Perbandingan Tingkat Keamanan Jaringan Metode *OpenVpn* Pada *Server* Debian dan *Server* Ubuntu

Muller Millian Sasauw[1], Gogor C. Setyawan[2], Ag. Rudatyo Himamunanto[3]
[1,2,3]Program Studi Informatika, Fakultas Sains dan Komputer
Universitas Kristen Immanuel
Jalan Solo KM.11,1 , Yogyakarta, Telp: 0274-496256
email: ***[1]mullermillian31@gmail.com**

Abstrak

Jaringan publik (public network/ internet) merupakan jaringan yang dapat dilalui oleh siapapun pengguna jasa layanan tersebut. Oleh karena itu, setiap pengguna dapat memanfaatkan kesempatan tersebut untuk melakukan gangguan terhadap privasi komunikasi yang dilakukan oleh pengguna lain, Sehingga pada dasarnya jaringan publik yang digunakan rentan terhadap serangan keamanan. Akan tetapi penggunaan VPN dapat menjadi solusi dalam permasalahan tersebut.

Pada penelitian ini akses VPN yang dipakai, menggunakan metode OpenVPN yang menggunakan protocol enkripsi SSL dengan menerapkan sertifikat digital dalam koneksi client dan server. Client akan melakukan serangan untuk menguji keamanan jaringan dari server yang dengan tool DDoS pada Kali Linux. Hasil QoS akan digunakan sebagai acuan dalam melakukan perbandingan tingkat keaamanan pada server.

Hasil pengujian QoS sesudah penyerangan kedua server tidak bisa melakukan proses pengiriman data dari client atau mengalami down karena efek dari serangan DDoS yang membanjiri kedua komputer server. Hasil pengujian, 30 paket yang dikirim dari client tidak sampai ke server.. Namun disaat tidak ada serangan jumlah pengujian QoS memiliki kekuatan yang berbeda.

Kata Kunci: Open VPN, Keamanan Jaringan

Abstract

The public network (public network / internet) is a network that anyone who uses these services can pass.therefore, every user can take advantage of this oppotunity to disturb with the privacy of communications made by other users.so that basically the public network used is vulnerable to security attacks. However, using VPN can be a sulution to this problem.

In this research, VPN access is using the the OpenVPN method which uses the SSL encryption protocol by implementing a digital certificate in the client and server connection. The client will perform an attack to test the network security of server connection.the client will perform an attack to test the network security of server using the DDoS tool on Kali Linux. The QoS results will be used as a reference in comparing the level of security on the server.

QoS test results after the attack, the two servers were unable to process data transmission from the client or experienced a downtime due to the DdoS attack which flooded the server computers. The results, 30 packetwere sent from the client did not reach the server. However, when there is no attcak, the number of QoS testing has a different strenght.

Keywords: *OpenVPN, Network Security*

1. PENDAHULUAN

1.1 Latar Belakang

Jaringan publik (public network/ internet) merupakan jaringan yang dapat dilalui oleh siapapun pengguna jasa layanan tersebut. Oleh karena itu, setiap pengguna dapat memanfaatkan kesempatan tersebut untuk melakukan gangguan terhadap privasi komunikasi yang dilakukan oleh pengguna lain, Sehingga pada dasarnya jaringan publik yang digunakan rentan terhadap serangan keamanan.

Setiap pengguna dapat memanfaatkan kesempatan tersebut untuk melakukan gangguan terhadap privasi komunikasi yang dilakukan oleh pengguna lain, seperti pencurian username dan password saat autentifikasi client ke server. Salah satu tantangan yang terjadi menyerang sistem keamanan. Sistem keamanan jaringan bisa secara fisik maupun non fisik. Admin server terkadang mengabaikan aspek-aspek keamanan yang sebenarnya umum diketahui terdapat celah-celah untuk disusupi. Akan tetapi penggunaan VPN dapat menjadi solusi dalam permasalahan tersebut. OpenVPN merupakan salah satu opensource gratis untuk teknologi VPN yang dapat bekerja dibanyak platform. OpenVPN menggunakan protokol enkripsi SSL dengan menerapkan sertifikat digital dalam koneksi client dan server.[1]

Pemilihan Server Debian dan Server Ubuntu sebagai objek yang dibandingkan atau diukur karena menurut sebuah website yaitu www.distrowatch.com kedua server ini merupakan unduhan terpopuler atau bias dikatakan banyak para pengguna atau user yang ingin memasang server dengan menggunakan sistem operasi tersebut. [2]

1.2 Tinjauan Pustaka

Penelitian pertama yang dilakukan oleh Akbar Kurnia Wicaksono (2018) yang berjudul "Implementasi OpenVPN Mobile dan Mikrotik Dial Dengan Autentikasi via Remote Dial-In Service dan Active Radius". Tujuan dari penelitian ini adalah mencegah kebocoran data dengan cara menerapkan Virtual Private Network pada jaringan sebuah perusahaan. Sistem VPN yang telah terintegrasi diharapkan dapat melindungi seluruh data milik perusahaan dari kebocoran. OpenVPN merupakan sebuah aplikasi VPN yang bersifat open source. Hasil dari penelitian ini memberikan keamanan data dari perusahaan dan mengurangi kebocoran data.

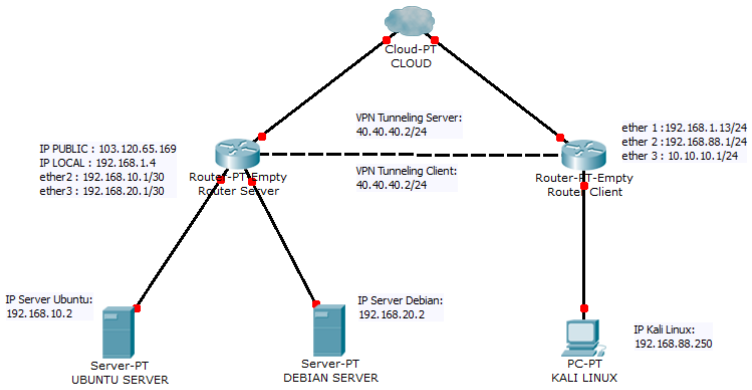
Penelitian kedua yang dilakukan oleh Fahrur Rozy, Yudhi Purwanto, dan Muhammad Iqbal (2012) yang berjudul " Analisis Performasi Jaringan Virtual Private Network (VPN) Berbasis SSL Dengan OpenVPN Ubuntu", dimana betujuan untuk menjaga keamanan data demi mengaman kan privasi komunikasi yang dilakukan pengguna jasa layanan publik dimana telah menjadi priotritas utama bagi peneydia jasa layanan tersebut. Namun keamanan tersebut masih tersebut masih pada akses server, tidak pada jaringanyang dilalui oleh pengguna menuju server. oleh karena itu, VPN akan menjadi salah satu solusi dalam menangani permasalahan keamanan data dalam jaringan. Hasil dari penelitian ini menunjukan VPN-SSL lebih dapat menjaga keamanan data dari ancaman sniffing dan disclosure attack.

2. METODE PENELITIAN

2.1 Desain Simulasi

2.1.1 Topologi

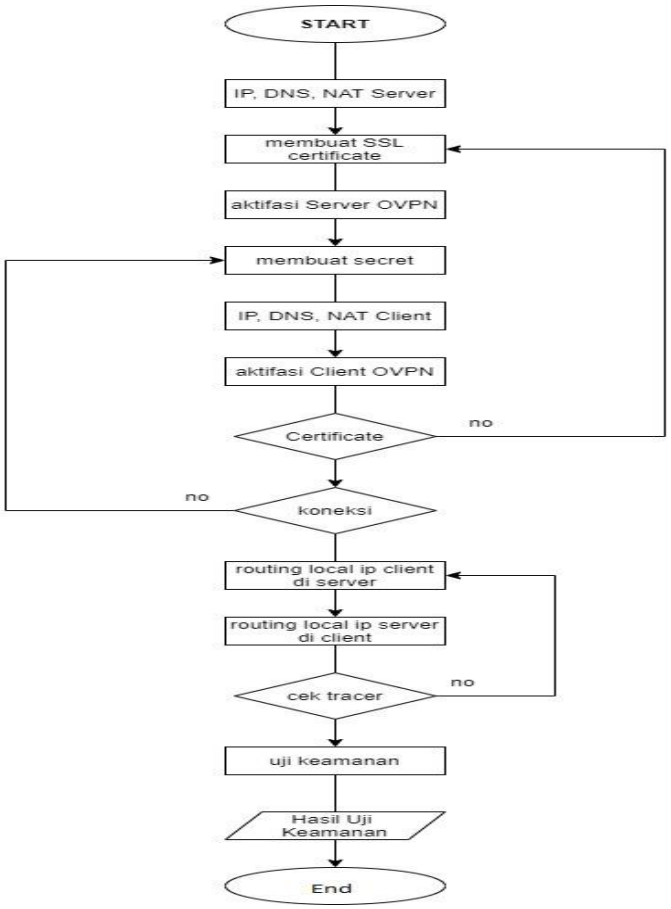
Desain topologi digunakan untuk dapat dijadikan pedoman dalam melakukan implementasi



Gambar 2.1 Topologi

2.1.2 Flowchart Penelitian

Langkah-langkah rancangan penelitian dan pengujian adalah sebagai berikut:



Gambar 2.2 Flowchart

2.1.3 Skema penelitian

Skema penelitian ini dilakukan melalui beberapa tahapan antara lain sebagi berikut:

1. Pembuatan jaringan dasar untuk memberi akses internet pada router-router yang dipakai, komputer server dan juga komputer client. Pemasangan Ip Public pada router server
2. Open VPN, pada konsep implementasinya meliputi pembanguanan OVPN server dan OVPN client, dimana pada kedua sisi dilakukan manajerial jaringan sehingga masing-masing router server dan client dapat berkomunikasi melalui tunneling VPN dan baik

server maupun client harus memiliki sertificate terlebih dahulu untuk autentifikasi.
Tahapan prosedur pembuatan simulasi OVPN adalah sebagi berikut:

a. Konfigurasi ip Address, DNS, Gateway dan NAT di router server.
b. Pembuatan CA certificate, server certificate dan client certificate.
c. Signing all certificate.
d. Pembuatan interface OVPN server.
e. Pembuatan secret OVPN.
f. Deklarasi local IP dan remote IP.
g. Konfigurasi ip Address, DNS, Gateway dan NAT dirouter client.
h. Pembuatan OVPN client
i. Connect to public ip OVPN.
j. Routing ip local client dengan gateway ip tunneling client pada router OVPN server.
k. Routing ip local server dengan gateway ip tunneling server pada router OVPN client.

3. Melakukan pengujian dimana melakukan pengiriman data tahap pertama untuk melihat jumlah troughput, packet loss dan delay sebelum melakukan serangan.
4. Melakukan serangan DDOS dari komputer client ke komputer server. lalu melakukan pengiriman data tahap kedua untuk melihat perbedaan sebelum dan sesudah diserang dari segi troughput, packet loss dan delay.
5. Melakukan perbandingan hasil dari serangan dan pengiriman data pada kedua server, menggunakan hasil dari uji coba yang sudah dilakukan.

2.2 Landasan Teori

Landasan teori yang digunakan dalam penelitian ini adalah sebagai berikut:

2.2.1 Jaringan Komputer

Jaringan komputer adalah jaringan telekomunikasi yang memungkinkan antar perangkat keras aupun perangkat lunak saling berkomunikasi dengan bertukar data.

2.2.2 Keamanan Jaringan

Keamanan jaringan adalah proses untuk mencegah dan mengidentifikasi penggunaan yang tidak sah dari jaringan komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah untuk mengakses setiap bagian dari sistem jaringan komputer. Keamanan jaringan komputer sendiri bertujuan untuk mengantisipasi resiko pada jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer. Secara umum terdapat 3 hal dalam konsep keamanan jaringan,yaitu:

1. Resiko atau tingkat bahaya *(risk).*
2. Ancaman *(threat).*
3. Kerapuhan sistem *(vulnerability).*(Suyuti,2017)

2.2.3 Open VPN

Open VPN adalah aplikasi open source yang mampu memberikan banyak konfigurasi terhadap VPNseperti remote access, site to site VPN, keamananWi-Fi dan remote access berskala enterprise. OpenVPN bekerja dengan cara membuat koneksi Point-to-Point tunnel yang dienkripsi menggunakan Open SSL. OpenVPN menggunakan private keys atau username-password untuk melakukan autentifikasi dalam membangun koneksi. (Wicaksono,2018).

2.2.4 Delay

Delay adalah parameter untuk menilai QOS (Quality of Service) dari sebuah jaringan . Delay atau waktu paket di dalam sistem adalah waktu sejak paket tiba ke dalam sistem sampai paket selesai ditransmisikan. Salah satu jenis delay adalah delay transmisi, yaitu

waktu yang dibutuhkan untuk sebuah pengirim mengirimkan sebuah paket.(Allen,2002).

Untuk menghitung rata-rata delay menggunakan:

$$Delay = \frac{\text{Total } Delay}{\text{Total paket yang diterima}}$$

2.2.5 *Throughput*

Throughput adalah bandwidth aktual atau bandwidth sebenarnya yang terukur pada suatu ukuran waktu tertentu dalam suatu hari menggunakan rute internet yang spesifik ketika sedang mendownload suatu file (Allen,2002).

Untuk menghitung Throughput digunakan persamaan:

$$Throughput = \frac{\text{Jumlah data yang dikirim}}{\text{Waktu pengiriman data}}$$

2.2.6 *Packet Loss*

Packet loss adalah gagalnya proses transmisi data kepada alamat yang ditujukan yang dapat menyebabkan hilangnya beberapa data dalam pengiriman. Umumnya perangkat jaringan memiliki buffer untuk menampung data yang diterima (Allen,2002).

Untuk menghitung Packet loss digunakan persamaan:

$$Packet\ Loss = \left(\frac{\text{data yang dikirim} - \text{paket data yang diterima}}{\text{paket data yang dikirim}}\right) \times 100\%$$

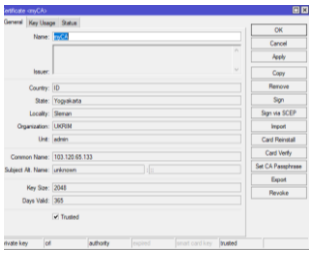
2.2.7 *DDoS Atack*

DDoS atau *Distributed Denial of Service* merupakan jenis *DDoS Attack* yang bekerja dengan melibatkan banyak host penyerang atau dengan komputer yang dipaksa menjadi zombie untuk menyerang sebuah host target dalam jaringan.

2.2.8 *Alur pembuatan Certificate SSL*

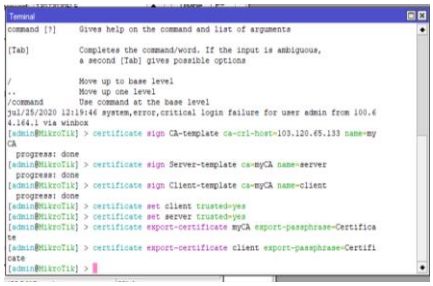
OVPN dapat berkoneksi dengan certificate SSL untuk autentifikasi, adapun pembuatan SSL certificate dapat ilakukan pada mikrotik sebagai berikut:

1. Membuat CA *certificate*, *Server Certificate* dan *Client Certificate* pada *interface system certificate* yang terdapat di router server



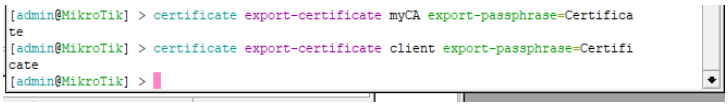
Gambar 2.3 Membuat CA *Certificate*

2. Membuat penandatanganan *certificate* pada terminal mikrotik

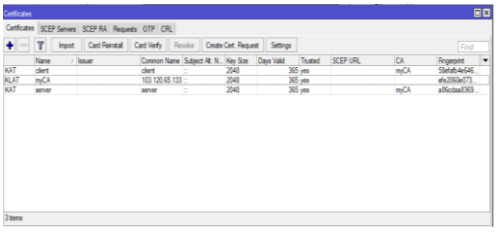


Gambar 2.4. Penandatangan *Certificate*

3. *Export certificate* untuk di importkan nantinya ke router *client*

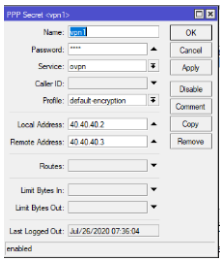


Gambar 2.5 *Export Certificate*



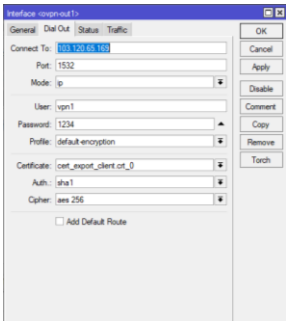
Gambar 2.6. *Certificate* yang dibentuk

2.2.9 Setting OVPN Server



Gambar 2.7. OVPN *server*

2.2.10 Setting OVPN Client

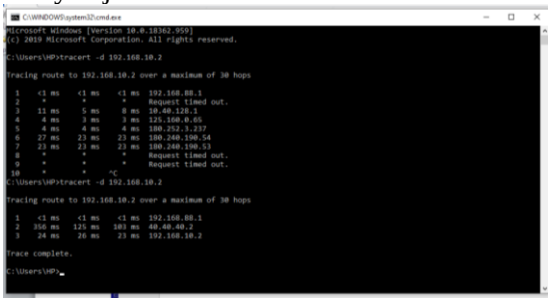


Gambar 2.8. OVPN *Client*

2.3 Pengujian

2.3.1 Pengujian jalur OVPN

Keberhasilan OVPN dapat dilihat melalui jalur yang dilewati komputer *client* menuju ke komputer *server*, dengan menggunakan perintah traceroute –d pada terminal komputer *client*. Gambar 2.9 menampakan kondisi dimana OVPN saat belum berjalan yang menunjukan rute yang dilalui harus melalui banyak jalur dan kondisi dimana OVPN sudah berjalan.



Gambar 2.9. pengujian OVPN

2.3.2 Perancangan keamanan

Konfigurasi keamanan server lewat router dengan membuat rules pada firewall dengan action drop terhadap alamat ip asal penyerang dengan tujuan alamat ip server

```
/ip firewall filter
add chain=forward connection-state=new src-address-list=ddoser dst-
address-list=ddosed action=drop
```

Langkah berikutnya membuat chain baru yaitu *detect-ddos*

```
/ip firewall filter
add chain=forward connection-state=new action=jump jump-
target=detect-ddos
```

Membuat *rule firewall*

```
/ip firewall filter
add chain=detect-ddos dst-limit=32,32,src-and-dst-addresses/1s
action=return
add chain=detect-ddos src-address=40.40.40.2 action=return
/ip firewall filter
add chain=detect-ddos action=add-dst-to-address-list address-
list=ddosed address-list-timeout=10m
add chain=detect-ddos action=add-src-to-address-list address-
list=ddoser address-list-timeout=10m
```

Dengan *rule firewall* diatas, maka ketika terdapat paket *new* yang tidak wajar, misalnya diatas 32 paket selama satu detik, maka *firewall* akan melakukan penandaan terhadap alamat asal dan alamat tujuan menggunakan *address list*. Sebagai contoh untuk alamat IP penyerang maka akan dilakukan *grouping* dengan nama "ddoser", kemudian untuk alamat IP target maka akan dilakukan grouping dengan nama "ddosed".

2.3.3 pengujian keamanan

Pengujian keamanan jaringan pada penelitian ini dilakukan dengan menggunakan DDoS Attack yang merupakan salah satu tool pada sistem operasi Kali Linux. Sebelum melakukan serangan harus melihat kondisi pengiriman paket disaat server belum diserang menggunakan tes ping yang dibatasi hanya melakukan 30 pengiriman data.

```
ping <IP Komputer server>-d 30
```

Pengujian keamaan dilakukan dengan menyerang server, dimana komputer server akan dibanjir banyak paket sebanyak 10000 paket. Adapun perintah DDoS Attack yang diberikan:

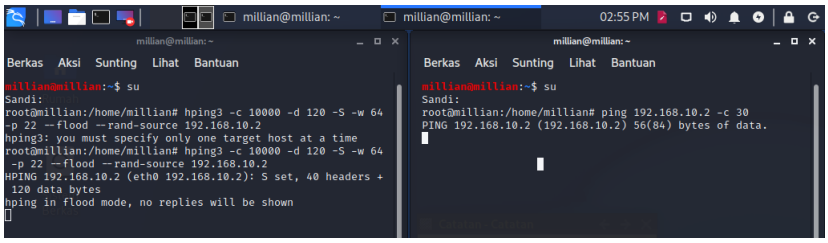
```
hping3 –c 10000 –d 120 –S –w 64 –p 22 --flood –randsource
```

Disaat yang sama komputer client melakukan ping ke komputer server seperti yang dilakukan sebelum penyerangan dimulai. Kemudian dilihat perbedaan yang terjadi sebelum diserang dan sesudah diserang.

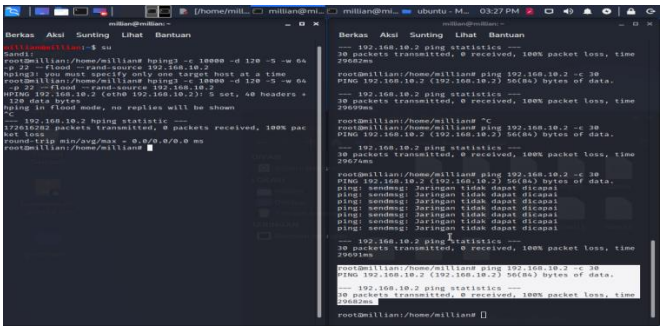
2.3.4 penyerangan pada server

Serangan yang dilakukan pada penelitian ini menggunakan tool DDoS Attack yang terdapat pada Kali Linux. Proses penyerangan pada masing – masing server dikirimkan paket sebanyak 10000, data size 120, winsize menggunakan default 64 dan port 22

1. Serangan DDos pada server Ubuntu

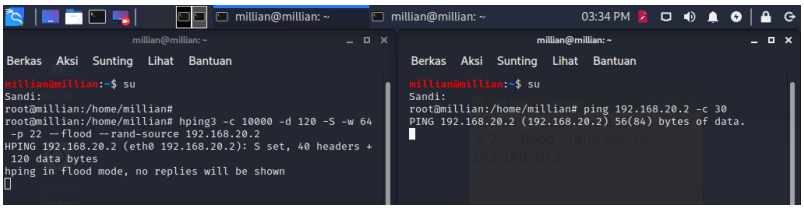


Gambar 2.10. Memulai serangan DDos pada *server* Ubuntu

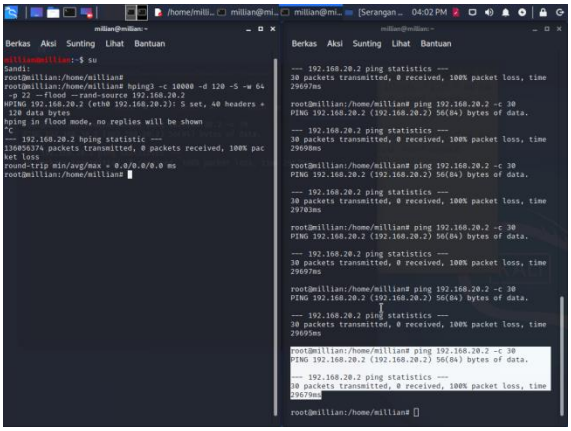


Gambar 2.11. Akhir dari serangan DDos pada *server* Ubuntu

2. Serangan DDos pada server Debian



Gambar 2.12 Memulai serangan DDos pada *server* Debian



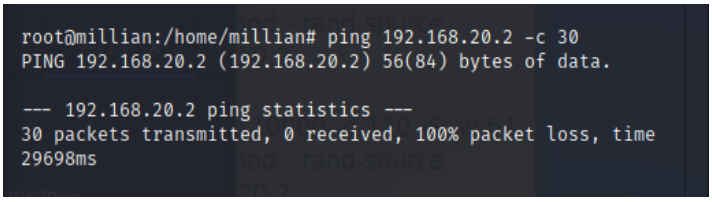
Gambar 2.13 Akhir dari serangan DDos pada server Debian

3. HASIL DAN PEMBAHASAN

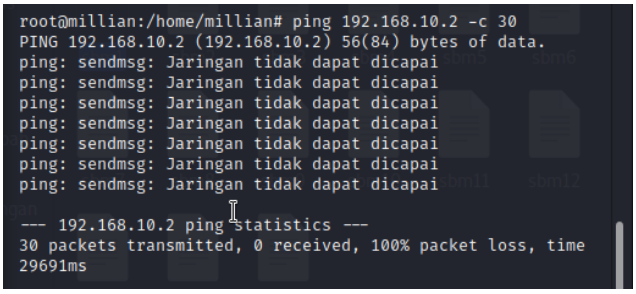
3.1 Hasil

Hasil penelitian didapatkan berdasarkan hasil dari perhitungan QoS dengan menjdaikan beberapa parameter sebagai acuan. Parameter yang digunakan ialah throughput, packet loss dan delay. Hasil perhitungan yang digunakan ialah sesudah penyerangan dilakukan.

3.1.1 Pengujian Setelah Melakukan Serangan



Gambar 3.1. ping *server* Debian setelah penyerangan



Gambar 3.2. ping *server* Ubuntu setelah penyerangan

1. *Packet Loss*

Tabel 3.1 Hasil Pengujian *Packet Loss* setelah penyerangan

PERHITUNGAN PACKET LOSS		
PENGUJIAN	***SERVER* UBUNTU**	***SERVER* DEBIAN**
1	100%	100%
2	100%	100%
3	100%	100%
4	100%	100%
5	100%	100%
6	100%	100%
7	100%	100%
8	100%	100%
9	100%	100%
10	100%	100%
11	100%	100%
12	100%	100%
13	100%	100%
14	100%	100%
15	100%	100%
KETERANGAN	**JELEK**	**JELEK**

2. Throughput

Tabel 3.2 Hasil Pengujian *Throughput* setelah penyerangan

PERHITUNGAN *THROUGHPUT*		
PENGUJIAN	***SERVER* UBUNTU**	***SERVER* DEBIAN**
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
JUMLAH	**0**	**0**
RATA-RATA	**0**	**0**
KETERANGAN	***BAD***	***BAD***

3. Delay

Tabel 3.3 Hasil Pengujian *Delay* setelah penyerangan

PERHITUNGAN *DELAY*		
PENGUJIAN	***SERVER* UBUNTU**	***SERVER* DEBIAN**
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
JUMLAH	**0**	**0**
RATA-RATA	**0**	**0**
KETERANGAN	**JELEK**	**JELEK**

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka dapat ditarik kesimpulan bahwa *Server* Debian dan *Server* Ubuntu memiliki kekuatan yang sama karena pada saat penyerangan dilakukan proses pengiriman paket tidak bisa berjalan atau sering diartikan dengan *server down*. Dan hasil penelitian yang didapatkan sebagai berikut:

1. *Server* manapun bisa terkena serangan ini. DDoS dilakukan oleh seorang penyerang artinya serangan ini memang sengaja dilakukan oleh pihak tertentu.
2. Hasil pengujian QoS sesudah penyerangan kedua *server* tidak bisa melakukan proses pengiriman data dari *client* atau mengalami *down* karena efek dari serangan DDoS yang membanjiri kedua komputer *server*. Hasil pengujian, 30 paket yang dikirim dari *client* namun ke-30 data tersebut tidak bisa diterima oleh komputer *server* dari 15 kali pengujian hasil yang dikeluarkan tetap sama, karena terlalu sibuk dengan serangan dari DDoS. Hasil yang didapatkan untuk *throughput* 0 Mbps, *delay* 0 ms (tidak dapat dihitung karena tidak ada data yang keluar), dan *packet loss* sebesar 100%.

5. SARAN

Saran penelitian yang bisa dikembangkan pada penelitian selanjutnya adalah:

1. Penelitian selanjutnya bisa menggunakan pengiriman data dari client ke *server* lalu melakukan serangan untuk mencari perhitungan QoS.
2. Metode untuk melakukan perbandingan bisa diperbanyak.

DAFTAR PUSTAKA

[1]Rozy, F.2012.Analisa Performasi Jaringan Virtual Private Network (VPN) Berbasis SSL dengan OpenVPN Ubuntu. Jurnal Jaringan Komputer.

[2]www.distrowatch.com

[3]Adriant, F.2015.Implementasi Wireshark Untuk Menyadap(Sniffing) Paket Data Jaringan.

[4]Allen N.2002. network maintenance and troubleshooting guide. Fluke Network. USA.

[5]Bima, A.2016. Pengamanan Virtual Private Network Berbasis OpenVPN dengan Kerbros Pada Ubuntu 14.04 Lts.Jurnal Jaringan Komputer.

[6]Daniel C.2013. *Jitter Visualization, Random Jitter*. UBM tech. San Fransisco.

[7]Husumardiana, D.2016.Analisa packet loss system telemetri pada pengukuran kecepatan angin berbasis x-bee menggunakan Kalman Fileter. Jurnal jaringan Komputer.

[8]Parmo, I. (2008, juni 6). Mengenal Dunia Hacking : Sniffing. Retrieved from isparmo.web.id: http://isparmo.web.id/2008/06/06/mengenal-dunia-hacking-sniffing/

[9]Prabowo, R.2015.Analisis dan Desain Keamanan Jaringan Komputer Dengan Metode Network Development Life Cycle (Studi Kasus : Universitas Telkom).

[10]Suyuti,M.2017.Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter.Jurnal Sistem dan Teknologi Informasi Vol.5, No. 1

[11]Wicaksono, A.2018.Implementasi OpenVPN Mobile dan Mikritik Dial Dengan Autentikasi via Remote Authentication Dial-In Service dan Active Radius.Jurnal Jaringan Komputer.