SISTEM KEAMANAN JARINGAN *LOCAL AREA NETWORK* MENGGUNAKAN TEKNIK *DE-MILITARIZED ZONE*

Ino Anugrah, R.Hengki Rahmanto
Program Studi Teknik Komputer Universitas Islam "45"
Jl. Cut Meutia No.83 Bekasi
Email : inoxyz333@gmail.com

ABSTRACT

Islamic University"45" computer network needs a safe network to strengthen the network security systems to protect servers from attacks such as Port Scanning and DoS attack (Denial of Service). One of the network security techniques is De-Militarized Zone (DMZ) that is a mechanism to protect the internal system from hacker attacks or other parties who want to enter the system with no access. The purpose of this Project is to implement LAN network security system using De-Militarized Zone (DMZ) technique, with a single firewall that supports the internal and external networks. The results of the DMZ technique implementation at the Islamic University's "45", it is found that filter DoS attack can be implemented well. Data analysis results show DoS attack with the type of ICMP Flooding attack, and UDP Flooding attack can be blocked with Percentage of success is 98%.

Keywords : *attack, network security, de-militarized zone*

ABSTRAK

Jaringan komputer Universitas Islam "45" memerlukan keamanan jaringan untuk dapat memperkuat sistem keamanan jaringan pada *server* dari serangan seperti *Port Scanning* dan DoS *(Denial of Service).* Salah satu teknik keamanan jaringan yaitu *De-Militarized Zone* (DMZ) yang merupakan mekanisme untuk melindungi sistem *internal* dari serangan *hacker* atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. Tujuan Tugas Akhir ini adalah untuk mengimplementasikan sistem keamanan jaringan LAN menggunakan teknik *De-Militarized Zone* (DMZ). metode dasar adalah dengan menggunakan *firewall* tunggal yang menjadi penyangga jaringan *internal* dan *external*. Hasil penelitian implementasi teknik DMZ pada layanan *server* jaringan komputer Universitas Islam "45" dapat melakukan *filter* DoS *attack* dengan baik, data hasil analisa menunjukan DoS *attack* dengan jenis ICMP *Flooding attack,* dan UDP *Flooding attack* dapat di-*block* dengan Persentase keberhasilan sebesar 98%.

Kata kunci *:* Serangan, Keamanan jaringan*, De-Militarized Zone*

1. Pendahuluan

Keamanan jaringan sangat vital bagi sebuah jaringan komputer. kelemahan-kelemahan yang terdapat pada jaringan komputer jika tidak dilindungi dan dijaga dengan baik akan menyebabkan kerugian berupa kehilangan data, kerusakan sistem *server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset-aset berharga institusi.(Ikhwan,2014). Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan meskipun terkadang beberapa organisasi lebih mendahulukan tampilan dan lain sebagainya dibandingkan masalah keamanannya, dan ketika sistem mendapat serangan dan terjadi kerusakan sistem, masalah dan kerugiannya akan lebih besar untuk melakukan perbaikan sistem. Maka sudah selayaknya keamanan jaringan harus lebih diperhatikan untuk melindungi sistem dari ancaman serangan yang semakin canggih dan beragam, terlebih lagi ketika jaringan *local* sudah terhubung ke *internet* maka ancaman keamanan jaringan akan

semakin meningkat. misalnya DDoS *attack* dan sebagainya, juga serangan *hacker, virus, trojan* yang semuanya merupakan ancaman yang tidak bisa diabaikan. (Wijaya,.dkk,2014)

Serangan yang paling sering digunakan adalah *Port Scanning* dan DoS *(Denial Of Service). 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 komputer tersebut. DoS adalah serangan yang bekerja dengan cara mengirimkan *request* ke *server* berulang kali untuk bertujuan membuat *server* menjadi sibuk menanggapi *request* dan *server* akan mengalami kerusakan atau *hang* (Mardiyanto,.dkk, 2016)

De-Militarized Zone (DMZ) merupakan mekanisme untuk melindungi sistem *internal* dari serangan *hacker* atau pihak-pihak lain yang ingin memasuki sistem tanpa mempunyai hak akses. DMZ terdiri dari semua *port* terbuka, yang dapat dilihat oleh pihak luar sehingga jika *hacker* menyerang dan melakukan *cracking* pada *server* yang mempunyai DMZ, maka *hacker* tersebut hanya dapat mengakses *host* yang berada pada DMZ dan tidak pada jaringan *internal*. Selain itu dengan melakukan pemotongan jalur komunikasi pada jaringan *internal*, *virus, trojan* dan sejenisnya sehingga tidak dapat lagi memasuki jaringan.(K Juman,2003). Untuk itu diperlukan teknik keamanan jaringan yang dapat menangkal ancaman serangan tersebut atau meminimalisir ancaman serangan yang bisa memasuki sistem jaringan. Dalam penelitian ini dilakukan implemetasi teknik DMZ pada system keamanan jaringan lokal di Universitas Islam 45 (Unisma) Bekasi.

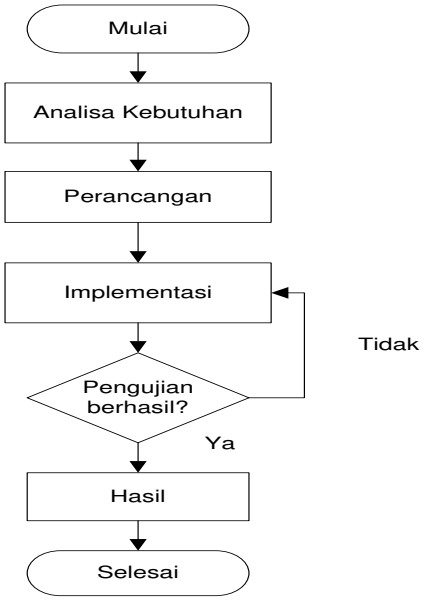
2. Bahan dan Metode Penelitian

2.1 Bahan

Untuk kebutuhan perangkat keras dan perangkat lunak yang digunakan dalam penelitian ini disajikan dalam Tabel 1 dan Tabel 2 sebagai berikut :

2.2 Metode Penelitian

Penelitian ini dilakukan dalam beberapa tahap seperti pada gambar 1.



Gambar 1. Tahapan Penelitian

1) Analisa Kebutuhan

   Tahap ini merupakan identifikasi masalah dari sistem keamanan jaringan di Unisma. Dari masalah yang ada kemudian diselesaikan dengan implementasi metode DMZ pada jaringan local.

2) Perancangan

   Dalam tahap perancangan dilakukan penentuan topologi dan konfigurasi jaringan.

Tabel 1 Spesifikasi *Hardware*

No	Perangkat	Jumlah	Spesifikasi Unit
1.	Mikrotik RB750GL	1	CPU : AR7242 400 Mhz RAM : 64 MB Main Storage : 64 MB LAN Ports : 5 Ports Dimensions : 113x89x28mm RouterOS License : Level4
2.	PC Local Client	1	Laptop Asus x450cc CPU : Intel R Pentium R Memory RAM : 2 GB Main Storage : 500 GB
3.	PC Server	1	CPU : Intel Pentium 4 Memory RAM : 1 GB Main Storage : 40 GB

Tabel 2 Spesifikas *Software*

No	Software	Keterangan
1.	Microsoft Windows 10 Pro	Sistem Operasi untuk *Admin* pada Laptop untuk keperluan konfigurasi
2.	Kali Linux Sana 2.0	Sistem Operasi untuk *Admin* pada Laptop untuk keperluan konfigurasi dan *Monitoring* sistem dan *penetration testing* sistem
3.	MikroTik RouterOS 5.16	Sistem Operasi pada Mikrotik RB750GL
4.	Ubuntu 16.10 *server* i386	Sistem Operasi pada *server*

3) Implementasi

Tahap implementasi merupakan tahap yang melakukan setting layanan DMZ pada server.

4) Pengujian

Tahap pengujian dilakukan untuk mengetahui sejauh mana implementasi dilakukan. Dalam penelitian dilakukan 2 pengujian yaitu pengujian tanpa menggunakan DMZ dan pengujian dengan menggunakan DMZ.

3. Hasil dan Pembahasan

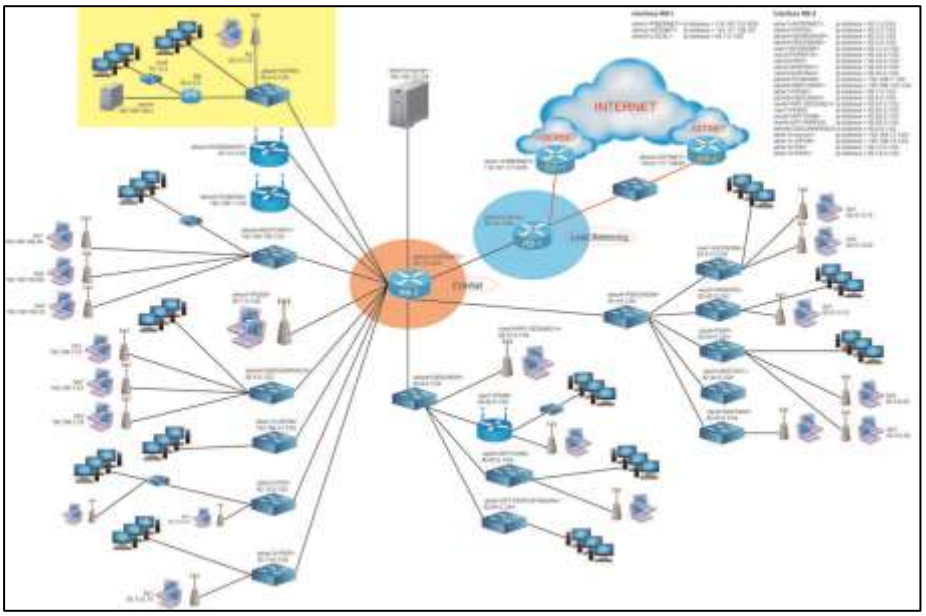
3.1 Hasil

1) Analisa kebutuhan

Keamanan jaringan dan komputer yang ada di Unisma masih rendah dan sangat rentan terhadap ancaman. Keamanan jaringan yang ada hanya menggunakan *filter firewall default* yaitu semua layanan *server* langsung berhadapan dengan *client*, sehingga jika terjadi serangan *hacker* atau pihak luar maka serangan itu akan langsung mengarah ke *server* dan besar kemungkinan *server* akan mengalami kerusakan sistem.

Jenis serangan pada *server* dan *router* yang paling sering digunakan adalah *Port Scanning* dan DoS *attack. 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 komputer tersebut dan biasanya dilanjutkan dengan serangan lainnya seperti DoS atau dengan DDoS. *M*etode serangan DoS yang sering dilakukan oleh *attackers* yaitu *Ping of Death* atau ICMP *Flooding Attack,* UDP *Flooding Attack, Syn Flooding Attack.* Oleh karena itu perlu penyelesaian untuk mengatasi keamanan jaringan di Unisma dengan menerapkan metode DMZ. Topologi

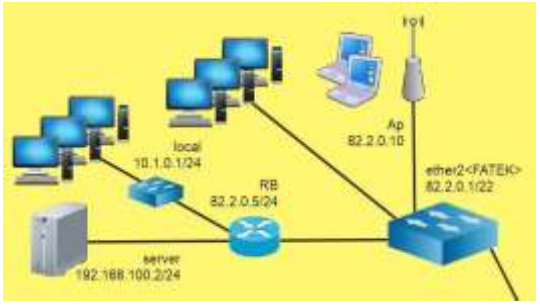
jaringan komputer di Unisma seperti dalam gambar 2.



Gambar 2. Topologi Jaringan Universitas Islam "45"

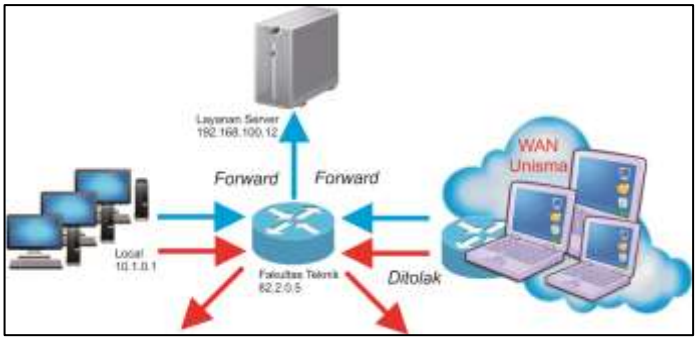
2) Perancangan

Topologi jaringan di Unisma dengan menggunakan metode DMZ seperti dalam gambar 3.



Gambar 3. Implementasi Topologi Jaringan DMZ

DMZ berfungsi memindahkan semua layanan suatu jaringan ke jaringan lain yang berbeda dan memindahkan *services* (layanan) pada *server* yang berada pada zona jaringan *internal* agar dapat diakses dari jaringan luar. Dengan demikian *server* tidak berhadapan langsung dengan jaringan luar *(external).* Dengan adanya DMZ maka serangan ke sistem *internal* tersebut lebih dapat dicegah ataupun dilindungi. Installasi dan konfigurasi DMZ dilakukan pada RouterBoard Mikrotik RB750GL dan akan menjadi router *firewall* yang melakukan *filter* ke semua akses *request* layanan *server.* Pada Gambar 4 merupakan *traffic* paket *request* dari *hosts client* yang mencoba mengakses layanan pada *server* DMZ.

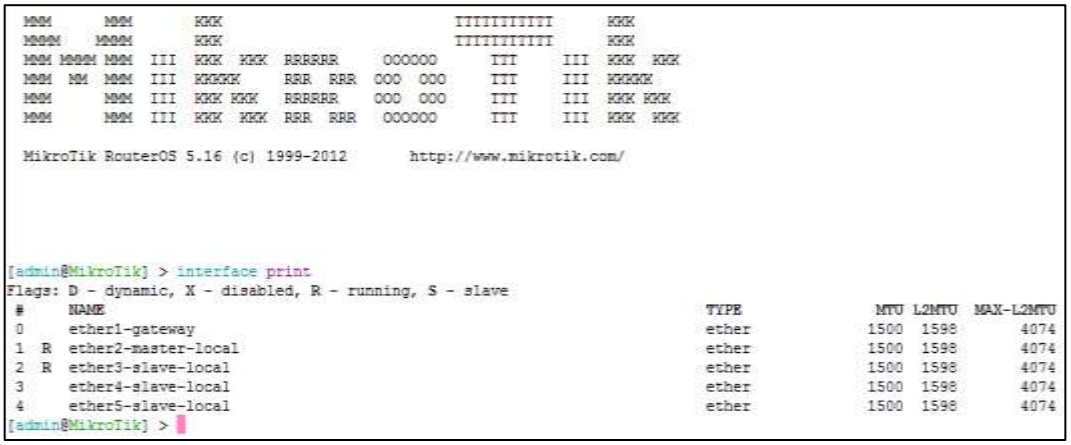


Gambar 4 Simulasi *Traffic* DMZ

RouterBoard Mikrotik atau router *firewall* berada diatas *server* yang nantinya akses ke arah *server* dari arah luar jaringan diarahkan melalui *IP address* router *firewall* kemudian diteruskan *(forward)* ke layanan DMZ yang berada pada *server* dengan *network address translation* (NAT) dan *port address translation* (PAT).

Tahapan installasi dan konfigurasi yang pertama kali dilakukan yaitu mempersiapkan RouterBoard Mikrotik RB750GL dengan melakukan *reset* sistem dan *Remove Configuration* dengan konfigurasi *default*. Konfigurasi *default* ini sudah lengkap sehingga RouterBouard dapat langsung diimplementasikan ke dalam jaringan. Konfigurasi memungkinkan beberapa komputer *user* mengakses *internet* melalui RouterBoard dan telah memasangkan *IP address* 192.168.88.1/24 pada *interface ether2*. Jika RouterBoard yang digunakan bukan merupakan router yang baru atau router yang pernah digunakan maka sebaiknya melakukan prosedur *reset*. Prosedur *reset* ini akan mengembalikan konfigurasi router menjadi konfigurasi *default* dan melakukan *Remove Configuration*.

Setelah melakukan prosedur *reset* sistem dan *Remove Configuration* pada sistem Mikrotik selanjutnya dapat membuat installasi dan konfigurasi sistem yang telah direncanakan. Installasi dan konfigurasi sistem dapat dilakukan dengan *terminal* seperti pada Gambar 5 yang merupakan tampilan *default* halaman *login* mikrotik dari menu *New Terminal* pada Winbox dan perintah *interface print.*



Gambar 5. *Login* Mikrotik RB750GL

Tahap berikutnya adalah memberikan nama *interface* dan konfigurasi *IP address* pada *interface*. Ether1 untuk akses *internet name interface* = ether1<INTERNET>, ether2 ke *server* DMZ *name interface* = ether2<SERVER>, ether3 untuk akses ke jaringan *local name interface* = ether3<LOCAL>.

Perintah-perintah yang dimasukan sebagai berikut :

interface set 2 name=ether1<INTERNET>

interface set 3 name=ether2<SERVER>

interface set 4 name=ether3<LOCAL>

Pada Gambar 6 merupakan hasil konfigurasi *interface print.*

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                                                                TYPE
 0  R  ether1<INTERNET>                                                   ether
 1  R  ether2<SERVER>                                                     ether
 2  R  ether3<LOCAL>                                                      ether
 3     ether4                                                             ether
 4     ether5                                                             ether
[admin@MikroTik] >
```

Gambar 6. Hasil Konfigurasi *Interface*

Selanjutnya melakukan kofigurasi *IP address* pada masing-masing *interface. Interface* ether1<INTERNET> dengan *IP address* 82.2.0.5/24 yang mengarah keluar jaringan *(external)*, *interface* ether2<SERVER> dengan *IP address* 192.168.100.1/24 mengarah ke *server*, dan *interface* ether3<LOCAL> dengan *IP address* 10.1.0.1/24 mengarah ke jaringan *local*.

Perintah-perintah yang dimasukan seperti berikut :

ip address add address=82.2.0.5/24 interface=ether1<INTERNET>

ip address add address=192.168.100.1/24 interface=ether2<SERVER>

ip address add address=10.1.0.124 interface=ether3<LOCAL>

Berikut pada Gambar 7 merupakan hasil konfigurasi *IP address print.*

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
 #   ADDRESS            NETWORK         INTERFACE
 0   82.2.0.5/24        82.2.0.0        ether1<INTERNET>
 1   192.168.100.1/24   192.168.100.0   ether2<SERVER>
 2   10.1.0.1/24        10.1.0.0        ether3<LOCAL>
[admin@MikroTik] >
```

Gambar 7. Hasil Konfigurasi *IP Address*

Setelah melakukan konfigurasi *interface* dan *IP address* pada tahapan selanjutnya akan dilakukan konfigurasi *routing* DMZ untuk melakukan *forward* dari router *firewall* Mikrotik *ke server.* Dengan cara ini layanan pada *server* akan menjadi area DMZ yang berada pada *interface* ether1<INTERNET> dengan *address* 82.2.0.5 yang merupakan *interface* yang menghubungkan jaringan *internal* dan *external* agar semua pihak dapat melakukan akses ke *server* pada *IP address* 192.168.100.2. Konfigurasi dilakukan pada fitur mikrotik *firewall* NAT, berikut perintah kofigurasi *IP firewall* NAT pada terminal mikrotik.

- Kofigurasi *forward* ke WEB *Server* DMZ

  ip firewall nat add comment="Forward http web server" action=dst-nat chain=dstnat protocol=tcp dst-port=80 to-port=80 dst-address=82.2.0.5 to-address=192.168.100.2
- Konfigurasi *forward* ke FTP *Server* DMZ
- *ip firewall nat add comment="Forward FTP server" action=dst-nat chain=dstnat protocol=tcp dst-port=21 to-port=21 dst-address=82.2.0.5 to-address=192.168.100.2*

Berikut pada Gambar 8 merupakan hasil *IP firewall nat print* yaitu *forward* WEB *server* dan FTP *server.*

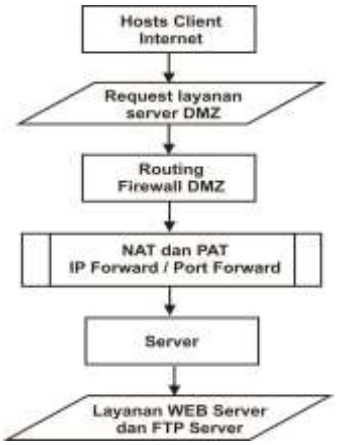
```
[admin@MikroTik] > ip firewall nat print
Flags: X - disabled, I - invalid, D - dynamic
 0   ;;; Forward http web server
     chain=dstnat action=dst-nat to-addresses=192.168.100.2 to-ports=80 protocol=tcp dst-address=82.2.0.5 dst-port=80

 1   ;;; Forward FTP server
     chain=dstnat action=dst-nat to-addresses=192.168.100.2 to-ports=21 protocol=tcp dst-address=82.2.0.5 dst-port=21
[admin@MikroTik] >
```

Gambar 8. Hasil Konfigurasi *IP Firewall NAT Print*

Kedua kofigurasi tersebut akan melakukan *filtering* ke semua akses paket data dan *request* ke *server*. Semua akses *host client* yang masuk melalui *ether1<INTERNET>* akan diproses di router *firewall*. Jika *request* paket merupakan akses ke layanan DMZ maka sistem akan melakukan *forward* penerusan paket dengan memanfaatkan NAT dan PAT yaitu paket *request host client* yang melakukan *request* layanan pada *port=80* dan *port=21* untuk menggunakan layanan WEB *server* dan FTP *server* melalui *ether1<INTERNET>* pada *IP address=82.2.0.5* akan diteruskan ke *IP address server* pada *IP address=192.168.100.2 port=80* untuk WEB *server* dan *port=21* untuk FTP *server*.

3) Implementasi

Pada Gambar 9 merupakan alur proses paket *request* dari *hosts client* yang mencoba mengakses layanan pada *server* DMZ.



Gambar 9. Alur Proses DMZ

Dalam alur proses DMZ akan memproses semua data *request client* yang melakukan akses menuju *server.*Sistem akan melakukan *filter* dan membuat *rule* (aturan) pada paket *request* berdasarkan layanan apa yang diminta kemudian pada proses *routing firewall* sistem akan menentukan jenis *request* paket mana yang diperbolehkan mengakses layanan *server* atau tidak. Jika *request* yang diminta merupakan layanan yang dikonfigurasikan sebagai DMZ maka akan diteruskan ke *server*. Terakhir menentukan *address* dan *port address* berdasarkan jalur yang telah dibuat dan ditentukan dari *IP address* router *firewall* yang kemudian diteruskan *(forward)* dan diterjemahkan *(translation)* oleh NAT dan PAT ke *server* DMZ.

4) Pengujian

Pengujian jaringan yang dilakukan dibagi dalam dua tahapan, pertama pengujian *server* tanpa DMZ yaitu pengujian jaringan pada saat sistem *server* belum menerapkan teknik DMZ, dan pengujian *server* DMZ yaitu pengujian jaringan pada saat sistem *server* sudah menerapkan teknik DMZ.

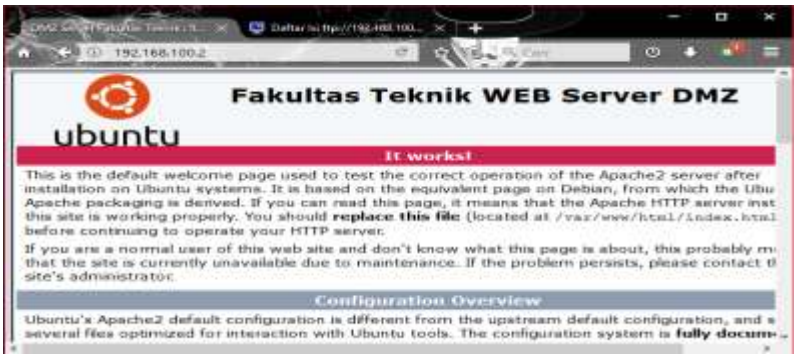
a. Pengujian *Server* tanpa DMZ

Pertama melakukan pengujian layanan WEB *server* dan FTP *server* sebelum menerapkan teknik DMZ. Sebelum

menerapkan teknik *De-Militarized Zone*, layanan *server* tidak dapat diakses dari luar jaringan *external* hanya dapat digunakan di jaringan *internal* saja dan diakses langsung ke *IP address* milik *server* 192.168.100.2 atau dengan kata lain *server* akan berhadapan langsung dengan *request host client*, dalam keadaan ini keamanan jaringan komputer sistem *server* akan sangat beresiko terhadap serangan *hacker* / atau pihak lain.

Pada Gambar 10 merupakan pengujian akses *request* pada layanan WEB *server* sebelum menerapkan teknik DMZ.

Pada Gambar 11 merupakan pengujian akses *request* pada layanan FTP *server* sebelum menerapkan teknik DMZ.



Gambar 10. *Request* Layanan WEB *Server*

Gambar 11. *Request* Layanan FTP *Server*

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 Kali Linux sana 2.0 sebagai sistem operasi yang digunakan oleh *attacker*. Jenis serangan yang dilakukan yaitu *information gathering* dengan teknik *port scanning* dengan Nmap dan *stress testing* dengan teknik *Denial of Service* (DoS) dengan Hping3 dan kedua *tools* tersebut telah ter-*install* secara *default* dalam sistem operasi Kali Linux sana 2.0 sebagai sistem operasi *penetration testing* yang digunakan.

Sebagai tahap awal pengujian serangan terhadap sistem yang dilakukan pertama kali oleh *attacker / hacker* adalah *information gathering* yaitu melakukan pencarian dan pengumpulan informasi pada *target* untuk mencari celah yang terbuka untuk disusupi, *information gathering* atau pencarian informasi yang dilakukan

menggunakan teknik *port scanning* dengan menggunakan *tool* Nmap *(Network Mapping)*. Nmap digunakan untuk mencari informasi *port* yang terbuka dalam sebuah jaringan. Nmap didisain khusus untuk melakukan *ping* menuju *port-port* yang terbuka dan kembali lagi kepada *attacker / hacker* dengan membawa informasi.

Dengan memanfaatkan data informasi dari *port scanning* yang telah ditemukan maka *hacker* dapat menemukan celah keamanan dan melakukan serangan *hacking* atau bahkan mengambil alih sistem *server.* Apabila *server* berhadapan langsung dengan hal ini sistem *server* akan sulit untuk bertahan dari serangan keamanan tersebut. Setelah mengetahui celah dari *port* yang terbuka selanjutnya dilakukan pengujian serangan *stress testing* menggunakan teknik DoS untuk menyerang *target* dengan cara membanjiri *resource* (sumber daya) dari sebuah layanan *server* menggunakan *tool* Hping3.

Serangan DoS dilakukan sebanyak tiga kali dengan jenis serangan DoS *Ping of Death* / ICMP *Flooding Attack,* UDP *Flooding Attack,* dan Syn *Flooding Attack* dan semua serangan DoS tersebut diarahkan pada *port 80* yang merupakan *port* untuk mengakses layanan WEB *server*. Hal tersebut dimaksudkan untuk menyerang layanan WEB *server* pada *port 80* agar layanan WEB *server* menjadi *down*.

Analisa hasil pengujian *server* tanpa DMZ yang dilakukan yaitu berupa data monitoring *loging* sistem *resource* pada *server* terhadap serangan DoS yang dilakukan sebelum menerapkan teknik DMZ dengan menggunakan *tool* Vmstat. Pada Gambar 12 disajikan hasil 10 kali pengujian *loging* sistem *resource* pada *server* dalam keadaan normal sebelum dilakukan serangan DoS untuk dijadikan pembanding *loging* sistem *resource* pada *server* saat terjadi serangan DoS.

```
inoxyz@server:~$ vmstat 1 10
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 1  0      0 547144  21064 228304    0    0    85     8 1750  142  1  1 96  3  0
 0  0      0 547136  21064 228304    0    0     0     0   32   61  0  0 100  0
0
 0  0      0 547136  21064 228304    0    0     0     0   29   58  0  1 99  0  0
 0  0      0 547136  21064 228304    0    0     0     0   30   63  0  0 100  0
0
 0  0      0 547136  21064 228304    0    0     0     0   30   67  0  0 100  0
0
 0  0      0 547136  21072 228296    0    0     0    40   40   74  0  0 97  3  0
 0  0      0 547136  21072 228304    0    0     0     0   30   64  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   29   60  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   26   58  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   33   68  0  0 99  1  0
inoxyz@server:~$
```

Gambar 12. *Loging* Sistem *Resource* Pada *Server* Sebelum Dilakukan Serangan DoS

Selanjutnya dilakukan monitoring *loging* sistem *resource* pada *server* saat terjadi serangan DoS dari ketiga jenis serangan DoS yang masing-masing dilakukan 10 kali pengujian, ketiga DoS *attack* tersebut yaitu *Ping of Death* / ICMP *Flooding Attack,* UDP *Flooding Attack,* dan Syn *Flooding Attack*.

Untuk memudahkan dalam penjelasannya penulis membuat data hasil

monitoring Vmstat dengan 10 kali pengujian *loging server* pada *system in* dari serangan DoS pada *server* dari ketiga jenis serangan DoS tersebut kedalam Tabel 3 Hasil pengujian serangan DoS pada server tanpa DMZ.

Tabel 3. Hasil Pengujian Server Tanpa DMZ

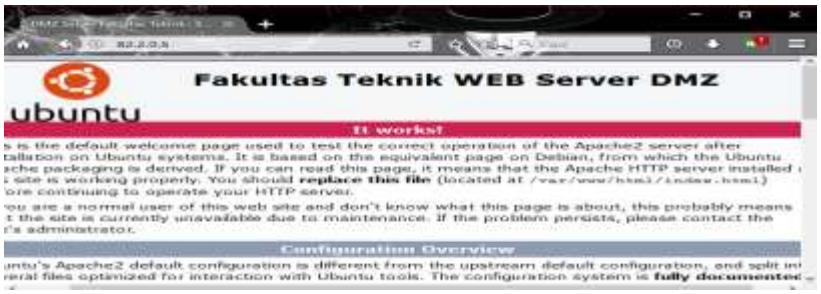
No.	**Hasil *Loging* Sistem *Resource server* pada *system in (Packet)***			
	Server Normal	ICMP *flooding*	UDP *flooding*	SYN *flooding*
1.	1750	1534	2066	2053
2.	32	16526	7582	7383
3.	29	16381	7561	8109
4.	30	16313	7613	7242
5.	30	16365	7676	7374
6.	40	16487	7771	7607
7.	30	16568	7526	7410
8.	29	16199	7638	7224
9.	26	16362	7744	6861
10.	33	16322	7656	7264

b. Pengujian *Server* DMZ

Pengujian layanan WEB *server* dan FTP *server* setelah dikonfigurasikan sebagai DMZ, yaitu memindahkan *request* layanan WEB *server* dan FTP *server* dari *IP address* 192.168.100.2 milik *server* ke *IP address* 82.2.0.5 milik router *firewall*. Jika semua layanan *server* yang akan dijadikan area DMZ dapat diakses melalui *IP address* milik router *firewall* artinya teknik DMZ telah berhasil diimplementasikan pada sistem jaringan komputer.

Pada Gambar 13 merupakan pengujian akses *request* pada layanan WEB *server* setelah dikonfigurasikan sebagai DMZ.

Pada Gambar 14 merupakan pengujian akses *request* pada layanan FTP *server* setelah dikonfigurasikan sebagai DMZ.



Gambar 13. *Request* Layanan WEB *Server* DMZ

Gambar 14. *Request* Layanan FTP *Server* DMZ

Dengan teknik DMZ tersebut sistem akan membatasi dan melakukan *filter* terhadap akses *client* yang melakukan *request* pada layanan *server* untuk diproses melalui router *firewall* terlebih dahulu sebelum dapat mengakses layanan yang ada pada *server*. Dengan demikian *server* akan lebih aman dari serangan karena *server* tidak secara langsung berhadapan dengan *client* dan jika terjadi serangan pada *server* maka *administrator* jaringan komputer lebih mudah untuk mencegah ataupun melindungi sistem dengan melakukan *block* dan *filter* melalui pertahanan pertama pada router *firewall*. Setelah sistem DMZ dapat digunakan, tahap berikutnya adalah melakukan pengujian sistem terhadap serangan *(penetration testing)* yang dilakukan pada sistem DMZ yang telah diimplementasikan pada jaringan komputer. Pengujian serangan yang dilakukan yaitu *information gathering* dengan teknik *port scanning* dengan menggunakan *tool* Nmap. Dengan teknik DMZ yang telah diimplementasikan pada jaringan komputer maka data informasi yang didapatkan dari *scaning port* tersebut bukan merupakan data dari *server* melainkan data dari router *firewall* sehingga *resource* sistem *server* dapat lebih terlindungi.

Selanjutnya dilakukan pengujian serangan DoS yang dilakukan sebanyak tiga kali dengan jenis serangan DoS *Ping of Death* / ICMP *Flooding Attack,* UDP *Flooding Attack,* dan Syn *Flooding Attack* setelah jaringan komputer sudah diimplementasikan teknik DMZ. Semua serangan DoS tersebut diarahkan pada *port 80* yang merupakan *port* untuk mengakses layanan WEB *server* hal tersebut dimaksudkan untuk menyerang layanan WEB *server* DMZ pada *port 80* agar layanan WEB *server* DMZ menjadi *down* dan untuk menguji sejauh mana sistem DMZ dapat melakukan *filter* terhadap serangan DoS untuk melindungi *server*.

Monitoring sistem router *firewall* dan *server* menggunakan *tools* yang telah ter-*install* secara *default* pada router *firewall* dan *server.* Pada router *firewall* RB750GL dengan Mikrotik RouterOS 5.16 untuk keperluan monitoring dapat menggunakan *tool* Torch.

Data hasil pengujian sistem terhadap serangan DoS yang telah dilakukan dibagi menjadi dua yaitu hasil pengujian serangan DoS pada *server* tanpa DMZ dan hasil pengujian serangan DoS pada *server* setelah menerapkan DMZ. Selanjutnya dibuat perbandingan dari kedua data pengujian tersebut pada analisa perbandingan hasil pengujian.

Setelah mendapatkan data monitoring dan hasil analisa dari pengujian *server* tanpa DMZ selanjutnya dilakukan monitoring *loging* sistem *resource* pada *server* dan router *firewall* setelah diimplementasikan dan dikonfigurasikan teknik DMZ terhadap tiga jenis serangan DoS. Monitoring *loging* sistem *resource* dilakukan pada router *firewall* dan *server,* karena akses layanan *server* dipindahkan ke router *firewall,* jadi dilakukan dua kali

monitoring yaitu pada sistem router *firewall* dan kemudian monitoring *server.*

Pada Gambar 15 merupakan monitoring *loging* sistem *resource* pada router *firewall* Mikrotik RouterOS 5.16 dalam keadaan normal sebelum dilakukan serangan DoS menggunakan *tool* Torch untuk dijadikan pembanding *loging* sistem *resource* pada *server* saat terjadi serangan DoS.

```
[admin@MikroTik] > tool torch interface=ether1<INTERNET> ip-protocol=any
IP-PROTOCOL          TX          RX TX-PACKETS RX-PACKETS
tcp             3.3kbps     1856bps          2          2
icmp             784bps      784bps          1          1
                4.1kbps     1840bps          3          3

-- [Q quit|D dump|C-z continue]
```

Gambar 15 *Tool* Torch Mikrotik RouterOS 5.16

Pada Gambar 16 merupakan 10 kali pengujian *loging* sistem *resource* pada *server* OS Ubuntu 16.10 *server* i386 menggunakan *tool* Vmstat dalam keadaan normal sebelum dilakukan serangan DoS.

```
inoxyz@server:~$ vmstat 1 10
procs -----------memory---------- ---swap-- -----io---- -system-- ------cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 1  0      0 547144  21064 228304    0    0    85     8 1750  142  1  1 96  3  0
 0  0      0 547136  21064 228304    0    0     0     0   32   61  0  0 100  0
0
 0  0      0 547136  21064 228304    0    0     0     0   29   58  0  1 99  0  0
 0  0      0 547136  21064 228304    0    0     0     0   30   63  0  0 100  0
0
 0  0      0 547136  21064 228304    0    0     0     0   30   67  0  0 100  0
0
 0  0      0 547136  21072 228296    0    0     0    40   40   74  0  0 97  3  0
 0  0      0 547136  21072 228304    0    0     0     0   30   64  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   29   60  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   26   58  0  0 100  0
0
 0  0      0 547136  21072 228304    0    0     0     0   33   68  0  0 99  1  0
inoxyz@server:~$
```

Gambar 16 *Tool* Vmstat OS Ubuntu 16.10 *Server* i386

Tujuan dari analisa hasil pengujian ini yaitu untuk mengetahui apakah router *firewall* yang dikonfigurasikan sebagai router DMZ dengan *IP address 82.2.0.5* dapat melakukan *filter* terhadap serangan DoS ke arah *server* dengan *IP address 192.168.100.2* atau tidak, jika terjadi serangan DoS pada layanan DMZ. Monitoring *loging* sistem *resource* dan *performance* dilakukan bersamaan ketika serangan DoS terjadi.

Untuk memudahkan dalam penjelasannya penulis membuat data hasil monitoring *loging* sistem *resource* dan *performance* pada router *firewall* dan *server* dari tiga jenis serangan DoS yang dilakukan tersebut kedalam Tabel 4 untuk hasil monitoring *loging* router *firewall* DMZ dan Tabel 4.5 untuk hasil monitoring *loging* server DMZ.

Dapat dilihat pada Tabel 4.4 untuk hasil monitoring *loging* router *firewall* DMZ bahwa terjadi aktivitas yang mencurigakan pada data hasil *loging* sistem router *firewall* saat terjadi DoS *attack* tersebut yaitu besar *traffic* TX-PACKETS *(transmit packets)* yang dikirim dan besar *traffic* RX-PACKETS *(receiver packet)* yang diterima naik dengan jumlah yang sangat besar dibandingkan dengan data *loging* sistem

router *firewall* saat keadaan normal, artinya router *firewall* mengalami *flooding*. Dan berikut pada Tabel 5 merupakan data hasil monitoring Vmstat dengan 10 kali pengujian *loging server* pada *system in* dari serangan DoS pada *server* DMZ dari ketiga jenis pengujian serangan DoS yang dilakukan.

Tabel 4. Hasil Pengujian DoS Attack Router *Firewall* DMZ

No.	Metode Serangan DoS	Sistem *resource* Router *firewall (Packet)*			
		Tx	Rx	Tx Packets	Rx Packets
1.	Normal	3.3 kbps	1056 bps	2	2
2.	ICMP *flooding*	2.8 Mbps	4.1 Mbps	8586	8586
3.	UDP *flooding*	0 bps	4.1 Mbps	0	8356
4.	SYN flooding	1248.2 kbps	3.5 Mbps	2686	7314

Table 5. Hasil Pengujian DoS *Attack Server* DMZ

No.	Hasil *Loging* Sistem *Resource server* pada *system in (Packet)*			
	Server Normal	ICMP *flooding*	UDP *flooding*	SYN *flooding*
1.	1750	622	616	606
2.	32	34	35	7681
3.	29	32	30	7695
4.	30	29	75	7802
5.	30	35	26	7534
6.	40	33	29	7319
7.	30	35	26	7238
8.	29	28	29	7143
9.	36	33	30	7133
10.	33	31	28	7126

3.2 Pembahasan

Hasil yang diperoleh dari hasil pengujian yang telah dilakukan yaitu berupa data perbandingan *loging server* saat terjadi DoS *attack* dari tiga jenis pengujian DoS *attack* sebelum dan sesudah *server* diimplementasi teknik DMZ, hasil perbandingan tersebut dapat dilihat pada tabel 6.

Untuk memudahkan dalam melihat perbandingan saat terjadi DoS *attack* dari tiga jenis pengujian DoS *attack* sebelum dan sesudah *server* diimplementasi teknik DMZ, maka dibuat grafik nilai *packet* data yang masuk pada *sistem in server* dalam satuan (*packet*). Untuk memudahkan dalam penjelasannya penulis akan membagi analisa hasil pengujian sistem tersebut menjadi tiga bagian berdasarkan jenis serangan DoS *Ping of Death* / ICMP *Flooding Attack,* UDP *Flooding Attack,* dan Syn *Flooding Attack*, dan untuk mengetahui jenis serangan DoS yang bagaimana yang membuat dampak kerusakan paling besar tarhadap sistem dari sisi router *firewall* dan *server.*

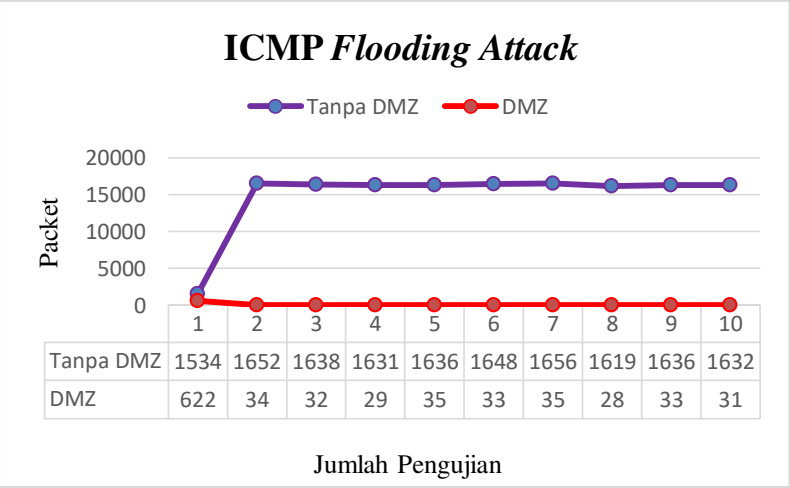
1. Data Perbandingan ICMP *Flooding Attack*

Pada Gambar 17 Grafik disajikan perbandingan hasil *loging* ICMP *flooding attack* pada *server* tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 16391,4 *packet* dan rata-rata *packet* yang diterima saat DMZ sebanyak 32,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat terjadi DoS *attack* sebesar 16359,2 *packet*

setelah implementasi teknik DMZ, artinya DMZ berhasil melakukan *filter* sebesar 16359,2 *packet* pada DoS *attack* tersebut. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang *valid.*

Tabel 6. Data Perbandingan *Loging Server*

No.	Hasil *Loging* Sistem *Resource server* pada *system in (Packet)*					
	Packet ICMP *flooding attack*		*Packet* UDP *flooding attack*		*Packet* SYN *flooding attack*	
	Tanpa DMZ	DMZ	Tanpa DMZ	DMZ	Tanpa DMZ	DMZ
1.	1534	622	2066	616	2053	606
2.	16526	34	7582	35	7383	7681
3.	16381	32	7561	30	8109	7695
4.	16313	29	7613	75	7242	7802
5.	16365	35	7676	26	7374	7534
6.	16487	33	7771	29	7607	7319
7.	16568	35	7526	26	7410	7238
8.	16199	28	7638	29	7224	7143
9.	16362	33	7744	30	6861	7133
10.	16322	31	7656	28	7264	7126



Gambar 17. Grafik Perbandingan ICMP *Flooding Attack*

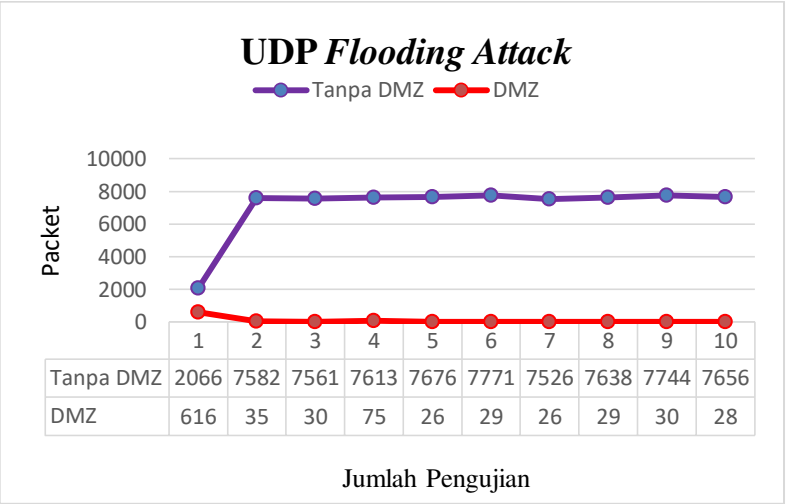
2. Data Perbandingan UDP *Flooding Attack*

Pada Gambar 18 Grafik disajikan perbandingan hasil *loging* UDP *flooding attack* pada *server* tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 7640,7 *packet* dan rata-rata *packet* yang diterima saat DMZ sebanyak 34,2 *packet*, sehingga didapatkan perbandingan penurunan jumlah *packet* saat terjadi DoS *attack* sebesar 7606,5 *packet* setelah implementasi teknik DMZ, artinya DMZ berhasil melakukan *filter* sebesar 7606,5 *packet* pada DoS *attack* tersebut. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang *valid.*

3. Data Perbandingan Syn *Flooding Attack*

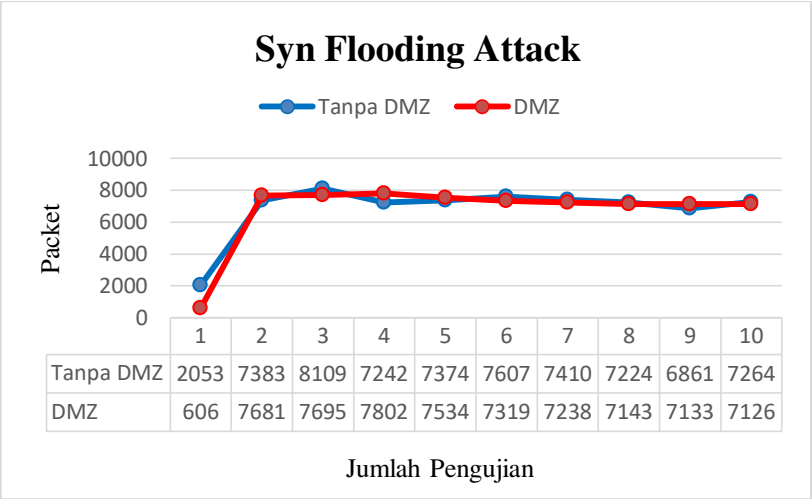
Pada Gambar 19 Grafik perbandingan hasil *loging* Syn *flooding attack* pada *server* tanpa DMZ rata-rata menunjukan jumlah *packet* yang diterima sebanyak 7386 *packet* dan rata-rata *packet* yang diterima saat DMZ

sebanyak 7407,8 *packet*, sehingga didapatkan perbandingan jumlah *packet* yang hampir sama pada *server* sebelum dan setelah implementasi teknik DMZ, artinya DMZ tidak berhasil melakukan *filter* pada jenis DoS Syn *flooding attack* tersebut karena *server* masih terkena *flooding*. Sebagai informasi data pengujian 1 (satu) tidak dihitung karena data tersebut bukan merupakan data yang *valid.*



	1	2	3	4	5	6	7	8	9	10
Tanpa DMZ	2066	7582	7561	7613	7676	7771	7526	7638	7744	7656
DMZ	616	35	30	75	26	29	26	29	30	28

Gambar 18. Grafik Perbandingan UDP *Flooding Attack*



	1	2	3	4	5	6	7	8	9	10
Tanpa DMZ	2053	7383	8109	7242	7374	7607	7410	7224	6861	7264
DMZ	606	7681	7695	7802	7534	7319	7238	7143	7133	7126

Gambar 19. Grafik Perbandingan Syn *Flooding Attack*

4. Kesimpulan Dan Saran

4.1 Kesimpulan

Kesimpulan yang dapat diambil dari penelitian ini yaitu teknik keamanan jaringan DMZ dapat diimplementasikan pada sistem jaringan komputer Universitas Islam "45" dengan baik, dan implementasi teknik DMZ pada layanan *server* jaringan LAN dapat melakukan *filter* terhadap serangan DoS jenis ICMP *flooding attack* dan UDP *flooding attack*

4.2 Saran

Berdasarkan hasil pembahasan dapat diberikan yaitu penggunaan spesifikasi *hardware* yang maksimal dan memaksimalkan fungsi *firewall filtering* pada router *firewall* Mikrotik untuk

memblokir *port* yang masih mungkin untuk disusupi.

DAFTAR PUSTAKA

Hermawan, Rudi,."Analisis Konsep Dan Cara Kerja Serangan Komputer *Distributed Denial Of Service* (DDoS), Faktor Exacta Vol. 5 No. 1: 1-14, ISSN: 1979 276X

Ikhwan,Syariful.,dan Ikhwana Elfitri.2014."Analisa Delay Yang Terjadi Pada Penerapan Demilitarized Zone (Dmz) Terhadap Server Universitas Andalas ".Jurnal Nasional Teknik Elektro,3(2)ISSN:2302-2949.

Juman,Kundang K,.2003."Membangun Keamanan Jaringan Komputer Dengan Sistem De-Militarised Zone (DMZ)".Jurnal FASILKOM,1(1).

Sasongko,Ashwin,.2011.*Pedoman Keamanan Web Server.*Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika, Kementrian Komunikasi dan Informatika.

Setiyo Sukarno,Aji,.2010. "Cara Memperkuat Keamanan Dari Dmz (Demilitarized Zones)".(0706100712)

Shimonski,Robert J,.2003.*Building DMZs for Enterprise Networks.*Printed in the United States of America,ISBN:1-931836-88-4,Group West in the United States and Jaguar Book Group in Canada.

Sujito.,dan Mukhamad Fathur Roji.2010."Sistem Keamanan Internet Dengan Menggunakan IPTABLES Sebagai Firewall".Jurnal Ilmiah DINAMIKA DOTCOM,1(1).

Sumarno,Eko.,dan Hanugrah Probo Hasmoro.2013."Implementasi Metode *Load Balancing* Dengan Dua Jalur".*Indonesian Jurnal on Networking and Security* (IJNS)-ijns.org

Sweatly Ekel, Zico,.dkk. *Attacking Side With Backtrack*. *Codewall-Security* PT.Pinhard Indonesia

S'To, 2014. *Kali Linux : 200% Attack*. Jasakom

Towidjojo,Rendra,.2013.*Mikrotik Kung Fu : Kitab 1*. Jasakom

Wijaya,Benny,.dkk.2014."Analisis Dan Perancangan Keamanan Jaringan Menggunakan Teknik *Demilitarized Zone* (Dmz)".Seminar Nasional Teknologi Informasi, Komunikasi dan Managemen.