CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 3, No. 2, November 2020, hlm. 22-27

METODE DEMILITARIZED ZONE DAN PORT KNOCKING UNTUK KEAMANAN JARINGAN KOMPUTER

Andik Saputro[1], Nanang Saputro[2], Hendro Wijayanto[3]

[1,2,3]Program Studi Informatika, STMIK Sinar Nusantara
Email: [1]18500102.andik@sinus.ac.id, [2]18500020.nanang@sinus.ac.id, [3]hendrowijayanto.lecturer@sinus.ac.id

(Naskah masuk: 20 Oktober 2020, diterima untuk diterbitkan: 31 November 2020)

Abstrak

Saat ini cara komunikasi jaringan sudah banyak berubah. Seluruh aspek menjadi sangat bergantung pada layanan *online*. Karyawan dapat bekerja dari rumah, dan siswa dari segala usia mengambil kelas secara *online*. Semakin publik bergantung untuk tetap terhubung dengan jaringan, semakin besar potensi serangan jaringan yang terjadi. Dalam jaringan komputer jika tidak dilindungi akan menyebabkan kerugian berupa kehilangan data atau *file*, kerusakan *system server*, tidak maksimal dalam melayani *user* atau bahkan kehilangan aset berharga institusi. Serangan yang paling sering digunakan dalam jaringan adalah *Port Scanning* dan *DDoS (Distributed Denial Of Service)*. Dalam penelitian ini menggabungkan metode *DeMilitarized Zone* dan *Port Knocking* untuk mengamankan jaringan komputer. Implemetasi teknik *DeMilitarized Zone* digunakan untuk mengakses server lokal agar bisa diakses dari luar dengan teknik *Port Knocking*. Hal ini untuk membuka *port* akses yang di filter pada konfigurasi *router* di sistem keamanan jaringan *server*. DeMilitarized Zone dan *Port Knocking* dapat diimplementasikan pada jaringan lokal maupun interlokal dimana jika suatu penyerang ingin meng*exploit* atau menyerang *server* utama maka yang pertama diserang adalah *server firewall* (*router*). *Port Knocking* juga dapat diimplementasikan pada jaringan lokal maupun interlokal dengan dipadukan *time limit ping request* yang menjadikan lebih aman, sehingga jika penyerang ingin mengakses *router*, dan tidak mengetahui aturan dari *remote* maka yang terjadi adalah penolakan terhadap akses port tersebut.

Kata kunci: *demilitarized zone, port knocking, keamanan jaringan, mikrotik, jaringan komputer*

DEMILITARIZED ZONE AND PORT KNOCKING METHODS FOR COMPUTER NETWORK SECURITY

Abstract

Currently, the way of network communication has changed a lot. All aspects become very dependent on online services. Employees can work from home, and students of all ages take online classes. The more the public depends on staying connected to the network, the greater potential network attacks to occur. In a computer network, if it is not protected, it will data or file loss, damage to the server system, not being optimal in serving users or even losing valuable institutional assets. The attacks most often used in networks are Port Scanning and DDoS (Distributed Denial Of Service). In this study, the DeMilitarized Zone and Port Knocking methods are combined to secure computer networks. DeMilitarized Zone technique implementation is used to access local servers, so that they can be accessed from outside with Port Knocking technique. To open the access port that is filtered in the router configuration on the server network security system. DeMilitarized Zone and Port Knocking can be implemented on local and long distance networks where if an attacker wants to exploit or attack the main server, the first to be attacked is the firewall server (router). Port Knocking can also be implemented on local and long distance networks with a combined ping request time limit which makes it safer, so that if an attacker wants to access the router, and doesn't know the rules from the remote, what happens is a rejection of port access.

Keywords: *demilitarized zone, port knocking, network security, mikrotik, networking*

1. PENDAHULUAN

Pada kuartal pertama tahun 2020, dalam hitungan minggu, cara hidup komunikasi jaringan berubah. Seluruh aspek menjadi sangat bergantung pada layanan online. Karyawan dapat bekerja dari rumah, dan siswa dari segala usia mengambil kelas secara online. Semakin publik bergantung untuk tetap terhubung dengan jaringan, semakin besar potensi serangan jaringan yang terjadi. Oleh karena itu, tidak mengherankan bahwa pada Q1 2020 (1 Januari 2020 hingga 31 Maret 2020) telah dilaporkan peningkatan jumlah serangan (Vivek Ganti, 2020) .

Keamanan jaringan sangat vital bagi sebuah jaringan komputer. Kelemahan yang ada di jaringan komputer jika tidak dilindungi akan menyebabkan kerugian berupa kehilangan data atau file, kerusakan system server, tidak maksimal dalam melayani user atau bahkan kehilangan aset berharga institusi. Keamanan jaringan merupakan hal yang sangat penting untuk diperhatikan karena ancaman serangan yang semakin canggih dan beragam, terlebih ketika jaringan lokal sudah terhubung ke internet maka ancaman keamanan jaringan akan meningkat. Misalnya *Distributed Denial of Service (DDoS)*, serangan *hacker*, virus, trojan yang semuanya merupakan ancaman yang tidak bisa dihindari.

Serangan yang paling sering digunakan adalah *Port Scanning* dan *DDoS (Distributed Denial Of Service)*. Hasil report Link11 menunjukkah bahwa terdapat peningkatan 81% maksimum bandwidth yang dialokasikan dalam menangani *DDoS* ini. Sedangkan volume packet tertinggi sebanyak 19 packet dengan lebih dari 50Gbps (Link11, 2020).

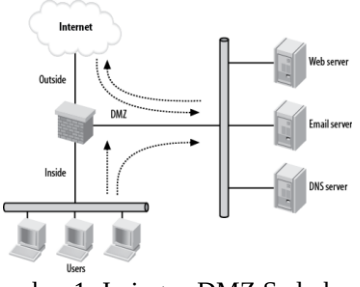
Dalam pemaparan Policy Brief dengan judul ”Kesiapan Perguruan Tinggi Wilayah Jawa Tengah Dalam Menghadapi Serangan Siber”, penggunaan teknologi informasi dan sumber daya merupakan bagian terpenting dari kesiapan Perguruan Tinggi dalam menghadapi serangan siber. Kondisi saat ini yang terjadi, banyak Perguruan Tinggi yang belum siap menghadapi serangan siber. Begitu pula minimnya pemahaman terhadap prosedur sebelum dan sesudah insiden (Hendro Wijayanto, 2020).

Untuk itu diperlukan teknik keamanan jaringan yang dapat menangkal ancaman serangan tersebut atau meminimalisir ancaman serangan yang bisa memasuki sistem jaringan. Dalam penelitian ini implemetasi teknik *DeMilitarized Zone (DMZ)* digunakan untuk mengakses server lokal agar bisa diakses dari luar dengan teknik *Port Knocking*. Hal ini untuk membuka port akses yang di filter pada konfigurasi router di sistem keamanan jaringan server.

2. TINJAUAN PUSTAKA

Serangan *Distributed Denial of Services (DDoS)* mempengaruhi korban dalam bentuk menemukan bug atau kelemahan untuk mengganggu layanan atau menghabiskan semua *bandwidth* sumber daya dari sistem korban. Penyerang memindai jaringan untuk menemukan bagian yang memiliki kerentanan dan kemudian bagian ini digunakan sebagai agen oleh penyerang. Ini disebut komputer *zombie*. *Internet Protokol (IP)* palsu digunakan oleh komputer *zombie*. Keamanan di internet tergantung pada host. Penyerang membahayakan keamanan host untuk meluncurkan serangan *DDoS* dan mereka menggunakan alamat IP palsu sehingga sulit untuk melacak sumber serangan. Target utama serangan *DDoS* adalah sumber daya seperti *bandwidth*, *CPU*, dan lainnya. Dan sumber daya terbatas dalam jaringan. Jika sumber daya ini ditingkatkan maka dampak serangan dapat diturunkan (Deshmukh & Devadkar, 2015) (Behal & Kumar, 2016).

Firewall sering kali memiliki apa yang biasa disebut DMZ. DMZ adalah singkatan dari *Demilitarized Zone*, yang tentunya tidak ada hubungannya dengan komputasi. Ini adalah istilah yang mengacu pada zona yang dibuat antara kekuatan yang berlawanan di mana tidak ada aktivitas luar yang diizinkan. Dalam ranah keamanan jaringan, *DMZ* adalah jaringan yang tidak berada di dalam maupun di luar *firewall*. Bahwa jaringan ketiga ini dapat diakses dari dalam (dan mungkin di luar) *firewall*, tetapi aturan keamanan akan melarang perangkat di *DMZ* untuk terhubung ke perangkat di dalamnya. *DMZ* kurang aman dibandingkan jaringan dalam, tetapi lebih aman daripada jaringan luar. Skenario *DMZ* secara umum ditunjukkan pada Gambar 1. Internet terletak di antarmuka luar. Pengguna berada di antarmuka bagian dalam. Semua server yang perlu dapat diakses dari Internet berada di jaringan *DMZ* (Donahue, 2011).

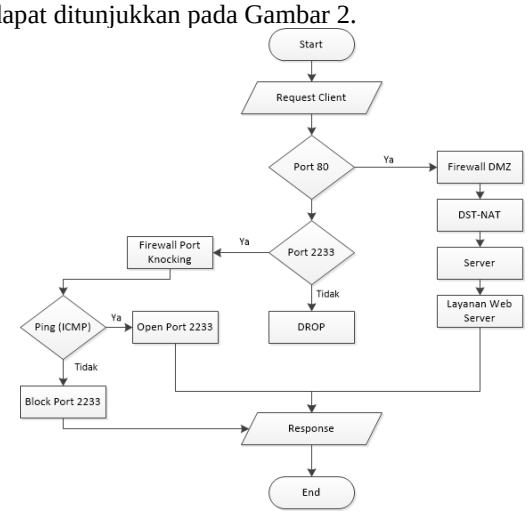


Gambar 1. Jaringan DMZ Sederhana

Port Knocking adalah metode yang dilakukan untuk membuka akses ke *port* tertentu yang telah diblock oleh *Firewall* pada perangkat jaringan dengan cara mengirimkan paket atau koneksi tertentu. Koneksi bisa berupa *protocol TCP*, *UDP* maupuan *ICMP*. Jika koneksi yang dikirimkan oleh *host* tersebut sudah sesuai dengan *rule knocking* yang diterapkan, maka secara dinamis *firewall* akan memberikan akses ke *port* yang sudah di*block*. Dengan cara ini, perangkat jaringan seperti *Router* akan lebih aman, sebab admin jaringan bisa melakukan *blocking* terhadap *port-port* yang rentan terhadap serangan seperti *Winbox* (*tcp* 8291), *SSH* (*tcp* 22), *Telnet* (*tcp* 23) atau *webfig* (*tcp* 80). Jika dilakukan *port scanning port-port* tersebut terlihat tertutup. Dari sisi administrator jaringan tetap bisa melakukan konfigurasi dan monitoring akan tetapi dengan langkah-langkah khusus (*knocking*) agar bisa diijinkan oleh *firewall* untuk akses *port* seperti *Winbox* dan *SSH*. Untuk dapat menerapkan metode *port knocking* sederhana, kita bisa memanfaatkan *Address-List* pada *Router*. Fitur *Address-List* dapat digunakan untuk melakukan pengelompokan / *grouping IP Address* yang selanjutnya group *IP* tersebut dapat digunakan pada fitur lain seperti *Firewall Filter*, *NAT* atau *Mangle* (Mikrotik, n.d.).

3. METODE PENELITIAN

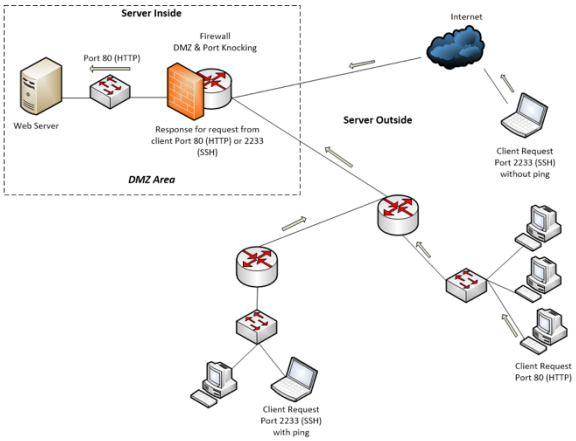
Model metode yang digunakan adalah penggabungan dari Demilitarized Zone dan Port Knocking. Adapun diagram model metode keduanya dapat ditunjukkan pada Gambar 2.



Gambar 2. Model *DMZ* dan *Port Knocking*

Dari Gambar 2 model *DMZ* dan *Port Knocking* diatas, dijelaskan bahwa alur proses dimulai dari *request client* yang mengarah ke *router*. Terdapat 2 *request* yang ditujukan ke *server*. Pertama adalah *request* ke *port* 80 (*web server*) dan yang kedua adalah *port* 2233 (*ssh*). *Router* akan menerima *request* dari *client*, jika *request* tersebut adalah *port* 80, maka *router* akan memberlakukan aturan *DMZ* kemudian diteruskan ke *web server* dan memberikan *response* ke *client*. Dan jika *request* pada *port* 2233 maka router akan memberlakukan aturan *Port Knocking*. Di *Port Knocking* akan memberlakukan aturan jika *client ping* ke *router*, maka *port* 2233 akan terbuka, jika *client* tidak melakukan *ping* ke *router*, maka ketika *client* mencoba koneksi ke *router* maka *response* ke *client* adalah menolak permintaan koneksi ke *port* 2233.

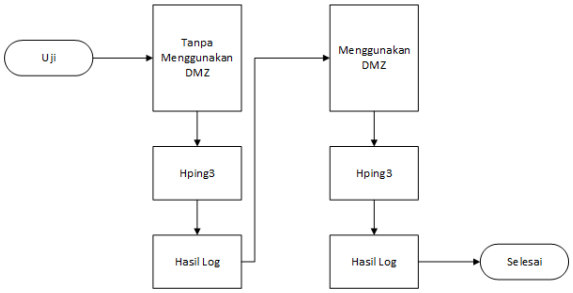
Sedangkan untuk topologi yang digunakan adalah seperti Gambar 3. Model topologi ini akan diimplementasikan pada Perguruan Tinggi swasta di Kota Surakarta, Jawa Tengah.



Gambar 3. Topologi Jaringan

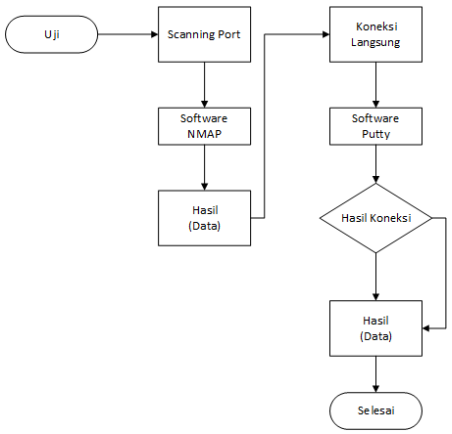
Dari Gambar 3 model topologi jaringan diatas, terdapat 2 area yaitu *server inside* dan *server outside*. *Server inside* adalah area terfilterisasi dari jaringan luar dan *server outside* area yang bebas dari filterisasi. Perbedaanya adalah jika suatu client mengakses atau melakukan koneksi ke *server inside* maka diberlakukan aturan filterisasi sedangkan pada *server outside* tidak diberlakukan aturan filterisasi. Selain itu pada area *server inside* akan menerima 2 *request* yaitu *http* dan *ssh*. Perbedaanya jika *request* ke *http* akan diberlakukan aturan *DMZ* kemudian diteruskan ke *server web*. Sedangkan jika *request* ke *ssh* akan berhenti di *router* dan diberlakukan aturan *Port Knocking*.

Sedangkan untuk tahap atau bagan alur dalam pengujian *DMZ* dan *Port Knocking* di representasikan pada Gambar dibawah ini :



Gambar 4. Bagan Alur Pengujian *DMZ*

Pada gambar 4 diatas adalah bagan alur proses pengujian *DMZ* adalah dilakukan secara 2 tahap, yaitu dengan tanpa menggunakan *DMZ* dan menggunakan *DMZ*. Dari tahap pengujian tanpa menggunakan *DMZ* alur prosesnya adalah menguji menggunakan tools *Hping3* lalu mendapatkan hasil data *log*. Kemudian dilanjutkan dengan pengujian menggunakan DMZ dengan *tools* yang sama lalu menghasilkan data *log*. Dari setiap hasil pengujian tersebut diperoleh perbandingan hasil data *log* dan seberapa banyak *resource* yang dipakai di server.



Gambar 5. Bagan Alur Pengujian *Port Knocking*

Sedangkan gambar 5 diatas adalah bagan alur proses pengujian *Port Knocking*. Tahap pengujian dilakukan secara 2 tahap, yaitu tahap pengujian *scanning port* dan tahap pengujian koneksi langsung. Dari tahap pertama yaitu pengujian scanning port dengan menggunakan tools *NMAP*, dari hasil *scanning* tersebut maka didapatkan hasil data. Kemudian dilanjut pengujian tahap kedua yaitu pengujian secara koneksi langsung menggunakan software putty. Dari koneksi langsung tersebut akan menghasilkan 2 kemungkinan yaitu koneksi yang diterima dan koneksi yang ditolak. Dari hasil pengujian tersebut maka didapatkan keseluruhan data pengujian.

4. HASIL DAN PEMBAHASAN

4.1. Implementasi

Pada penelitian ini akan terfokus pada Gambar 3 yang akan menerapkan aturan *DMZ* sebagai *firewall* utama yang berfungsi untuk mengubah alamat *IP* server lokal menjadi alamat *IP* publik agar jaringan lokal dari server dapat diakses melalui luar dengan menggunakan *IP* server dengan asumsi semua jaringan sudah terintegrasi dengan konfigurasi *routing*. Sedangkan untuk *Port Knocking* akan terfokus pada *firewall blocking port* untuk memfilter setiap akses masuk dari *port* yang terbuka. Dibawah ini service yang diterapkan pada konfigurasi *DMZ* di router :

- Konfigurasi firewall NAT (Network Address Translation) pada router utama yang berfungsi untuk mengubah IP lokal dapat merespon request dari luar :

```
[admin@Router Utama] > ip firewall nat
add chain=srcnat out-interface=ether1
action=masquerade
```

- Kemudian konfigurasi DMZ yang berfungsi untuk mengubah alamat IP router jika diakses maka akan di redirect ke IP Server Lokal :

```
[admin@Router Utama] ip firewall nat add
chain=dstnat dst-address=10.10.10.1
protocol=tcp dst-port=80 action=dst-nat
to-addresses=192.168.100.2 to-ports=80
```

- Kemudian konfigurasi Routing pada setiap router yang berfungsi agar setiap jaringan dapat mengakses server. Pada penelitian ini menggunakan jenis *routing RIP* dikarenakan jumlah pengguna komputer yang tidak begitu luas dan besar (fokus pada satu area)
- Kemudian konfigurasi *Port Knocking* yang berfungsi untuk memfilter *port* yang digunakan untuk konfigurasi saja, dan menonaktifkan *port* yang tidak digunakan (kecuali *port* 22).
- Selanjutnya konfigurasi firewall filter untuk port knocking sebagai berikut :

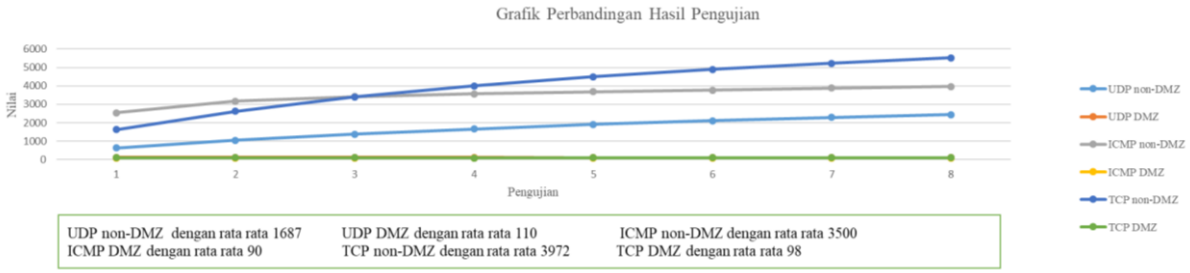
```
[admin@Router Utama] > ip firewall filter
add chain=input protocol=icmp action=add-
src-to-address-list address-list=ping
address-list-timeout=00:00:01

[admin@Router Utama] > ip firewall filter
add chain=input protocol=tcp dst-
port=2233 src-address-list=ping
action=accept

[admin@Router Utama] > ip firewall filter
add chain=input protocol=tcp action=add-
src-to-address-list address-list=scanport
address-list-timeout=00:10:00

[admin@Router Utama] > ip firewall filter
add chain=input protocol=tcp src-address-
list=scanport action=drop

[admin@Router Utama] > ip firewall filter
add chain=input protocol=tcp dst-
port=2233 action=add-src-to-address-list
address-list=scanssh address-list-
timeout=00:10:00

[admin@Router Utama] > ip firewall filter
add chain=input protocol=tcp src-address-
list=scanssh action=drop
```

4.2. Pengujian

Pengujian pada *server DMZ* dilakukan dalam 2 tahap yaitu tanpa menggunakan *DMZ* dan menggunakan *DMZ*. Pada pengujian ini, *tools* yang digunakan adalah *Hping3* pada *client Linux*. *Hping3* adalah tools yang digunakan untuk membanjiri paket ke *server* dengan *request* yang tinggi dan secara cepat. Tabel 1 dibawah ini adalah data sistem *resource* pada *server* (*traffic network*) yang diperoleh dari pengujian tanpa menggunakan *DMZ*

(secara langsung pada jaringan lokal) dalam 8 kali percobaan :

Grafik Perbandingan Hasil Pengujian dari Hping3



Gambar 6. Grafik Perbandingan Hasil Pengujian

Hasil yang diperoleh dari pengujian yang telah dilakukan yaitu berupa data perbandingan *loging server* saat terjadi *DDoS attack* dari tiga jenis pengujian *DDoS attack* sebelum dan sesudah server diimplementasi teknik *DMZ*. Hasil perbandingan tersebut dapat dilihat pada Gambar 6. Dari delapan kali percobaan bahwa jika tanpa menggunakan *DMZ* sistem *resource logging* pada *server* mengalami peningkatan yang sangat tinggi, hal tersebut hanya ada satu penyerang, jika ada banyak penyerang maka secara otomatis *server* akan sibuk dengan permintaan dari penyerang dan apabila tidak segera ditangani akan menyebabkan *server* mengalami kerusakan. Sistem *resource logging* pada *server* dari delapan kali percobaan tidak mengalami peningkatan yang signifikan, akan tetapi di beberapa percobaan mengalami penurunan *resource* karena hal tersebut sudah ditangani langsung oleh *server router* semua permintaan dari *client*. Maka dengan adanya *DMZ*, *server* dapat terhindar dari penyerangan *request* yang bersifat *flooding*. Selain itu jika menggunakan *DMZ*, maka *router* secara otomatis akan menonaktifkan *interface* yang sedang diserang oleh penyerang dan akan mengaktifkan kembali jika penyerang tidak melakukan serangan ke *server*.

Pengujian *port knocking* dilakukan secara dua tahap yaitu proses *scanning port* dengan menggunakan *tools nmap* di *client linux* dan koneksi langsung ke *server router* menggunakan *software putty* di *client windows* dengan *request ping* secara bersamaan. Pada pengujian pertama diperoleh data yang disajikan pada Gambar 7 berikut :

```
anon anon # nmap 10.10.10.1

Starting Nmap 7.01 ( https://nmap.org ) at 2020-10-05 19:54 WIB
Nmap scan report for 10.10.10.1
Host is up (0.0013s latency).
All 1000 scanned ports on 10.10.10.1 are filtered

Nmap done: 1 IP address (1 host up) scanned in 34.47 seconds
anon anon #
```

Gambar 7 Pengujian port scanning

Sedangkan pengujian kedua dilakukan sebanyak 10 kali percobaan dengan hasil yang disajikan pada Tabel 1 dibawah ini :

Tabel 1 Pengujian koneksi *server router*

Pengujian Ke	Keterangan
1	Gagal
2	Berhasil
3	Berhasil
4	Berhasil
5	Berhasil
6	Gagal
7	Gagal
8	Berhasil
9	Berhasil
10	Berhasil

Pengujian pertama dilakukan *port scanning* ke alamat *IP server router* untuk melihat *port - port* yang terbuka. Pada Gambar 7 disajikan hasil dari proses *port scanning*, dari gambar tersebut tidak ada satupun *port* yang ditampilkan (*terfilter*). Hal tersebut mengindikasikan bahwa *firewall* pada *router* bekerja dengan baik. Sedangkan pada pengujian kedua diperoleh data hasil koneksi ke *server router* dengan menggunakan *software putty* yang disajikan pada Tabel 1. Dari data tersebut terjadi tiga kegagalan dalam koneksi ke *server router* dari sepuluh kali percobaan. Satu dari tiga kegagalan mengalami *error* ketika sudah memasuki *remote router*. Dari masalah tersebut dapat diambil kesimpulan bahwa terjadinya kegagalan tersebut akibat dari aturan time limit yang dibuat. Jika suatu *client* ingin me*remote router* maka diharuskan *ping* ke *server router* dengan jangka waktu *request* sesuai dengan penggunaan, jika *ping* dengan waktu yang singkat maka akan terjadi *error* atau kegagalan koneksi ke *remote server router*.

5. KESIMPULAN

Teknik keamanan jaringan *DMZ* dan *Port Knocking* dapat diimplementasikan pada jaringan lokal maupun interlokal dimana jika suatu penyerang ingin meng*exploit* atau menyerang *server* utama maka yang pertama diserang adalah *server firewall* (*router*). Sedangkan *Port Knocking* juga dapat diimplementasikan pada jaringan lokal maupun interlokal dengan dipadukan *time limit ping request* yang menjadikan lebih aman, sehingga jika penyerang ingin mengakses *router*, dan tidak

mengetahui aturan dari *remote* maka yang terjadi adalah penolakan terhadap akses port tersebut.

Berdasarkan hasil pembahasan dapat diberikan informasi yaitu penggunaan fungsi *DMZ* dan *firewall filtering* untuk *Port Knocking* pada *router firewall* Mikrotik dapat memberikan keamanan kepada *server* utama (*DMZ*) dan keamanan pada *server router* (*Port Knocking*). Disamping itu diperlukan spesifikasi *hardware* yang maksimal pada perangkat *router* untuk mengantisipasi terjadinya penyerangan secara individu maupun kelompok dan memblokir *port* yang mungkin bisa disusupi.

Berdasarkan hasil penelitian dapat diberikan informasi yaitu penggunaan fungsi *DMZ* dan *Port Knocking* dapat memberikan keamanan kepada server utama (*DMZ*) dan server router (*Port Knocking*) dari serangan *Distributed Denial of Services (DDoS)* dan *Port Scanning* yang dapat membahayakan server. Akan tetapi keamanan tersebut hanya berlaku pada area *outside* (luar), sedangkan area *inside* (dalam) memiliki keamanan yang berbeda dari *outside*, sehingga perlu penambahan keamanan dari sisi yang lain misal seperti keamanan pada ruang penyimpanan dan sistem enkripsi password pada server.

DAFTAR PUSTAKA

BEHAL, S., & KUMAR, K. (2016). Trends in Validation of DDoS Research. *Procedia Computer Science*, *85*(Cms), 7–15. https://doi.org/10.1016/j.procs.2016.05.170

DESHMUKH, R. V., & DEVADKAR, K. K. (2015). Understanding DDoS attack & its effect in cloud environment. *Procedia Computer Science*, *49*(1), 202–210. https://doi.org/10.1016/j.procs.2015.04.245

DONAHUE, G. A. (2011). *Network Warrior* (2nd ed.; O. Media, Ed.). United State: O'Reilly Media.

HENDRO WIJAYANTO, I. A. P. (2020). *Policy Brief : Kesiapan Perguruan Tinggi Wilayah Jawa Tengah Dalam Menghadapi Serangan Siber*. Indonesia: LPPM Universitas Dian Nuswantoro.

LINK11. (2020). *DDoS Statistics (infographic) for the 1st Quarter of 2020*. Retrieved from https://www.link11.com/en/downloads/ddos-statistics-infographic-for-the-1st-quarter-of-2020/

MIKROTIK. (n.d.). Simple Port Knocking. Retrieved October 19, 2020, from Mikrotik website: http://www.mikrotik.co.id/artikel_lihat.php?id=105

VIVEK GANTI, O. Y. (2020). Network-layer DDoS attack trends for Q2 2020. Retrieved October 19, 2020, from Cloudflare website: https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q2-2020/