PERANCANGAN SISTEM KEAMANAN JARINGAN UNTUK MENGURANGI KEJAHATAN *CYBER* MENGGUNAKAN TEKNIK *DEMILITARIZED ZONE (DMZ)* DAN *FIREWALL RULES* (Studi Kasus: Laboratorium Basis Data IST AKPRIND)

Eka Suteja[1], Erna Kumalasari N[2], Suwanto Raharjo[3]
[1,2,3]Jurusan Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
Jl Kalisahak No. 28 Komplek Balapan Tromol Pos 45, Yogyakarta 55222 Telp : (0274) 563029
Email: Ekasuteja123@gmail.com[1], ernakumala@akprind.ac.id[2],wa2n@akprind.ac.id[3]

ABSTRACT

The concept of network security installed in one of the laboratories on The Campus of The Institut Sains & Teknologi AKPRIND *Yogyakarta, more precisely in the Database Lab. has poor network security, where data traffic on the network is not filtered so that the internal system in this case is a server device has no security apart from the built'in security system that is in the operation system. users who access the internet network using the ip address commonly used by practitioners can also enter the network used by the server directly without filters.*

Collecting data in this study using the method of observation and decision study methods. The system built in network security is using a DMZ (Demilitarized Zone) and a Firewall which is a security solution for the internal network. DMZ is an interface between the internal and external network areas. This technique works by separating data traffic from IP Public internet and IP Local to protect the server by creating a special environment in the network.

The results of this study use a dmz and firewall on server services. testing security by trying to access servers in the dmz area and using a network hack tool using Nmap (network mapper) and from the results of testing the lab database computer network can filter so that the existing server data traffic will be separated from the network used by lecturers and students, so that students can only access the specified port.

***Keywords**: DMZ (Demilitarized Zone), Firewall, port scenner.*

INTISARI

Konsep keamanan jaringan yang terpasang pada salah satu Laboratorium yang berada di Kampus Institut Sains & Teknologi AKPRIND Yogyakarta, lebih tepatnya pada Lab Basis Data. Memiliki kemanan jaringan yang kurang baik, dimana lalulintas data pada jaringan tidak terfilter sehingga sistem internal yang ada dalam hal ini adalah perangkat server tidak memiliki pengamanan selain sistem keamanan *built in* yang ada pada sistem oprasi. Pengguna yang ngakses jaringan internet menggunakan IP Address yang biasa digunakan mahasiswa praktikan dapat juga memasuki jaringan yang digunakan oleh server secara langsung tanpa *filter*.

Pengumpulan data dalam penelitian ini menggunakan metode observasi dan metode studi keputusan. Sistem yang dibangun dalam keamanan jaringan adalah menggunakan DMZ (*Demilitarized Zone*) dan Firewall yang merupakan salah satu solusi pengamanan dari jaringan internal. DMZ merupakan *interface* yang berada diantara area jaringan internal dan eksternal Teknik ini bekerja dengan memisahkan *traffic* data dengan *IP Public* internet dan *IP Local* untuk melindungi server dengan membuat lingkungan khusus dalam jaringan.

Hasil dari penelitian menggunakan DMZ dan Firewall pada layanan server. Testing terhadap keamanan dengan mencoba mengakses server yang berada pada area DMZ dan menggunakan *tools hack* jaringan menggunakan Nmap (*Network Mapper*) dan hasil testing jaringan komputer Lab Basis Data dapat melakukan *filter* sehingga lalulintas data server yang ada akan di pisah dari jaringan yang digunakan oleh dosen dan mahasiswa, sehingga server tidak terbebani.

Kata Kunci : DMZ (*Demilitarized Zone*), Firewall, *port scenner*.

PENDAHULUAN

Latar Belakang Masalah

Pengaruh teknologi informasi sangat dibutuhkan oleh semua orang untuk melakukan pekerjaan atau pembelajaran, agar pembelajaran dan pekerjaan tersebut dapat lebih mudah. Teknologi informasi ini sangat sangat penting dalam segala aspek yang terhubung dengan teknologi informasi dan teknologi. Hal ini bisa dilihat semakain banyak organisai, perusahaan, instansi pemerintah, dan instansi kampus yang menggunakan jaringan komputer untuk melancarkan arus informasi dalam aktivitas sehari-hari.

Perkembangan ini tidak lepas dari perkembangan teknologi jaringan, *software* maupun *hardware*nya. Jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain, sehingga memungkinkan pengguna untuk saling bertukar informasi berupa suara, video, gambar dan data pada jaringan yang sama, jaringan komputer memerlukan keamanan agar terhindar dari agar terhindar dari kejahatan *cyber* yang di lakukan oleh orang yang tidak bertanggung jawab yang mengakibatkan kehilangan data-data yang sangat penting.

Menurut Dwi Bayu Rendro., dkk (2020), menjelaskan tentang “Analisis Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP” (Studi Kasus di SMK Negeri 1 Kota Serang). Didapat bahwa seorang admin mampu melakukan scanning jaringan secara mudah untuk mendapatkan informasi yang ada pada jaringan. Seperti pemindai port jaringan dengan versi layanan dan mesin pendeteksi sistem operasi. User Nmap juga dapat melihat rute jaringan yang dilewati dalam mengakses sumber host target, seperti host jaringan dan host website.

Menurut Murdiyanto dkk. (2016) serangan yang paling sering digunakan adalah *Port Scanning* dan DoS. *Port Scanning* adalah serangan yang bekerja untuk mencari port yang terbuka pada suatu jaringan komputer, dari hasil *port scanning* akan didapat letak kelemahan sistem jaringan tersebut. DoS adalah serangan yang bekerja dengan mengirimkan request ke server berulang kali untuk bertujuan membuat server menjadi sangat sibuk untuk menanggapi request sehingga server akan mengalami kerusakan atau server down.

Menurut Anugrah and Rahmanto (2018), menjelaskan tentang sistem keamanan jaringan pada server dari serangan *Port Scanning* dan DoS. Salah satu teknik keamanan jaringan DMZ (*Demilitarized Zone*), yang merupakan mekanisme untuk melindungi sistem internal dari serangan hacker atau dari pihak yang tidak bertanggung jawab, dengan menggunakan filter menolak pihak-pihak yang ingin memasuki sistem tanpa hak akses.

Berdasarkan uraikan diatas maka permasalahan yang ada dapat teratasi dengan sistem DMZ dan Firewall *Rules* yang telah dikonfigurasi dalam alat jaringan Mikrotik termasuk pengamanan server. Keamanan jaringan menjadi lebih baik dibandingkan dengan konfigurasi *default.* Maka dari itu dibuat sebuah penelitian yang berjudul “Perancangan Sistem Keamanan Jaringan Untuk Mengurangi Kejahatan *Cyber* Menggunakan Metode *Demilitarized Zone* (DMZ) dan *Firewall Rulles*“.

Tujuan dalam penelitian ini adalah merancang sistem keamanan jaringan yang aman dan menerapkan beberapa metode yaitu keamanan DMZ dan *Firewall Rules*, dengan demikian diharapkan jaringan yang ada di Lab Basis Data akan lebih aman dari serangan luar. Adapun beberapa penelitian-penelitian yang sudah dilakukan terdahulu bisa dijadikan sebagai acuan serta memperoleh perbandingan-perbandingan yang sesui dengan topik yang di teliti. Beberapa penelitian yang sudah dilakukan yang terkait dengan penelitian ini adalah sebagai berikut ini. Penelitian yang dilakukan oleh M. Arifin and A. Zulius, (2019), melakukan penelitian yang berjudul “ Perancangan sistem keamanan jaringan pada Universitas Bina Insan Lubuklinggau menggunakan Teknik DMZ, Hasil dari penelitian ini Fokus membahas tentang DMZ, DMZ bekerja pada seluruh layanan dasar, pada jaringan komputer yang membutuhkan akses terhadap jaringan internet ke jaringan yang lainnya, sehingga semua port yang terbuka dan terhubung dengan internet dan akan berada pada jaringan yang berada dalam jangkauan pengelola jaringan. Pada penelitian ini tidak dijelaskan keamanan apa yang digunakan. Penelitian yang dilakukan oleh I. Anugrah, & R. Rahmanto (2018), melakukan penelitian yang berjudul “Sistem Keamanan Jaringan Local Area Network menggunakan Teknik DMZ” Hasil dari penelitian tersebut meliputi Teknik keamanan jaringan dengan DMZ dapat diimplementasikan pada sistem jaringan komputer yang berada pada universitas islam 45 dengan baik, Teknik DMZ pada layanan server jaringan LAN dapat melakukan filter terhadap serangan DOS, ICMP *flooding attack* dan UDP *flooding attack*. Pada penelitian ini hanya menjelaskan tentang serangan yang dihapai tidak menjelaskan bagaimana mengatasi serangan tersebut. Penelitian yang dilakukan oleh Muhammad Diah Maulidin, dkk (2015), melakukan Penelitian yang berjudul “Analisis dan Implementasi Metode DMZ untuk jaringan keamanan pada LPSE Kota Palembang”. Hasil dari penelitian tersebut menjelaskan

Teknik DMZ pada router Mikrotik dengan melihat hasil *scan tools Nmap* pada *web server* LPSE dan *server email.* Dan menutup celah celah keamanan diperangkat jaringan *web server* LPSE dan *server email* dengan menggunakan Nmap yang dapat memetakan jaringan (*host discovery*) dari jaringan yang diakses melalui internal maupun eksternal. Pada penelitian ini untuk keamnan jaringan hanya menggunakan Nmap saja.

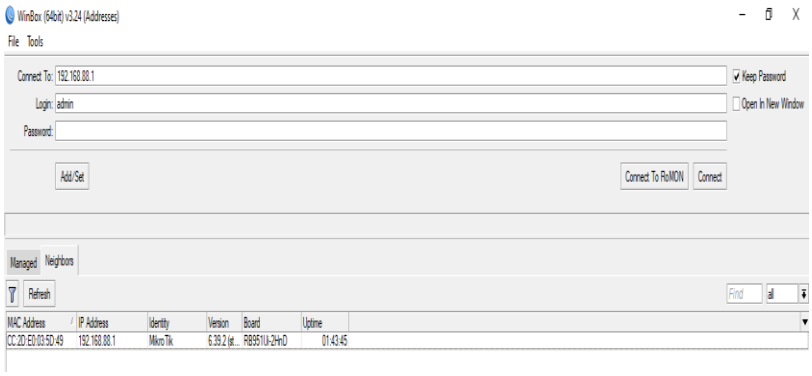
Dari tinjauan Pustaka diatas dapat disimpulkan bahwa penelitian ini digunakan untuk mekanisme Perancangan keamanan jaringan yang ada pada Lab Basis Data Kampus 3 IST AKPRIND Yogyakarta, yang menjadi pembeda dengan penelitian yang lainnya adalah penelitian ini menggunakan metode DMZ dan firawell, dengan *Screened-Subnet* yakni dengan memfilter berdasarkan *destination addres* nya serta menutup *port* yang terbuka agar terhindar dari serangan *port scenner*.

HASIL DAN PEMBAHASAN

Pembahasan

Konfigurasi Dasar

Pada tahap awal untuk masuk ke dalam *sofware* Mikrotik adalah menyamakan terlebih dahulu IP pada jaringan yang terhubung dengan internet, dengan IP yang akan di akses melalui *Winbox*, pada tahap ini digunakan untuk menghubungkan antara Mikrotik dan jaringan yang ada, jika IP pada Jaringan lokal dan pada *winbox* berbeda maka tidak akan bisa terhubung pada Mikrotik. Jika sudah menyamakan keduanya seperti yang dilihat pada gambar di dibawah dengan IP *Address* yang di dapat 192.168.88.1 dan IP tujuannya 192.168.88.1. Proses konfigurasi pada winbox dan jaringan lokal di tunjukan pada Gambar 1.

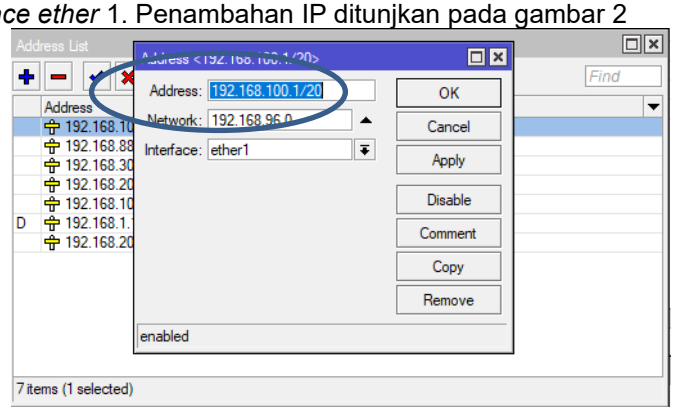


Gambar 1. konfigurasi Winbox dan jaringan lokal

Setelah konfigurasi berhasil dilakukan, maka akan menampilkan dengan jelas tampilan awal pada Mikrotik Router.

Tahap konfigurasi IP

Langkah selanjutnya dalam pembuatan sistem keamanan jaringan ini adalah dengan mengatur terlebih dahulu pengelamatan IP, yang akan digunakan untuk alamat *client*, untuk pengalamatan IP pada *device* yang digunakan untuk komputer Praktikan pada penelitian ini dikonfigurasi pada Router Mikrotik dengan IP *Address* 192.168.100.1/24 dengan *interface ether* 1. Penambahan IP ditunjkan pada gambar 2



Gambar 2. Konfigurasi IP

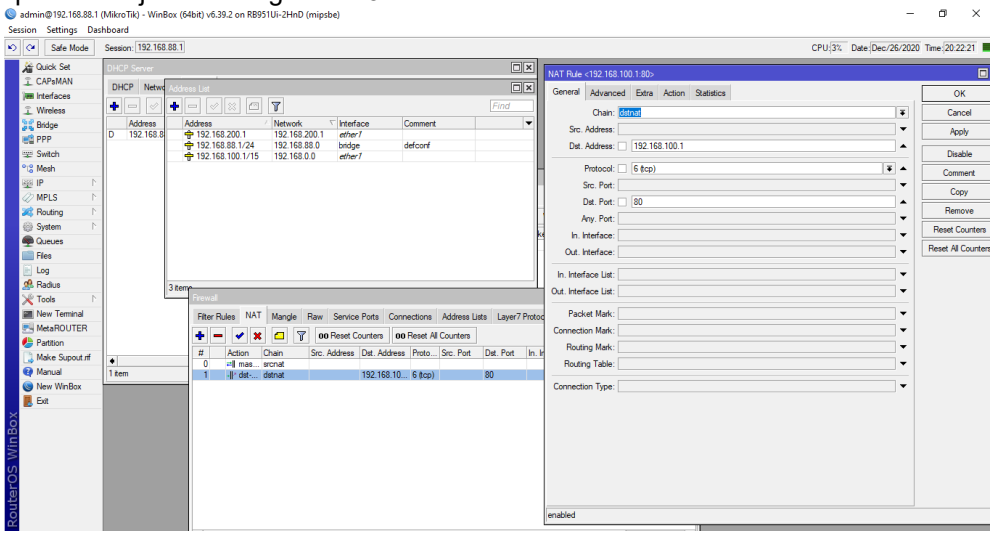
Konfigurasi DMZ (*Demilitarized Zone)*

1. Konfigurasi pada *tools* Firewall

Pada tahap awal konfigurasi pada mikrotik untuk mengaktifkan fitur Firewall yang digunakan untuk melindungi akses yang tidak diinginkan dari *public*, yaitu dengan memilih *tools* IP*, Firewall* maka akan muncul Tab baru dari Firewall dan menampilkan data.

2. Konfigurasi pada tools NAT

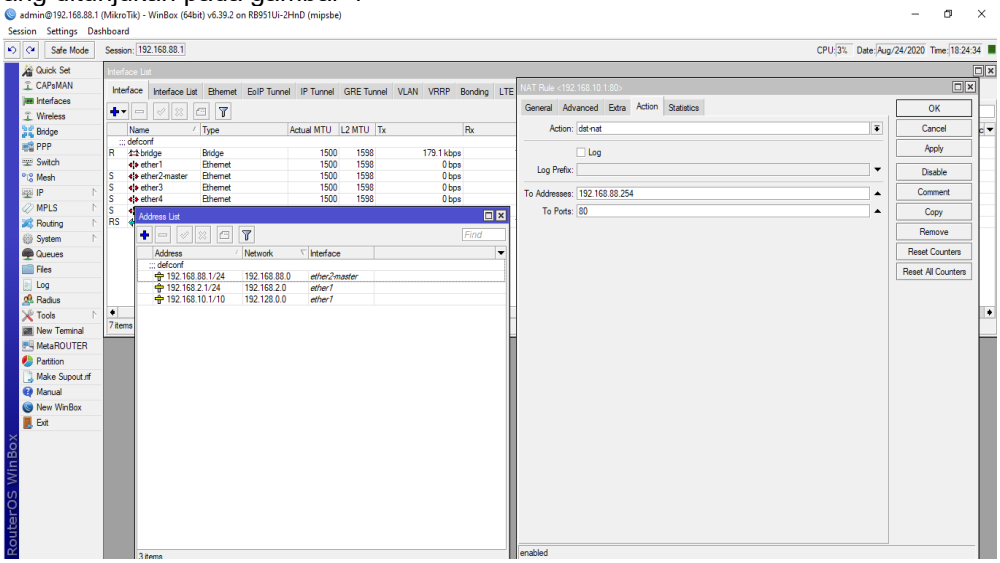
Pada tahap selanjutnya adalah dengan konfigurasi IP oleh fitur Firewall sebagai konsep dari DMZ itu sendiri, dengan cara menambahkan pada *NAT*, masuk pad tab *General* pada *Chain* di ubah dengan *dstnat*. Dan pada Dst. *Address* 192.168.100.1 adalah IP yang akan dialarang untuk mengakses server, pada protocol diubah dengan *tcp* dan *dst*. *port* 80. Seperti di tunjukan oleh gambar 3



Gambar 3. Konfigurasi Nat pada *teb General*

3. Konfigurasi pada *tools Action*

Pada konfigurasi selanjutnya adalah pengaturan pada tab *Action* yang masih di dalam tab NAT, yaitu dimana *trafik* yang akan mengakses kedalam server maka akan di alihkan ke DHCP *server* dengan IP tujuan *Address* 192.168.254, dan To *port* 80. Seperti yang ditunjukan pada gambar 4



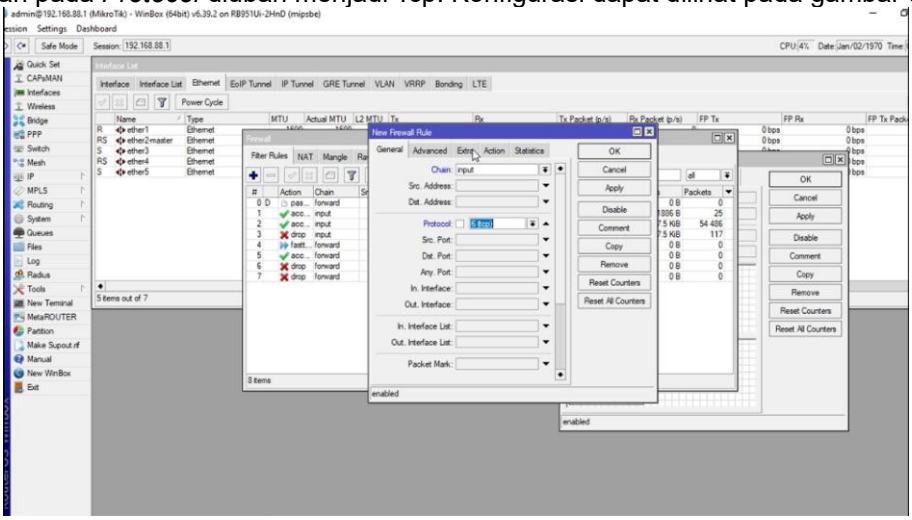
Gambar 4 Konfigurasi Nat pada *teb Action*

Konfigurasi Firewall

1. Konfigurasi pada *tools* Firewall

Dimana pada tahap ini adalah untuk menerapkan fitur PSD dimana konfigurasi ini digunakan untuk mengaktifkan rulesnya saja. Untuk mengaktifkannya fitur tersebut adapun

tahapanya adalah pada *tools* IP, Firewall, menu *filter Rules* dan pilih simbol tambah untuk menambah *rules* maka akan muncul menu baru yaitu menu *New Firewall Rules*. Pada menu ini adalah tahapan selanjutnya untuk mengaktifkan *rules* yaitu dengan mengubah *Chain* menjadi *input* dan pada *Protocol* diubah menjadi Tcp. Konfigurasi dapat dilihat pada gambar 5.

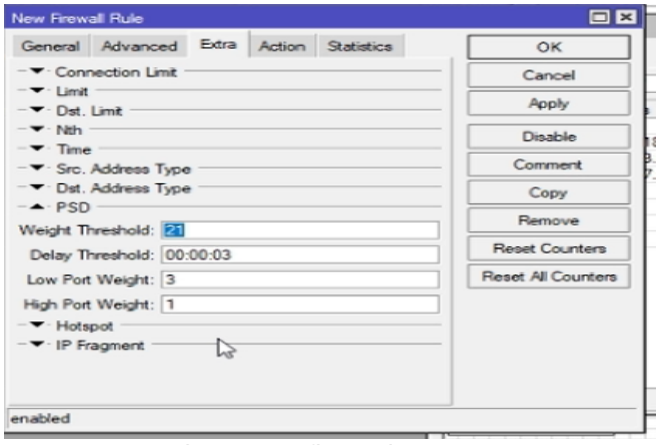


Gambar 5 Konfigurasi Tools Firewall

2. Konfigurasi pada menu Extra

Konfigurasi kedua adalah konfigurasi pada menu extra yaitu pada menu PSD itu sendiri. Berikut penjelasan pada menu PSD:

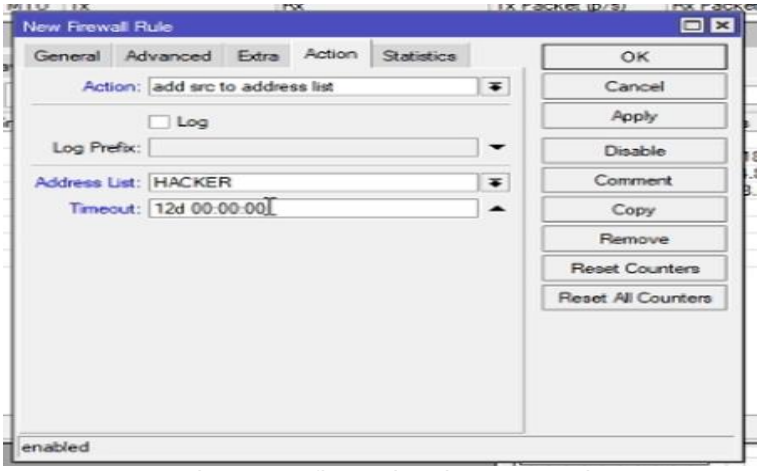
- ***Weight Threshold***: Nilai total dari '*LowPortWeight*' dan '*HighPortWeight*' untuk paket-paket TCP/UDP dengan tujuan port yang berbeda ynag berasal dari *host/Source* IP Address yang sama. Rule PSD akan berjalan ketika sudah mencapai nilai Weight Threshold ini. (Secara default nilainya adalah 21).
- ***Delay Threshold***: Merupakan nilai waktu jeda *(delay*) dari trafik/paket yang dikirimkan oleh aplikasi *port sacnner* dari sebuah *host/Source* IP *Address* yang sama dengan tujuan berbeda *port*. (Default adalah 00:00:03)
- ***Low Port Weight***: Sebuah nilai yang diberikan oleh *system* ketika terdapat trafik/paket dari *Port Scanner* yang memiliki destinasi ke *'Low Port'*. Disini yang dimaksud dari *low port* adalah port dibawah 1024 atau yang masuk dalam kategori *System/Well-Known Port*. Seperti port 80 (HTTP), 443 (HTTPS), 53 (DNS), 22 (SSH), 23 (Telnet), 110 (POP3), SMTP (25), dll.
- ***High Port Weight***: Sebuah nilai yang diberikan oleh *system* ketika terdapat trafik/paket dari *Port Scanner* yang memiliki destinasi ke *'High Port'*. Disini yang dimaksud dari *high port* adalah *port* yang diatas 1024 atau yang masuk dalam kategori *registered port* dan *dynamic/private port.* Seperti 3128 (Squid web-Proxy), 1080 (SOCKS Proxy), 1701 (L2TP), 1723 (PPTP), dll. Konfigurasi pada menu extra dapat dilihat pada gambar 6.



Gambar 6. Konfigurasi menu extra

3. Konfigurasi pada menu Action

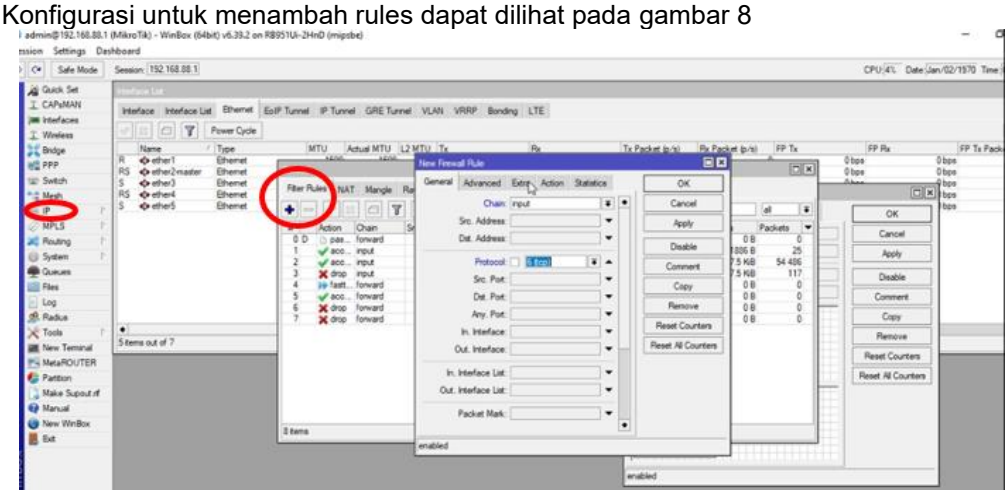
Pada tahap ketiga ini adalah tahapan konfigurasi pada menu *action* dimana pada menu ini mengubah menu *Action* menjadi add *src address list,* memberi nama pada menu *address list* (contoh Hacker) agar dapat diingat dengan baik dan terakhir adalah pada menu timeout. Konfigurasi tersebut dapat dilihat pada gamabar 7



Gambar 7 Konfigurasi pada menu Action

4. Konfigurasi menambah Rules Drop

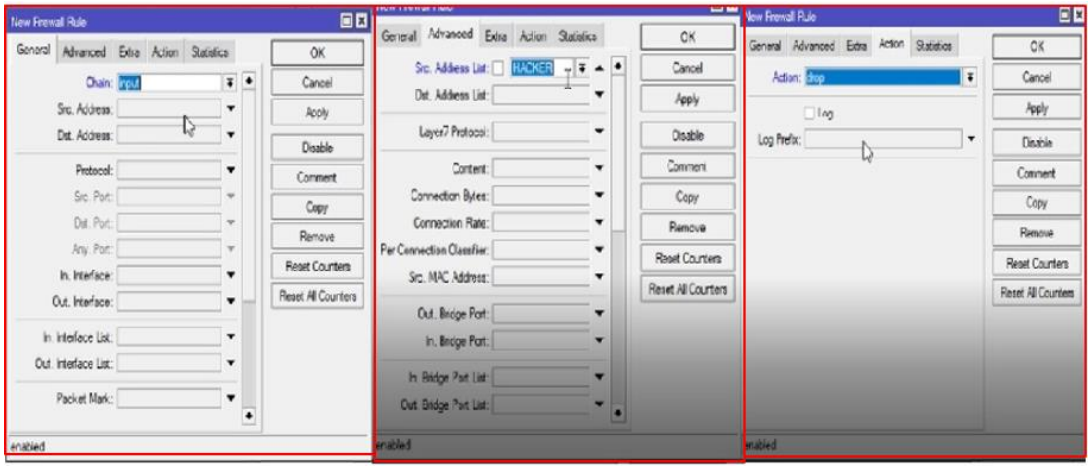
Pada pertama untuk melakukan rules drop adalah untuk melakukan *Drop* pada semua *request* yang diminta oleh pelaku *port scenner*, yaitu dengam menambah rules yaitu pada *tools* IP, Firewall, menu filter Rules lalu pilih simbol tambah untuk menambah rules. Konfigurasi untuk menambah rules dapat dilihat pada gambar 8



Gambar 8 konfigurasi menambah *rules drop*

5. Konfigurasi Rules Drop

Pada konfigurasi selanjutnya adalah untuk mengaktifkan Rules Drop untuk semua *request port scenner* pada router, untuk mengaktifkannya ada beberapa tahapan yaitu setelah melakukan konfigurasi yang pertama yaitu menuju pada menu *General* pada *Chain* di ubah nenjadi *input* lalu ok, pada menu *Advanced* pada tools *Src.address list* memasukan *address list* yang sudah kita beri nama (contoh Hacker) lalu ok, yang terakhir adalah pada menu *action* yaitu *tools action* pilih menu drop lalu oke. Konfigurasi dapat dilihat pada gambar 9



Gamabar 9 untuk mengaktifkan rules drop

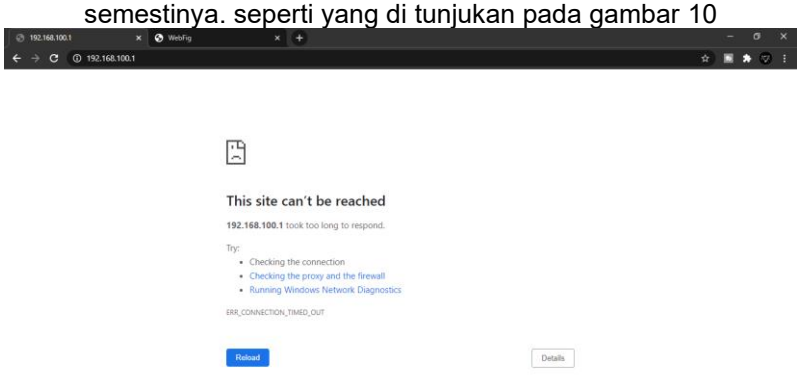
Simulasi Serangan

Pengujian sistem terhadap serangan (*penetration testing*) yang dilakukan pada sistem *server* sebelum dan sesudah installasi dan konfigurasi teknik DMZ, *penetration testing* atau pengujian terhadap serangan yang dilakukan menggunakan sistem operasi Windows 10, sebagai sistem operasi yang digunakan oleh *attacker*. Jenis serangan yang dilakukan yaitu *information gathering* dengan teknik *port scanning* dengan Nmap. Berikut adalah tahapan-tahapan yang akan dilakukan:

1. Uji Kelayakan DMZ

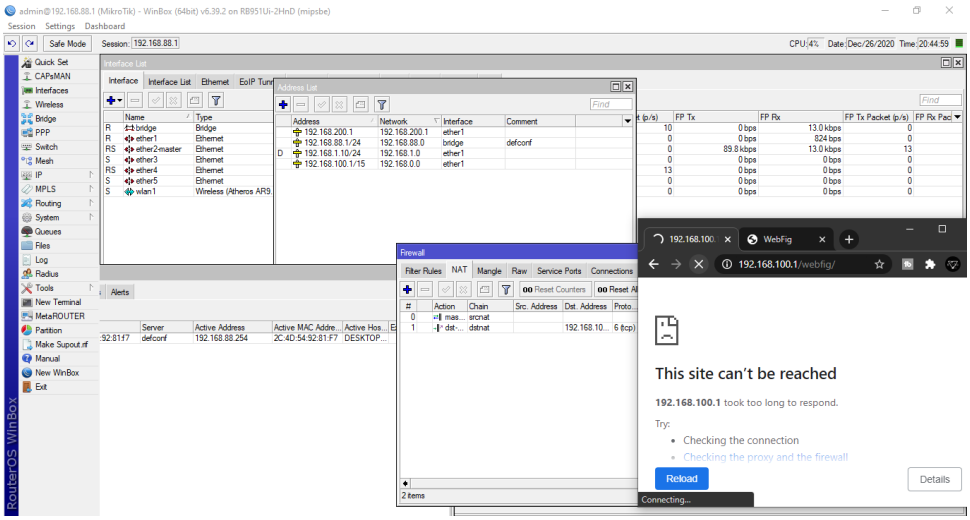
DMZ akan dikatakan layak jika *rule* yang diterapkan telah berjalan dengan semestinya. Dimana *Rule* tersebut adalah: “Jika trafik yang berasal dari komputer praktikan atau IP 192.168.100.1 menuju WEB *server* dengan protocol *tcp* dengan *Dst. Port* 80, maka *request* layanan WEB *server* akan dialihkan ke IP *address* 192.168.88.254 milik Router atau mengalihkan trafik ke server local”.

Pada pengujian pertama melakukan akses pada WEB Mikrotik Router setelah dikonfigurasi sebagai DMZ, Berdasarkan *Rule* pertama ketika di akses melalui WEB dengan IP 192.168.100.1 sebagai alamat praktikan. maka akan gagal karena *request* sudah di alihkan oleh fitur konfigurasi DMZ, maka rules yang dibuat sudah bekerja dengan semestinya. seperti yang di tunjukan pada gambar 10



Gambar 10. Setelah adanya konfigurasi DMZ

a. Pada tampilan dari Mikrotik Router yang diakses menggunkan Winbox, menampilkan beberapa tampilan seperti *Firewall* dan *interface List*, pada kedua tab ini paket *Bytes* masih berjalan, menandakan adanya paket masih terhubung dengan jaringan. Penjelasan akan di tunjukan seperti pada gambar 11



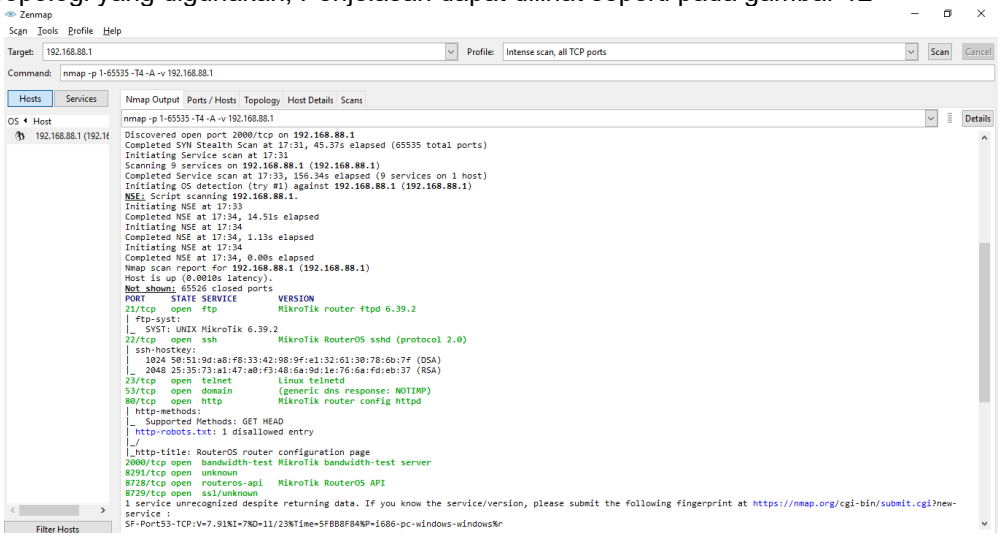
Gambar 11 Tampilan Mikrotik router

2. Pengujian Firewall Menggunakan Nmap

Firewall akan dikatakan layak jika rule yang diterapkan berjalan dengan semestinya. Diman rule tersebut adalah:" rule akan membaca *trafik* dari *port scanner* dan memberikan nilai dari port yang di-scan sesuai dengan nilai *LOW PORT* atau *HIGH PORT WEIGHT*. Setelah total *WEIGHT* mencapai nilai sesuai yang didefinisikan pada *'Weight Threshold'* maka Rule PSD akan dijalankan".

a) Pengujian Tanpa konfigurasi Firewall

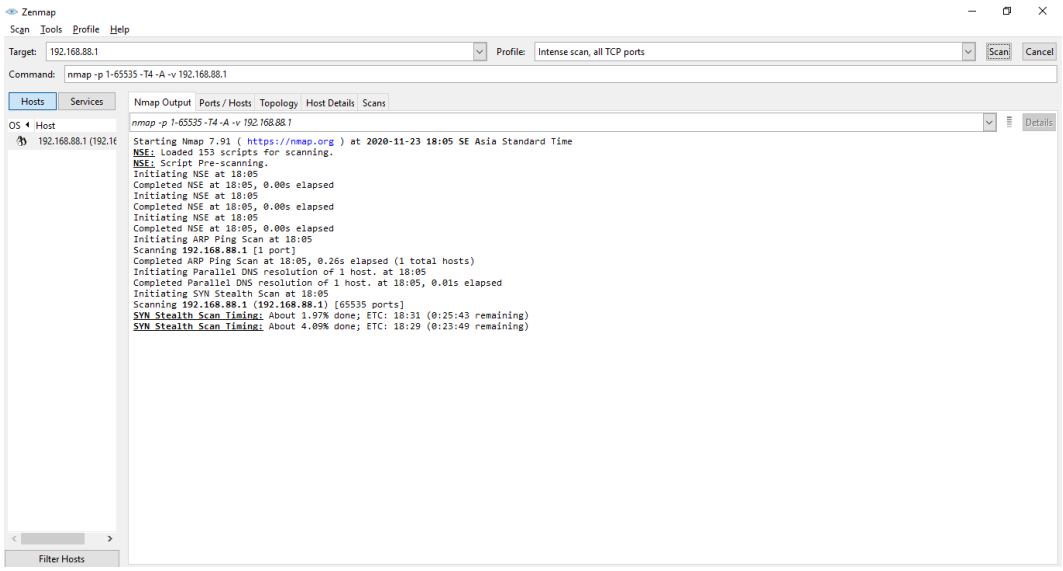
Dengan cara memasukan alamat *IP address* 192.168.88.1 dari target yang akan menjadi tujuan serangan dan menu profil diubah dengan *Intense scan, all TCP ports* setelah itu tombol *scan* dipilih, jika *Rule* Firewall belum di aktifkan maka akan menampilkan seluruh informasi penting yang ada pada Router yang di *scen* informasi status *port* yang terbuka dan *port* yang masih terbuka dalam sebuah perangkat yaitu *port* yang masih berwarna hijau. Beberapa detail informasi yang berhasil dibuka adalah *Sevice type, Sistem Oprasi* hinga Topologi yang digunakan, Penjelasan dapat dilihat seperti pada gambar 12



Gambar 12 *Port* yang terdeteksi oleh *port scanner*

b) Pengujian menggunkan konfigurasi Firewall

Pengujian kembali dengan melakukan *port scanner* dengan menggunakan nmap, pada rule Firewal yang sudah aktif maka tidak akan terlihat lagi *port* yang terbuka sehingga akan membuat para oknum yang melakukan *port scenner* tidak bisa lagi melihat celah pada jaringan. *Port* yang sudah terlindungi akan di tunjukan pada gambar 13.



Gambar 13 *port* yang sudah terlindungi dari *port scenner*

Dalam tahap ini adalah tahap analisa dimana perbandingan antara kemanan jaringan menggunakan teknik DMZ dan Firewall rules. Penjelasan selengkapnya di tunjukan pada tabel 1

Tabel 1 Perbandingan keamanan DMZ dan Firewall

No	Teknik	Keterangan	Kekurangan
1.	***Demilitarized Zone (DMZ)***	Mampu mengalihkan trafik pada server yang berada pada area DMZ, jika seorang hacker melakukan serangan dan melakukan crack pada server yang menggunakan sistem DMZ, hacker tersebut hanya akan dapat mengakses hostnya saja, tidak pada jaringan internal.	1. rentan terhdapa seranagn DoS *attac* 2. Rentan terhadap serangan *port scenner*
2.	**Firewall**	Port Scan Detection dalam jaringan untuk mencegah serangan serta memperingatkan Administrator sedini mungkin, dimana *Port Scan Detection* akan berusaha melakukan pencegahan saat penyerang masih berada dalam tahap Information Gathering atau pengumpulan informasi yang ada dalam jaringan target.	1. Tidak dapat mendeteksi ancaman serangan yang tahapannya tidak menggunakan port scanning 2. Perlu dikombinasikan dengan rule - rule lain agar rule Port Scan Detection lebih optimal.

KESIMPULAN

Setelah dilakukan penelitian, pengujian dan analisis hasil pengujian terhadap perancangan sistem keamanan jaringan untuk mengurangi kejahatan *Cyber* menggunakan teknik *Demilitarized Zone (DMZ)* Dan *Firewall Rules*, maka dapat diambil kesimpulan sebagai berikut:

1. Teknik keamanan jaringan DMZ dapat dikonfigurasi dengan baik, dimana keamanan jarinagan pada Lab Basis Data menjadi lebih baik dengan adanya konfigurasi yang tidak sama dengan konfigurasi *defoult* pada awal pembelian alat jaringan. Dimana jarinagan melakukan filter serangan dari client yang melakukan *crack* pada *Server* pelakunya hanya akan dapat mengakses server lokal saja dan bukan pada jaringan internal Lab.
2. Pada layanan Router dengan menggunakan PSD yang berada pada Firewall sitem *port scenner* tidak dapat dilakukan pencurian informasi karena PSD digunakan untuk menangkap trafik *port scenner* dengan melakukan penerapan Firewall *Rules*.

Saran untuk pengembangan sistem jaringan *Demilitarized Zone* (DMZ) dan *Firewall Rules* maka saran yang diberikan utuk penelitian selanjutnya adalah:

1. Keamana jaringan menggunakan DMZ dan Firewall rules hanya diuji coba pada skala kecil yaitu pada jaringan Lab, belum di coba pada jaringan dengan skala yang lebih besar.
2. Dapat mengkombinasikan dengan perangkat keamanan lainnya seperti IPS, IDS atau *Honeypot.*
3. Penggunaan spesifikasi hardware yang maksimal dan memaksimalkan fungsi Firewall *filteri.*

Daftar Pustaka

Anugrah, I., & Rahmanto, R. H. (2018). Sistem Keamanan Jaringan Local Area Network Menggunakan Teknik De-Militarized Zone. *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, *5*(2), 91–106. https://doi.org/10.33558/piksel.v5i2.271

Arifin, M. A. S., & Zulius, A. (2019). Perancangan Sistem Keamanan Jaringan Pada Universitas Bina Insan Lubuklinggau Menggunakan Teknik Demilitarized Zone (Dmz). *Jusikom : Jurnal Sistem Komputer Musirawas*, *4*(1), 19–24. https://doi.org/10.32767/jusikom.v4i1.443

Ariyadi, T. ((Juni 2017)). JUSIKOM Vol 2, No. 1,. *Desain Keamanan DHCP Snooping Untuk Mengurangi Serangan Local Area Network (LAN)*, Hal : 33.

Frengky Novrian1., Catur Iswahyudi & Prita Haryani (2019). *Jurnal JARKOM Vol . 7 No . 2 Desember 2019 PERANCANGAN JARINGAN KOMPUTER LOKAL MENGGUNAKAN MODEL Jurnal JARKOM Vol . 7 No . 2 Desember 2019*. *7*(2), 103–111.

Fajar Adhi Purwaningrum, Agus Purwanto & Eko Agus Darmadi. (3 November 2018 ISSN 2580-4316). OPTIMALISASI JARINGAN MENGGUNAKAN FIREWALL. *Jurnal IKRA-ITH Informatika* , 18-19.

Inawa, S. (2015, Mei 3). *Perancangan Jaringan Komputer Menggunakan Metode PPDIOO*. Retrieved from www.Wordpress.Com: Https://Sofyaninawan.Wordpress.Com

Jostein, A. A., Najoan, M. E. I., & Manembu, P. D. K. (2015). Perancangan Routing Protocol di Jaringan PT. Kawanua Internetindo. *E-Journal Teknik Elektro Dan Komputer*, *4*(4), 23–28. https://ejournal.unsrat.ac.id/index.php/elekdankom/article/download/8568/8141

Munandar, A., Ulinuha, A., & Gunawan, M. T. D. (2015). *PERANCANGAN DAN IMPLEMENTASI JARINGAN KOMPUTER DENGAN STUDI KASUS DI SMK MUHAMMADIYAH 2 SRAGEN Makalah Program Studi Informatika Fakultas Komunikasi dan Informatika Diajukan oleh*.