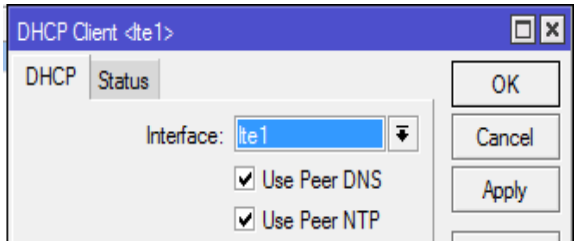
Pada tahap ini dilakukan konfigurasi pada *routerboard* mikrotik RB951 menggunakan perangkat lunak WinBox. Pada tahap pertama yaitu melakukan beberapa langkah konfigurasi pada mikrotik agar

dapat melakukan akses internet. Sumber internet yang digunakan berasal dari *tethering handphone* menggunakan USB pada mikrotik. Pada saat *tethering* diaktifkan, mikrotik akan membaca *interface* LTE seperti yang ditunjukkan pada Gambar 10.

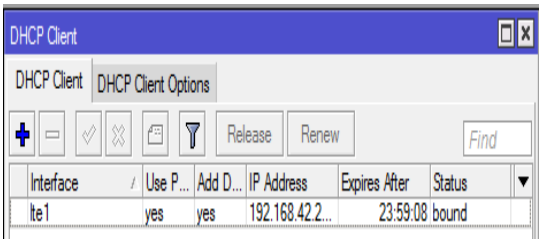



Gambar 10 *Interface* mikrotik

Pada saat mengaktifkan fitur *tethering* pada *handphone* tersebut sudah menyediakan DHCP server dan DNS. Konfigurasi DHCP client pada mikrotik dengan parameter *interface* yang menuju ke *handphone* (*interface* LTE) seperti yang ditunjukkan pada Gambar 11.




Gambar 2 Konfigurasi DHCP client




Gambar 3 Status DHCP client

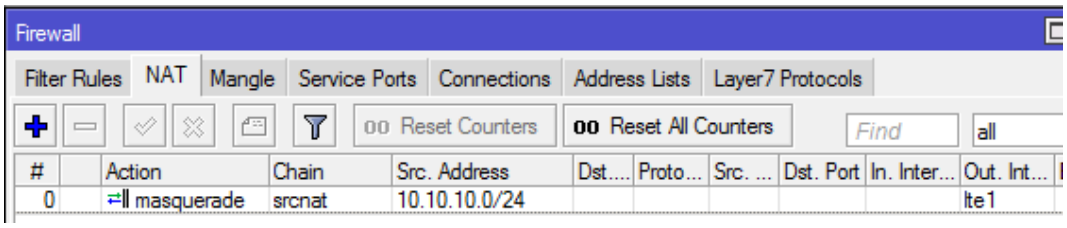
DHCP client pada *router* akan berubah menjadi status *bound* ini artinya *router* berhasil mendapatkan informasi IP *Address* dari *handphone* yang ditunjukkan pada Gambar 12.

Konfigurasi yang digunakan hampir sama seperti konfigurasi mikrotik yang bersifat *dynamic* untuk melakukan konfigurasi DHCP client. Apabila DNS sudah didapatkan mikrotik sudah dapat melakukan akses internet, pengecekan dilakukan dengan melakukan ping ke internet seperti terlihat pada Gambar 13.

```
[admin@MikroTik] > ping 192.168.42.129
  SEQ HOST                                     SIZE TTL TIME  STATUS
    0 192.168.42.129                             56  64 1ms
    1 192.168.42.129                             56  64 0ms
    2 192.168.42.129                             56  64 0ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=0ms
   max-rtt=1ms
```

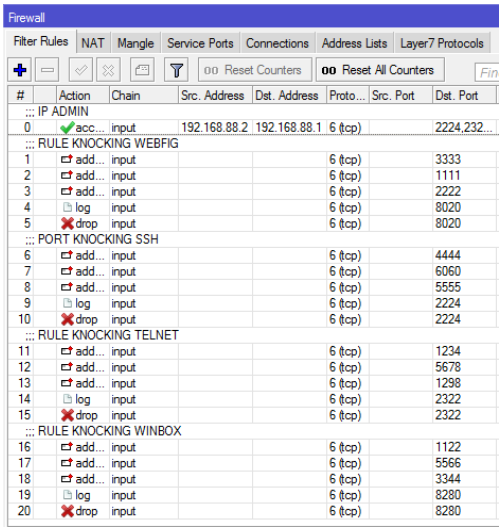
Gambar 4 Pengecekan ping akses internet

Koneksi *access point* yang telah dibuat pada *router* belum didistribusikan pada IP *private*, hal tersebut karena IP *private* belum mengenali koneksi masuk yang berasal dari *access point*. Konfigurasi selanjutnya dapat dilakukan pada bagian *firewall* agar IP *private* yang digunakan sebagai *client* pada pembuatan *port knocking* dapat terkoneksi dengan internet. Konfigurasi yang dilakukan seperti ditunjukan pada Gambar 14.



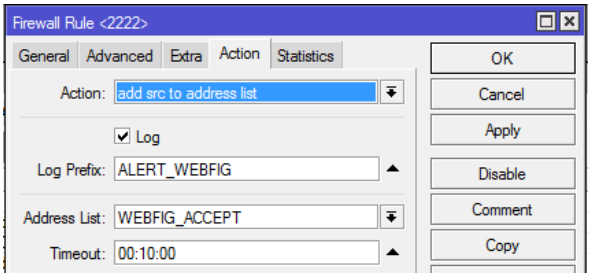

Gambar 5 Konfigurasi NAT

Konfigurasi utama dalam pembuatan *port knocking* dengan notifikasi *email* adalah konfigurasi *firewall filter rule*, memasukan akun *email* dan pembuatan *scheduler* pada mikrotik. Pada konfigurasi ini, *firewall filter rule* digunakan untuk pembuatan *rule* log. Log adalah suatu fitur mikrotik untuk menambahkan segala informasi ataupun paket data yang masuk maupun keluar ke log. Penggunaan log berfungsi sebagai pencatat setiap kejadian dalam *router*. Pembuatan *port knocking* dengan notifikasi *email* menggunakan fitur log sebagai media pencatat yang dilakukan *client* untuk membuka *port* yang telah ditutup. Pembuatan log menggunakan satu kata kunci yang dapat dikenali untuk setiap *port* dan disamakan dengan pembuatan *scheduler,* agar *scheduler* menangkap perintah yang keluar pada log dengan kata kunci yang sama. Penambah konfigurasi log pada *firewall filter rule* ditunjukan pada Gambar 15.

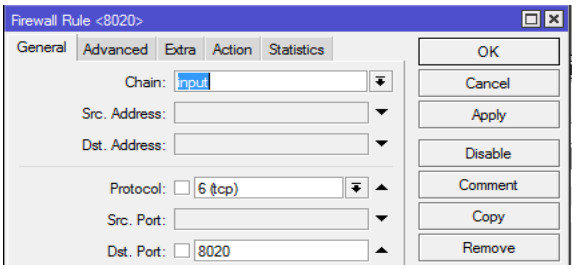



Gambar 6 Penambahan konfigurasi log

Proses pembuatan konfigurasi log terlebih dahulu melakukan penambahan konfigurasi pada *port* pemicu ketiga yang telah dibuat sebelumnya. Pada *port* pemicu ketiga akan diaktifkan log dengan nama “ALERT_WEBFIG” hal ini dilakukan agar ketika *client* berhasil masuk ke *port* pemicu ketiga akan langsung tercatat dalam log. Konfigurasi ditunjukan pada Gambar 16.

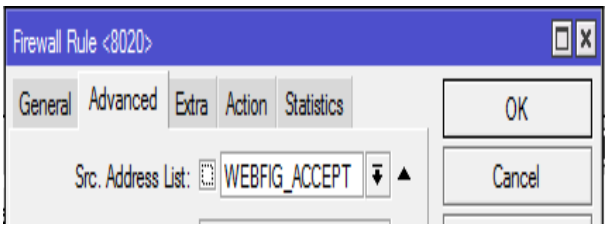



Gambar 7 Penambahan log pada *port* pemicu ketiga

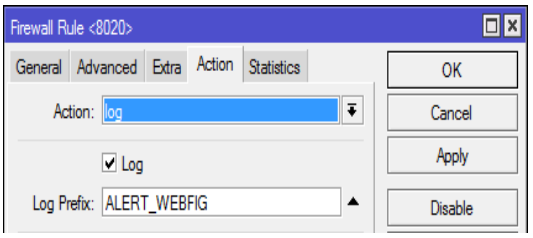



Gambar 8 Pembuatan log pertama

Konfigurasi log selanjutnya pada pembuatan *firewall filter rule* dengan *action log* untuk salah satu contoh *port* mikrotik yaitu *port* webfig. Konfigurasi dilakukan dengan memasukkan "*chain input*" yang artinya menangani setiap paket yang masuk ke *router* atau menuju *router* berupa protokol tcp dengan *port* tujuan yaitu *port* baru dari webfig 8020. Konfigurasi tersebut ditunjukan pada Gambar 17.



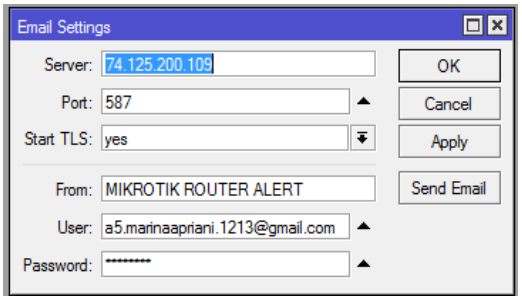

Gambar 9 Pembuatan log kedua



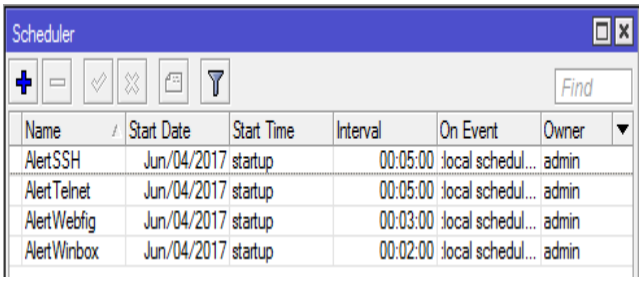

Gambar 10 Pembuatan log terakhir

Gambar 18 menunjukan bahwa paket yang masuk pada *router* seperti pembuatan log pertama bisa dilakukan apabila sumbernya sudah tercatat sebelumnya pada "*address list*" yang diberi nama WEBFIG_ACCEPT ini merupakan penamaan *address list* pada *port* pemicu ketiga. Hal ini berarti log akan tercatat apabila sumber alamat telah melakukan knocking sampai pada *port* pemicu ketiga. Sedangkan Gambar 19 menunjukan perintah atau tindakan yang dilakukan selanjutnya dengan perintah log yang diberi nama ALERT_WEBFIG. Perintah tersebut menjadi perintah terakhir dalam pembuatan log dan setiap masukan yang dibuat dapat tercatat pada log.

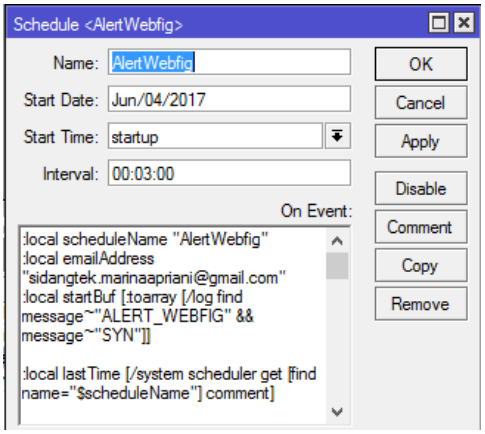
Pembuatan *port knocking* dengan notifikasi *email* dapat berjalan dengan memasukan data-data yang dibutuhkan */tool email* pada fitur mikrotik. Hal ini bertujuan agar mikrotik dapat mengirim *email* dengan meminjam akun *email* yang telah ada. IP *server* yang digunakan berasal dari alamat SMTP *server gmail* dan *port gmail*. Konfigurasi lebih lengkap ditunjukan pada Gambar 20.




Gambar 11 Konfigurasi *email* mikrotik




Gambar 12 Baris perintah *script scheduler*

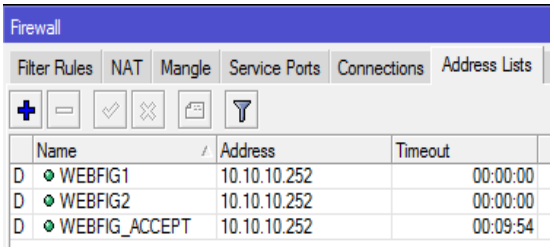



Gambar 13 Pembuatan *schedule* mikrotik

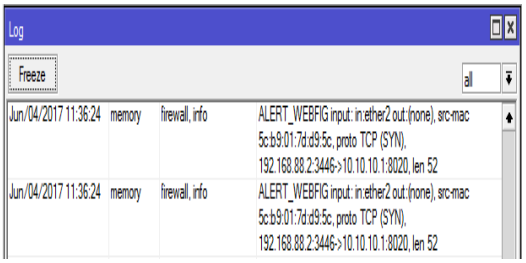
Gambar 21 menunjukan baris perintah dari masing-masing *port* mikrotik yang telah dipasang *port knocking*. Sedangkan Gambar 22 menunjukan pembuatan *schedule* lebih lengkap dengan salah satu *port* mikrotik yaitu *port* webfig. Pada pembuatan *schedule* menggunakan *email* yang berbeda pada *tool box* "on event" dengan konfigurasi *email* sebelumnya dikarenakan fungsi email yang satu hanya sebagai peminjam akun untuk mikrotik agar dapat mengirimkan *email* ke alamat *email* lain. Namun *email* kedua sebagai penerima pesan masuk berupa notifikasi jika *client* berhasil masuk pada *port* mikrotik. Pembuatan *schedule* bertujuan untuk menangkap log yang tercatat dengan nama ALERT_WEBFIG dan mengirimkan *email* ke administrator untuk mengetahui bahwa *port* pada mikrotik telah diketahui.

**Fase Pengujian**

Pengujian dilakukan untuk mengetahui keberhasilan notifikasi *email*, sehingga *port knocking* dengan notifikasi *email* dapat dikatakan berhasil apabila *email* dapat masuk ketika *client* sudah melakukan *knocking* pada *port* mikrotik. Pengujian menggunakan *browser* dan membuka layanan gmail yang telah dibuat. Pada pengujian ini mengambil salah satu *port* mikrotik yaitu *port* webfig.




Gambar 14 IP tercatat masuk *port* webfig




Gambar 15 Serangan tercatat pada log

Gambar 23 menunjukan bahwa *client* mencoba membuka port pemicu pertama, kedua dan ketiga untuk selanjutnya masuk ke *port* webfig yang telah dialihkan. Pada saat *client* berhasil masuk ke *port* webfig yang telah dialihkan perintah log pun mulai tercatat. Perintah log yang tercatat ditunjukan pada Gambar 24.

Selang waktu beberapa menit administrator jaringan akan mendapatkan pesan masuk berupa *email* peringatan bahwa *port-port* pemicu telah berhasil dibuka oleh *client* hingga *port* pemicu terakhir. Hal

ini membuat administrator dapat segera merubah *port* pemicu agar *client* tidak dapat membuka *port* yang telah dibuka. Pesan masuk berupa notifikasi *email* ditunjukan pada Gambar 25.


Gambar 16 Pesan notifikasi *email* yang masuk

## SIMPULAN DAN SARAN

Setelah dilakukan keamanan *port* pada mikrotik dengan metode *port knocking,* dapat dipastikan mikrotik telah memiliki keamanan yang dapat membatasi penggunaan *remote access* menuju mikrotik dapat dibatasi. Sehingga *client* yang tidak mempunyai hak akses tidak dapat membuka mikrotik.

Simpulan yang dapat diambil adalah keamanan *port* menggunakan metode *port knocking* dengan notifikasi *email* telah berhasil dilakukan. Serta notifikasi *email* sudah bisa diterapkan dan sudah berjalan dengan fungsinya. Sehingga administrator mudah memantau *router* tanpa datang ke tempat *router* diletakkan dengan pesan notifikasi *email* yang masuk.

Saran yang dapat diberikan untuk penelitian selanjutnya diintegrasikan notifikasi dengan metode API dan protokol SMTP .

## DAFTAR RUJUKAN

Athailah. 2013. Mikrotik untuk Pemula. Jakarta(ID): Mediakita.

Azwir A. 2014. Mikrotik Firewall : Securing your Router with Port Knocking [Internet]. [diunduh pada 2017 April 02]. Tersedia pada https://www.slideshare.net/akbarazwir/portknock

Towidjojo R. 2015. *Mikrotik Kung Fu: Kitab 1 Edisi 2015*. Palu(ID):Jasakom.

Nurika O. 2012. Review of various firewall deployment models.

Purnama W. 2014. Analisis dan Perancangan Sistem Pengamanan Akses Otentikasi Menggunakan Metode Port Knocking dan Firewall Action Tarpit pada Mikrotik RB951-2N [Internet]. [diunduh pada 2017 Februari 04]. Tersedia pada http://repository.amikom.ac.id/files/Publikasi 11.11.4693.pdf

Frehner C. 2008. Email, SMS, MMS : The linguistic Creativity of asynchronous Discourse in the new media age. Halaman 37

Krzywinski M. 2003. Port Knocking: Network Authentication Across Closed Ports. SysAdmin Magazine 12: 12-17.