PEMANFATAAN METODE *PORT KNOCKING* DAN *BLOCKING* UNTUK KEAMANAN JARINGAN BPKAD PROVINSI SUMSEL

[1]Tito Brades, [2*]Irwansyah
[1,2]Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma
[*]irwansyah@binadarma.ac.id

Abstract - *Network security system at the Regional Financial and Asset Management Agency of South Sumatra Province that has not been optimally at risk of being misused by irresponsible users. This can be proven when scanning the port, it appears that the service port (winbox, telnet and webfig) to perform remote access on the mikrotik router in the open port state. Almost some network security attacks are carried out by knowing the information on open ports and then exploiting. prevention efforts that can be done for security on the service port is to block the port using a firewall. access to the port can still be done through the use of port knocking method. Port knocking is a method to access ports that have been blocked by sending packets or connections in accordance with the knocking rules that have been made.*

Keyword: Port Scanning, Port Knocking, Service Port.

Abstrak – Sistem keamanan jaringan pada Badan Pengelola Keuangan dan Aset Daerah Provinsi Sumatera Selatan yang belum optimal beresiko untuk disalahgunakan oleh pengguna yang tidak bertanggungjawab. Hal ini dapat dibuktikan ketika dilakukan *scanning port*, terlihat bahwa *service port* (winbox, telnet dan webfig) untuk melakukan *remote* akses pada *router* mikrotik dalam status *open port*. Hampir sebagian serangan keamanan jaringan dilakukan dengan cara mengetahui informasi terhadap *port-port* yang terbuka kemudian dilakukan eksploit. Usaha pencegahan yang dapat dilakukan untuk pengamanan pada *service port* yaitu dengan melakukan *blocking port* menggunakan *firewall*. Akses terdahap *port* tetap bisa dilakukan melalui pemanfaatan metode *port knocking*. *Port knocking* merupakan metode untuk mengakses *port* yang telah diblok dengan mengirimkan *packet* atau koneksi sesuai dengan aturan *knocking* yang telah dibuat.

Kata kunci: Port Scaninng, Port Knocking, Service Port.

1. Pendahuluan

Badan Pengelola Keuangan dan Aset Daerah (BPKAD) Provinsi Sumatera Selatan merupakan lembaga pemerintah yang bertanggung jawab terhadap laporan keuangan dan pengelolaan aset daerah khususnya di Provinsi Sumatera Selatan. BPKAD Prov Sumsel memanfaatkan layanan jaringan internet dari ISP (*Internet Service Provider*) Indihome serta mikrotik *routerboard* sebagai pusat pengelolaan jaringannya. Semakin banyak jumlah komputer (*user*) yang terhubung di jaringan lokal maupun publik pada BPKAD Prov Sumsel maka probabilitas serangan *hacker* pada sistem keamanan jaringan tentu tidak dapat dihindari.

Keamanan jaringan merupakan sistem yang dipakai agar terhindar dari ancaman luar yang dapat merusak jaringan dan pencurian data perusahaan dengan cara memberikan proteksi atau perlindungan [1]. Beberapa ancaman keamanan yang sering ditemukan diantaranya *virus*, *malware*, *trojan* dan *port scanning*. *Port scanning* merupakan teknik mendeteksi port-port yang terbuka di sebuah komputer melalui sebuah jaringan [2]. Port yang terbuka rentan untuk diserang oleh *attacker*. Serangan terhadap port yang terbuka dapat dihindari dengan menerapkan metode *Port Knocking* dan *Port Blocking* pada router Mikrotik. *Port Knocking* dan *Port Blocking* bekerja

dengan menutup semua port yang ada pada sistem komputer dan hanya pengguna tertentu yang dapat mengakses sebuah port yang telah ditentukan yaitu dengan cara mengetuk terlebih dahulu.

Permasalahan keamanan jaringan sering terjadi dikarenakan terdapat port yang terbuka dan secara autentikasi maupun otorisasi menyebabkan pengguna yang tidak valid dapat mengakses jaringan secara ilegal [3]. Saat ini dalam sistem keamanan jaringan di BPKAD Prov Sumsel belum terdapat sistem keamanan pada akses layanan port (*port service*) dalam mengatasi serangan khususnya pada port 8291 (winbox), 80 (webfig) dan 23 (telnet). Layanan port tersebut berfungsi agar administrator jaringan dapat mengakses ke router dalam rangka melakukan pengelolaan jaringan di instansi BPKAD Provinsi Sumatera Selatan. Berdasarkan uraian di atas maka diperlukan pemanfaatan metode *port knocking* dan *port blocking* dalam sistem keamanan jaringan. Maka dari itu, penulis tertarik untuk melakukan pengujian pemanfaatan metode *port knocking* dan *port blocking* pada sistem keamanan jaringan di BPKAD Provinsi Sumatera Selatan menggunakan Mikrotik Routerboard.

2. Tinjauan Pustaka

2.1 Keamanan Jaringan

Keamanan jaringan adalah istilah yang luas dan banyak mencakup teknologi, perangkat maupun proses. Dalam istilah paling sederhana, sistem keamanan jaringan adalah proses untuk mengenali dan mencegah seseorang yang tidak mempunyai izin untuk mengakses ke sebuah jaringan. Tujuan dari keamanan jaringan tersebut agar mengantisipasi adanya risiko ancaman pencurian data maupun pengrusakan fisik pada komputer [4]. Beberapa contoh serangan keamanan jaringan diataranya *hacking, port scanning,* dan *distributed denial of service* (DDoS).

2.2 Mikrotik

Mikrotik merupakan perangkat jaringan komputer berupa *hardware* (perangkat keras) seperti *routerboard* maupun *software* (perangkat lunak) seperti *routers OS* yang difungsikan sebagai *router* yang berguna sebagai alat *filtering, switching* maupun yang lainnya [5]. Salah satu jenis mikrotik yang banyak dimanfaatkan oleh adminstrator jaringan adalah mikrotik *routerboard*. Jenis-jenis layanan yang terdapat pada mikrotik diataranya API (*Aplicataion Programmable Interface*), API-SSL, FTP (*File Transfer Protocol*), SSH (*Secure Shell*), Telnet, Winbox, WWW (*Wolrd Wide Web*), dan WWW-SSL.

2.3 Port Knocking dan Port Blocking

Port knocking merupakan metode yang dilakukan untuk membuka akses *port* tertentu yang telah diblok (*port blocking*) oleh *firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi berupa *protocol* (TCP, UDP maupun ICMP) [6]. Apabila koneksi yang dikirimkan oleh *host* sesuai dengan aturan (*rule*) *knocking* yang telah diterapkan maka *firewall* akan membuka atau memberikan akses ke *port* yang telah di-*block*. Dengan menerapkan cara ini, perangkat jaringan yang digunakan yaitu *router* akan menjadi lebih aman.

2.4 Firewall

Firewall merupakan sistem keamanan yang melindungi komputer dari berbagai ancaman di jaringan internet yang bekerja sebagai sekat atau tembok untuk membatasi komputer di jaringan internet dan *firewall* terdapat dua macam, yaitu *firewall* berbasis *hardware* dan berbasis *software* [7]. Beberapa fungsi *firewall* diantaranya memblokir konten yang tidak diinginkan, melindungi data pribadi, memonitor *bandwith* serta mengakses VPN (*Virtual Private Network*). Sedangkan menurut jenisnya *firewall* dapat dikategorikan kedalam *firewall* perangkat lunak, perangkat keras dan berbasis *cloud* [8].

2.5 PuTTY

PuTTY merupakan aplikasi *remote access* yang berbasis *open source* yang berguna untuk mengendalikan sistem dari jarak jauh atau di tempat yang berbeda dengan memanfaatkan protokol jaringan untuk melakukan *remote* pada komputer maupun *server* dengan menampilkan *command* teks untuk menjalankan perinah tertentu [9]. Adapun fitur-fitur pada PuTTY seperti mendukung

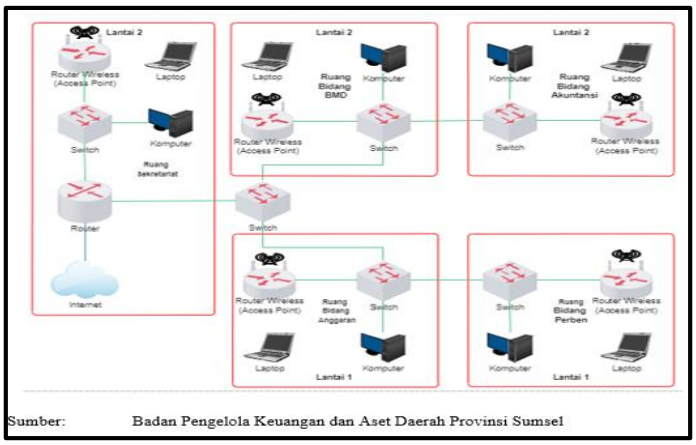
OS Windows, mendukung sistem 32-bit maupun 64-bit dan mendukung layanan *remote* (telnet, ssh, sftp, dan lainnya).

3. Metodologi Penelitian

3.1 Melakukan Diagnosa

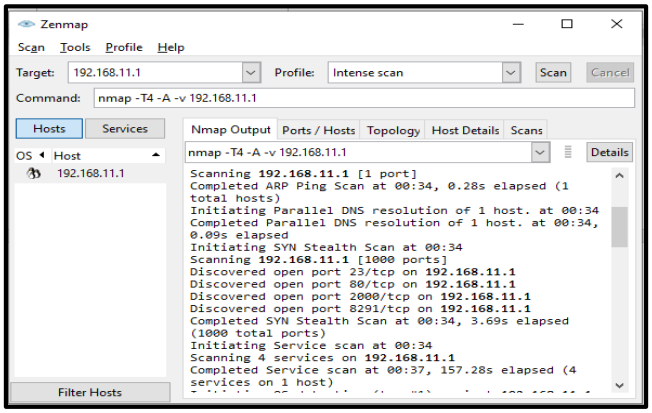
Pada tahap ini dilakukan diagnosa kebutuhan terhadap permasalahan jaringan di Badan Pengelola Keuangan dan Aset Daerah Provinsi Sumatera Selatan (BPKAD Prov Sumsel). BPKAD Prov Sumsel telah menggunakan serangkaian perangkat komputer yang terhubung ke sebuah jaringan baik lokal maupun publik yang berguna untuk bertukar data serta informasi. Adapun perangkat komputer berupa hardware seperti *router* Mikrotik, *switch* Cisco serta *router wireless* untuk menghubungkan komputer ke sebuah jaringan *Local Area Network* (LAN) maupun *Wireless Local Area Network* (WLAN) dan satu buah modem untuk terhubung ke jaringan internet.

Jaringan internet di BPKAD Prov Sumsel menggunakan layanan *Internet Service Provider* (ISP) dari Telkom. Terdapat ruangan *server* di lantai 2 gedung BPKAD Prov Sumsel bertepatan di ruangan bidang sekretariat. Di ruangan tersebut terdiri dari modem internet yang terhubung ke *router* mikrotik, lalu dihubungkan kembali melalui *switch* kemudian dikoneksikan ke *client-client* secara *wired* ataupun *wireless* melalui *access point* yang terhubung pada *switch*.



Gambar 1. Topologi Jaringan

BPKAD Prov Sumsel belum memiliki keamanan jaringan pada router mikrotik salah satunya keamanan pada layanan port (port service) untuk mengakses router tersebut. Pada saat dilakukan pengujian keamanan (Gambar 2.) dengan menggunakan aplikasi Nmap, port service pada mikrotik terlihat dalam keadaan open port. Hal ini dapat memungkinkan adanya aktifitas ilegal yang dapat merugikan BPKAD Prov Sumsel baik dari segi internal maupun eksternal.



Gambar 2. Pengecekkan Keamanan *Port Service* Mikrotik

3.2 Rencana Tindakan

Pada tahap ini penulis akan menerapkan rencana tindakan di jaringan dengan menggunakan metode *port knocking* dan *port blocking* pada router mikrotik. Alat dan perangkat lunak yang digunakan diantaranya laptop Lenovo Ideapad 110, aplikasi Winbox, aplikasi PuTTY, dan aplikasi Nmap dengan tahapan sebagai berikut:

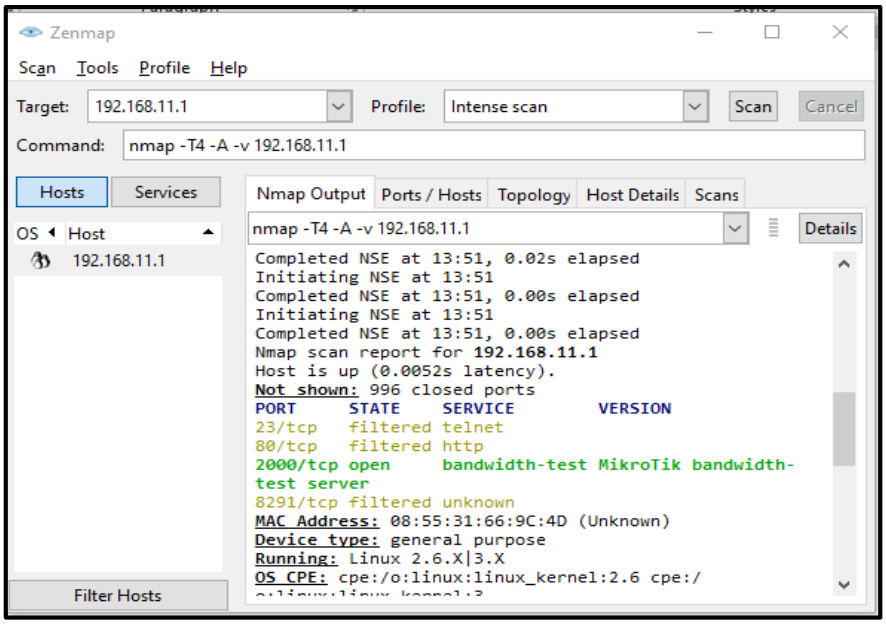
1) Menjalankan aplikasi winbox.
2) Melakukan pengecekkan *port service* (winbox, telnet dan webfig).
3) Membuat *rules* pada *firewall*.
4) Melakukan *knocking port*.
5) Melakukan *remote* pada *router* mikrotik.

4. Hasil dan Pembahasan

4.1 Hasil

4.1.1 Pengujian Scanning Port pada Router Mikrotik

Dari penerapan metode *port knocking* dan *port blocking* ketika dilakukan *scanning port* dengan target IP *router* mikrotik hasilnya adalah *service port* (winbox, telnet, dan webfig) yang status awalnya terbuka (*open port*) telah menjadi *filtered*. Melalui pemanfaatan *firewall* pada mikrotik, memungkinkan akses terhadap *port service* dapat diblok. Untuk tetap bisa mengakses ke *service port* tersebut *host* atau *administrator* jaringan perlu melakukan rangkain *knocking* pada *port* yang telah dibuat pada *filter rules* di *firewall* dengan mengirimkan paket atau koneksi melalui *protocol* tcp.



Gambar 3. *Port Service* Mikrotik Ter-*Filtered*

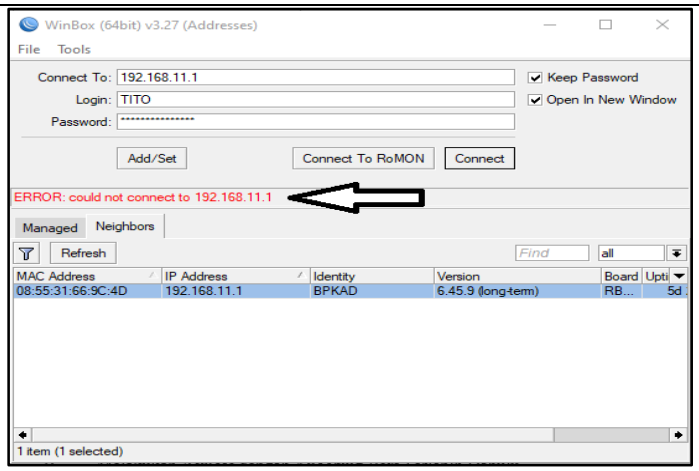
4.1.2 Hasil Pengujian *Remote* Secara Langsung

Pada tahap ini dilakukan pengujian *remote* ke *router* secara langsung melalui *service port* (winbox, telnet dan webfig) pada mikrotik yang bertujuan untuk mengetahui kemungkinan berhasil terhubung ke *router* atau tidak.

1) Melalui winbox

Dilakukan *remote* pada *router* secara langsung dengan winbox terlihat bahwa terjadi error atau tidak bisa terhubung ke *router*. Berdasarkan gambar 4. menunjukkan bahwa akses ke *router* ditolak karena belum melakukan *knocking port*.

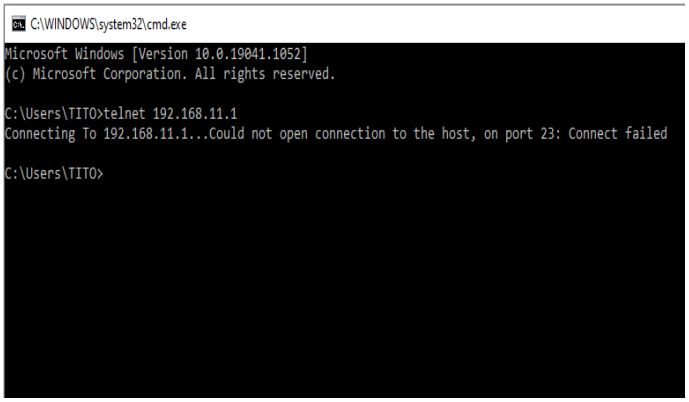
 ISSN: 2654-5438



Gambar 4. *Remote* Melalui Winbox *Error*

2) Melalui telnet

Dilakukan telnet secara langsung (tanpa *knocking* port) dengan target IP address 192.168.11.1 pada *router*. Berdasarkan gambar 5. menunjukkan bahwa koneksi gagal atau tidak dapat terhubung ke *router* dan akses ditolak.



Gambar 5. *Remote* Melalui Telnet *Error*

3) Melalui webfig

Dilakukan *remote router* secara langsung (tanpa *knocking* port) melalui webfig dengan target IP address 192.168.11.1 pada *router*. Berdasarkan gambar 6. menunjukkan bahwa *form login* yang seharusnya muncul untuk *login* dengan memasukkan *username* ataupun *password* tidak tampil.

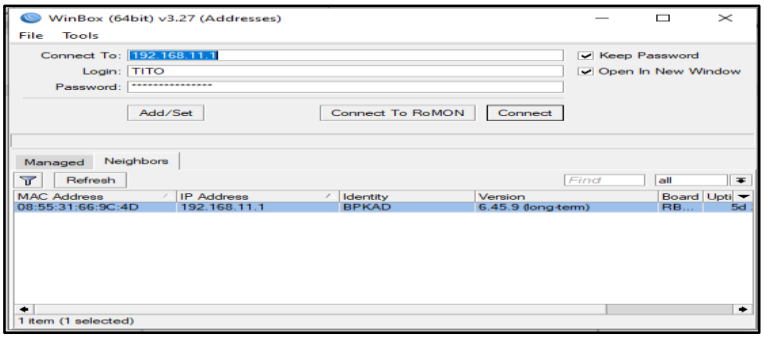
Gambar 6. *Remote* Melalui Webfig *Error*

4.1.3 Hasil Pengujian *Remote* Dengan *Knocking Port*

Pada tahap ini dilakukan pengujian *remote* ke *router* dengan melakukan *knocking port* terlebih dahulu melalui *service port* (winbox, telnet dan webfig) pada mikrotik yang bertujuan untuk mengetahui kemungkinan berhasil terhubung ke *router* atau tidak.

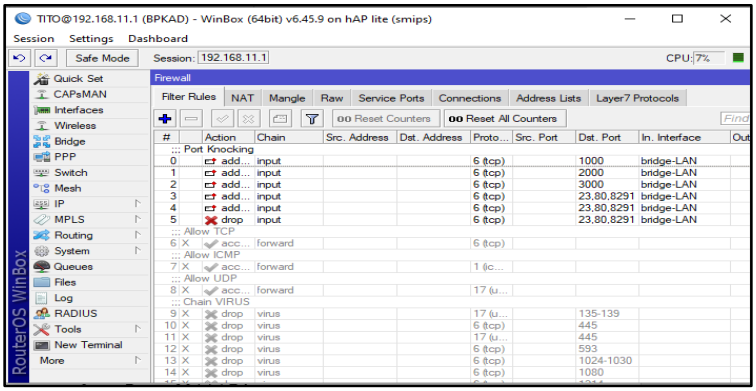
1) Melalui winbox

Dilakukan *remote* pada *router* melalui winbox dengan terlebih dahulu melakukan *knocking port (*1000, 2000, 3000) maka tampilan ketika menghubungkan (connect) ke *router* akan berbeda tidak ada pesan *error.*



Gambar 7. Tampilan *Form Login* Winbox

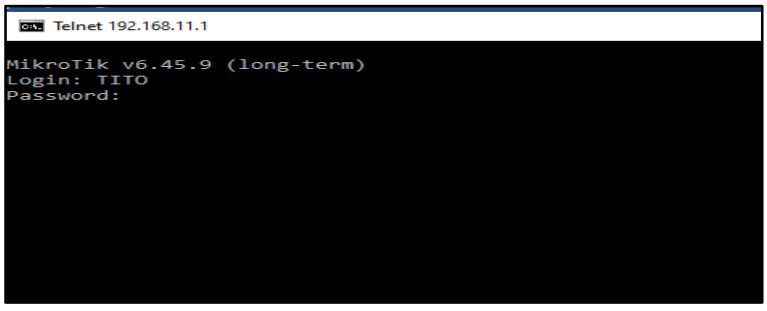
Setelah berhasil terhubung atau *login* ke *router* maka tampilan menu-menu pada winbox bisa kita lihat seperti pada gambar 8.



Gambar 8. *Remote* Melalui Winbox Berhasil

2) Melalui telnet

Dilakukan telnet pada *router* mikrotik dengan target IP address 192.168.11.1 terlihat pada gambar 9. bahwa tampilan *form login* pada telnet muncul dan dapat diisikan berupa *username* maupun *password* dari *router* tersebut.



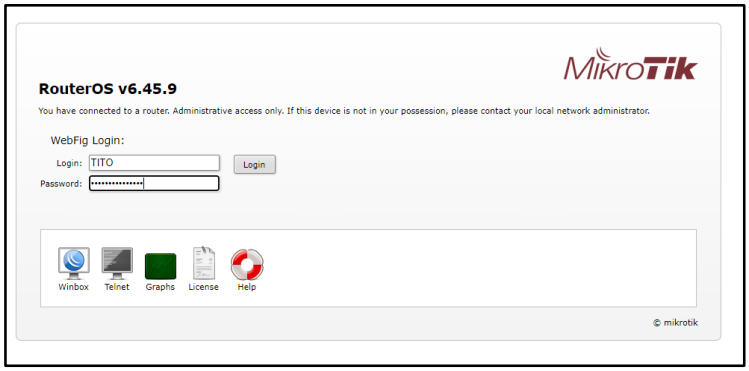
Gambar 9. Tampilan *Form Login* Telnet

Setelah mengisikan *username* maupun *password* dapat terhubung atau *login* ke router mikrotik. Apabila berhasil terhubung ke *router* akan muncul tampilan seperti pada gambar 9. *router* mikrotik dengan target IP address 192.168.11.1 terlihat pada gambar 10.

Gambar 10. *Remote* Melalui Telnet Berhasil

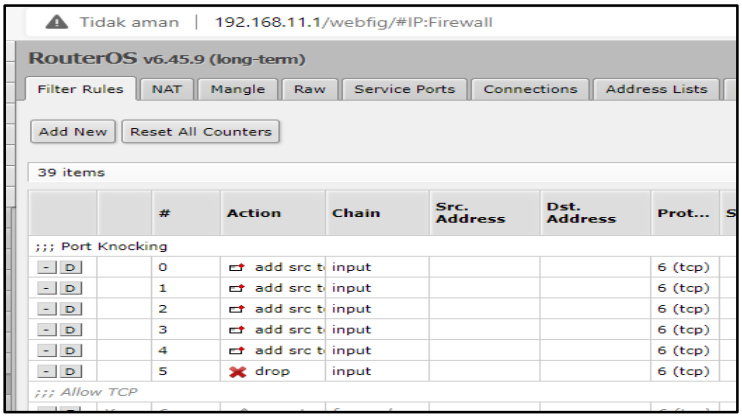
3) Melalui webfig

Dilakukan pengujian *remote router* melalui webfig dengan target IP address 192.168.11.1 terlihat pada gambar 11. *form login* muncul dan bisa diisikan *username* maupun password.



Gambar 11. *Remote* Melalui Webfig *Error*

Berdasarkan gambar 12. menunjukkan bahwa proses *remote* melalui webfig telah berhasil dilakukan serta berhasil *login* ke *router*.



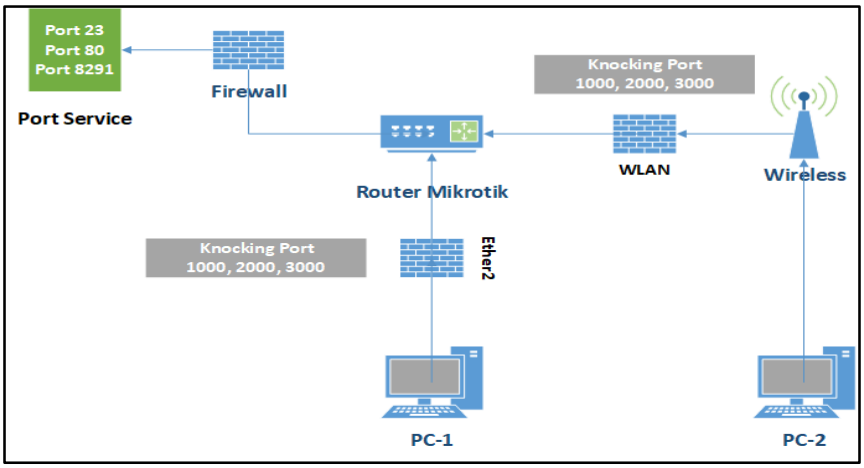
Gambar 12. *Remote* Melalui Webfig Berhasil

4.2 Pembahasan

4.2.1 Topologi Rancangan Pengujian

Adapun rancangan topologi pengujian bersifat virtualisasi dikarenakan kondisi pandemi yang tidak memungkinkan untuk penerapan langsung dilokasi penelitian yaitu BPKAD Provinsi

Sumsel. Pengujian tetap dilakukan sesuai dengan rancangan yang ingin diterapkan dilokasi penelitian sehingga tidak mengurangi kualitas data hasil pengujian.



Gambar 13. Rancangan Topologi Pengujian

4.2.2 Konfigurasi *Knocking Port*

Konfigurasi *knocking port* dilakukan dengan cara mengirimkan *packet* atau koneksi melalui *protocol* tcp. Untuk mengirimkan *packet* atau koneksi tersebut diperlukan sebuah aplikasi, dalam hal ini aplikasi yang digunakan yaitu PuTTY. Cara kerjanya hanya perlu mengisikan IP target (IP *router*) dan sejumlah *port* yang diperlukan untuk melakukan *knocking* (*port* 1000, 2000, 3000) serta dilakukan secara berurutan.

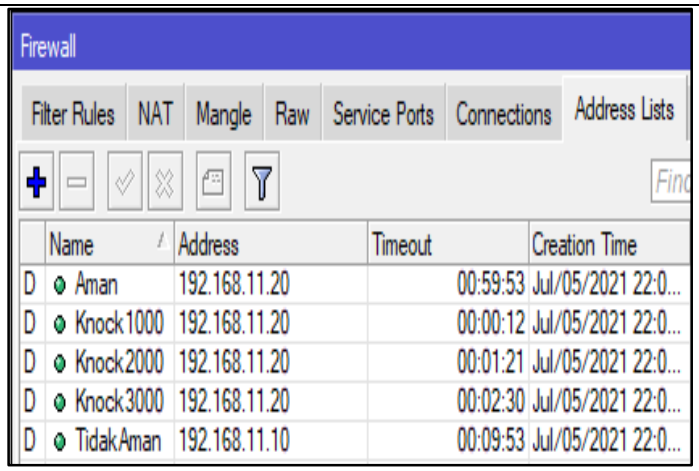
4.2.3 Perbandingan *Remote* Sebelum dan Sesudah Melakukan *Knocking*

Tabel 1. Hasil Pengujian *Remote*

No.	Pengujian	Parameter Uji	Keterangan
1	Pertama (Sebelum *Knocking)*	Akses *service port* (winbox, telnet, dan webfig)	Gagal
2		Akses ke router	Gagal
1	Kedua (Setelah *Knocking*)	*Knocking Port 1000*	Berhasil
2		*Knocking Port 2000*	Berhasil
3		*Knocking Port 3000*	Berhasil
4		Akses *service port* (winbox, telnet, dan webfig)	Berhasil
5		Akses ke *router*	Berhasil

4.2.4 Tampilan *Address Lists* Pada Firewall

Tampilan *address lists* pada *firewall* menunjukkan bahwa ketika ada yang melakukan *remote* ke *router* mikrotik akan secara otomatis terdeteksi dan dikelompokkan. *User* atau pengguna yang melakukan *remote* secara langsung atau tanpa melakukan *knocking port* terlebih dahulu akan terdaftar atau dikelompokkan pada *address list* "TidakAman". Sedangkan, *user* atau pengguna yang melakukan *remote* dengan melakukan *knocking port* terlebih dahulu akan dikelompokkan ke dalam *address list* "Aman". Hal ini tentunya akan mempermudah administrator jaringan dalam memonitoing, lebih jelas dapat dilihat pada gambar 15.



Gambar 14. Tampilan *Address Lists* Pada *Firewall*

5. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan pada jaringan BPKAD Prov Sumsel, penulis memiliki beberapa kesimpulan sebagai berikut:

1) Rules knocking yang dibuat menjadi tambahan pengamanan autentikasi untuk terhubung ke *router*.
2) *Service port* yang terbuka dapat diamankan dengan melakukan *blocking port* sehingga menjadi ter-*filtered*.
3) Metode *port knocking* dan *blocking* dapat meningkatkan keamanan sistem jaringan terutama dari akses yang ilegal.

Referensi

[1] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network", *International Arab Journal of e-Technology*, *Jurnal Sistem Teknologi dan Informasi*, Vol 1, No. 2, h. 52-59, 2009.
[2] I. Iskandar, *Belajar Port Scanning dan Sniffing*, diakses 1 April 2021, dari https://iwaniskandar.wordpress.com/2011/03/10/belajar-port-scanning-dan-sniffing/, 2011
[3] D. R. Suchendra dkk, "Penerapan sistem pengamanan port pada layanan jaringan menggunakan port knocking", *J. Lpkia, Jurnal Information Communication & Technology*, Vol. 10, No. 2, h. 2, 2017.
[4] L. Klaus, *Kenali Keamanan Jaringan*, diakses 29 April 2021, dari https://nordvpn.com/id/blog/keamanan-jaringan/, 2020.
[5] Amarudin, "Desain Keamanan Jaringan Pada Mikrotik Router OS Menggunakan Metode Port Knocking", *Jurnal Teknoinfo*, Vol. 12, No.2 h. 73, 2018.
[6] A, Saputro dkk, "Metode Demilitarized dan Port Knocking Untuk Keamanan Jaringan Komputer", *CyberSecurity dan Forensik Digital*, Vol. 3, No. 2, h. 22-27, 2020.
[7] I. Indra, *Pengertian, Cara Kerja & Pentingnya Menggunakan Firewall*, diakses 30 April 2021, dari https://www.niagahoster.co.id/blog/firewall-adalah/, 2020.
[8] L. Klaus, *Apa itu Firewall: Penjelasan Sederhana*, diakses 1 Mei 2021, dari https://nordvpn.com/id/blog/apa-itu-firewall/, 2020.
[9] Y. K, *Pengertian DDOS dan Bagaimana Menanggulanginya*, diakses 4 April 2021, dari https://www.niagahoster.co.id/blog/cara-menggunakan-putty/, 2018.