KELAS	**: JTD - 4D**
NO. ABSEN	**: 07**

USULAN PROPOSAL SKRIPSI

TENTANG

PERBANDINGAN SIMULASI SISTEM KEAMANAN JARINGAN DENGAN KONDISI SESUNGGUHNYA YANG MEMILIKI ANCAMAN *TROJAN*

Diajukan sebagai persyaratan untuk memperoleh gelar
Sarjana Sains Terapan

Disusun oleh :

Eka Saktiawan Prakoso

NIM. 1641160117

PROGRAM STUDI JARINGAN TELEKOMUNIKASI DIGITAL

JURUSAN TEKNIK ELEKTRO

POLITEKNIK NEGERI MALANG

2019

PERNYATAAN

ORISINALITAS SKRIPSI

Saya menyatakan dengan sebenar-benarnya bahwa sepanjang pengetahuan saya, didalam naskah skripsi ini tidak terdapat karya ilmiah yang pernah diajukan oleh orang lain untuk memperoleh gelar akademik di suatu Perguruan Tinggi dan tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip dalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata didalam naskah skripsi ini dapat dibuktikan terdapat unsur-unsur plagiasi, saya bersedia skripsi ini digugurkan dan gelar akademik yang telah saya peroleh (Sarjana Sains Terapan) dibatalkan, serta diproses sesuai dengan peraturan perundang undangan yang berlaku. (UU no 20 Tahun 2003, Pasal 25 ayat 2 dan pasal 70).

Malang, 23 Oktober 2019

Eka Saktiawan Prakoso

NIM. 1641160117

PS. Jaringan Telekomunikasi Digital

DAFTAR ISI

Daftar Gambar

BAB I

Pendahuluan

1.1 Latar Belakang

Dunia maya merupakan suatu tempat untuk dapat mencari informasi dengan mudah. Banyak orang di dunia ini yang sudah mengunakan internet untuk mecari pekerjaan, belajar, dan lain lain. Dengan banyak orang yang menggunakan internet tidak menutup kemungkinan penjahat yang berusaha untuk merugikan orang lain dengan hanya duduk di depan komputer , misalnya mencuri rekening bank, mencuri data pribadi orang lain dan masih banyak lagi.

Objek yang paling banyak diserang oleh yang biasa kita sebut dengan *hacker* ataupun *cracker* merupakan sebuah server – server besar dari perusahaan yang terkemuka contohnya google, facebook dan lain lain. Dari kedua penyerang tersebut yang paling berbahaya adalah *cracker* seseorang yang bukan hanya ingin menyusup atau meretas saja. *cracker* diartikan dengan seseorang yang memiliki kencenderungan untuk merusak sistem atau jaringan komputer yang sudah dia retas. Jadi, *cracker* lebih memiliki niat yang negatif jika dibandingkan dengan *hacker*. Tak jarang, para *cracker* doyan untuk mencomot berbagai informasi rahasia untuk kepentingan yang tidak baik [1].

Keamanan jaringan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah [2]. Untuk itu kita harus membuat harus membuat sebuah sistem keamanan agar untuk menghindari bocornya data pribadi ataupun kehilangan rekening bank. Sebelum membuat sistem keamanan terlebih dahulu untuk memakai simulasi, Karena akan di uji terlebih dahulu dengan *trojan* yang sebenarnya agar lebih aman setelah berhasil. Proses selanjutnya adalah membuat akan membuat sistem dalam keadaan yang sebenarnya menggunakan sebuah router , swicth dan laptop sungguhan.

1.2 Rumusan Masalah

Rumusan masalah dari skripsi ini adalah sebagai berikut :

1. Cara membuat sistem keamanan jaringan yang dapat mengatasi *trojan* tersebut jika sudah terlanjur terinfeksi ?
2. Bagaimana cara mendeteksi dini pada *trojan* tersebut ?
3. Membandingkan antara simulasi sistem keamanan jaringan dengan kejadian yang sebenarnya ?

1.3 Batasan Masalah

Batasan masalah dari skripsi ini adalah sebagai berikut :

1. Jumlah router 2, swict 2 dan komputer 3
2. Menggunakan software GNS3 untuk simulasi
3. Menggunakan *trojan* sebagai bahan untuk menyerang server
4. Menggunakan Software Development Kit MS Visual Basic 6.0

1.4 Tujuan Penelitian

Tujuan dari skripsi ini adalah sebagai berikut :

1. Membuat sistem keamanan jaringan yang lebih minim celah keamanan dari *trojan*
2. Mengetahui karakteristik dari *trojan* itu sendiri
3. Dapat mengatahui seberapa jauh perbedaan antara simulasi dengan keadaan yang sebenarnya

1.5 Manfaat Penelitian

Manfaat penelitian dari skripsi ini adalah sebagai berikut :

1. Dapat membuat perusahaan besar seperti google ataupun perusahaan yang bergerak pada bidang yang membutuhkan internet lebih aman

2. Dapat mengetahui sistem keamanan yang tepat untuk mengatasi *trojan*

1.6 Iuran Penelitian

Luaran Penelitian dari skripsi ini adalah sebagai berikut :

1. Sosialisasi tentang bahaya yang dapat ditimbulkan oleh *trojan* kepada perusahaan *startup*
2. Sumbangan untuk referensi jurnal tentang sistem keamanan terhadap *trojan* untuk perpustakaan polinema

BAB II

Tinjaun Pustaka

2.1 Penelitian Terdahulu

Bagi pembuat program *malware*, sistem operasi Windows masih menjadi 'ladang basah' yang menggoda. Wajar mengingat sistem operasi (OS) buatan Microsoft ini merupakan OS yang paling banyak digunakan di dunia [3].

Lalu bagaimana dengan OS pesaing Windows, yakni macOS? Apple mengklaim sistem operasi andalannya itu aman dari *malware* atau .

Namun, baru-baru ini, sebuah *malware* bernama Mac Dok disebut sebagai *trojan* berbahaya pertama yang dapat menginfeksi laptop atau PC Mac OS.

Adalah peneliti di Check Point yang berhasil menemukan *malware* Mac Dok tersebut. Dikutip dari laman *Ubergizmo*, Selasa (2/5/2017), *malware* ini menyebar menggunakan metode email *phishing*.

Dengan menyamarkan diri di dalam email, pengguna yang tak sadar diminta untuk mengunduh *file* berekstensi ZIP, yang ketika dibuka memungkinkan *malware* tersebut menguasai sistem.

Berhubung *malware* macOS ini 'menempel' di lampiran email, laptop atau PC kamu tidak akan terinfeksi meskipun hanya membuka email. *Malware* baru aktif dan membuat 'lubang belakang' di OS ketika malware tersebut diunduh dan dibuka oleh pengguna.

Para peneliti menghimbau, "Ada baiknya pengguna harus lebih berhati-hati ketika membuka email yang tidak dikenal pengirimnya, apalagi mengunduh *file* yang terlampir dan berpotensi ada *malware* di dalamnya."

2.2 Kajian Teori

2.2.1 Trojan

Trojan Backdoor pada dasarnya adalah *Trojan* (Kuda Troya), Backdoor arti harfiahnya adalah “pintu belakang” maksudnya untuk menguatkan karakter *Trojan* yang bergerak secara tersembunyi dari pintu belakang dan tidak terdeteksi sehingga ia bisa melakukan aktivitas jahatnya dengan leluasa [4].

Biasanya tujuan *Trojan* adalah untuk bercokol di komputer yang diinfeksinya dan melakukan aktivitas jahat seperti mencuri data, melakukan keylogging dan terkadang menjadikan komputer sebagai zombie untuk menjalankan perintahnya.

Trojan horse yang terbaik adalah yang tidak terdeteksi oleh anti karena ia bisa melakukan aktivitasnya jahatnya dengan bebas tanpa disadari oleh korbannya dan mendapatkan keuntungan atas aktivitas tersebut selama mungkin, sekali terdeteksi biasanya *Trojan* horse langsung dibasmi oleh anti dan tidak didiamkan karena akan terus melakukan aktivitas jahatnya jika tidak dimusnahkan.

Asal *Trojan* Backdoor agak sulit dijawab. Apakah maksud Anda negara yang membuat atau siapa yang membuatnya. Pembuat *Trojan* backdoor adalah siapapun yang berkepentingan untuk mendapatkan data dari komputer yang diincarnya dan memutuskan untuk mendapatkan data itu dengan menyebarkan *Trojan*.

Kalau asalnya pada saat ini siapapun yang terhubung ke internet dengan tanpa pengetahuan pemrograman yang tinggi sekalipun bisa membuat dan menyebarkan *Trojan* horse dengan bantuan tools.

Jadi pembuat *trojan* itu bisa script kiddie (promgrammer pemula) sampai dinas rahasia suatu negara bisa membuat malware sejenis *trojan* seperti Uroburos dari Rusia yang berhasil wara wiri selama 3 tahun tanpa terdeteksi dan menjalankan aksinya mencuri data komputer negara musuhnya.

Baidu anti merupakan produk anti gratis yang berasal dari China. Untuk mendapatkan gambaran mengenai performa anti, salah satu sumber independen yang cukup terpercaya adalah Bulletin.

Untuk mengetahui perbandingan performa anti dunia terakhir kamu bisa lihat dari Reactive and Proactive Quadrant Bulletin Award di sini

Saya tidak mengatakan Baidu benar atau Avira yang salah dalam kasus Anda. Untuk mendapatkan gambaran yang lebih obyektif terhadap satu sampel malware kamu bisa mengupload sampel tersebut ke total dimana Total (yang

sudah diakuisisi oleh Google) akan melakukan scanning atas sample yang kamu curigai sebagai malware tersebut dengan 48 merek anti.

2.2.2 GNS3

GNS3 adalah software permodelan yang berbasis *GUI* atau *(Graphical User Interface). Software* ini bisa dibilang gabungan dari *Cisco Paket Tracer* dan *Virtualbox*, akan tetapi *software* ini lebih menggambarkan kondisi nyata dalam mengkonfigurasi *router* langsung dibanding dengan *Cisco Paket Tracer*. GNS3 pun memungkinkan simulasi jaringan yang komplek, karena menggunakan operating system asli dari perangkat jaringan seperti *cisco* dan *juniper* [5].

Prinsip kerja dari GNS3 adalah mengemulasikan *Cisco IOS* pada komputer anda, sehingga *PC* atau *Laptop* anda dapat berfungsi layaknya sebuah atau beberapa *router* bahkan *switch*, dengan cara mengaktifkan fungsi dari *EthernetSwicth Card*. GNS adalah program open source, program ini gratis dan dapat digunakan pada beberapa *Operating System* seperti *Windows*, *Linux*, dan *MacOS X*.

2.2.3 Router

Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau Internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai *routing*. Proses *routing* terjadi pada lapisan 3 (Lapisan jaringan seperti Internet Protocol) dari stack protokol tujuh-lapis OSI.

Gambar 1. Router Mikrotik

Router berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya. Router berbeda dengan *switch*. *Switch* merupakan penghubung beberapa alat untuk membentuk suatu *Local Area Network* (LAN).

2.2.4 Swicth

Switch adalah suatu jenis komponen jaringan komputer yang digunakan untuk menghubungkan beberapa HUB dalam membentuk jaringan komputer yang lebih besar atau menghubungkan komputer-komputer yang memiliki kebutuhan akan bandwidth yang cukup besar [6].

Beberapa fungsi switch yaitu sebagai manajemen lalu lintas yang terdapat pada suatu jaringan komputer, switch bertugas bagaimana cara mengirimkan paket data untuk sampai ke tujuan dengan perangkat yang tepat, Switch juga bertugas untuk mencari jalur yang paling baik dan optimal serta memastikan pengiriman paket data yang efisien ketujuannya.

Switch merupakan *hardware* (perangkat keras) jaringan komputer yang sama dengan HUB, perbedaanya switch ini lebih pintar walaupun harganya sedikit lebih mahalan ketibang HUB. Cara kerja switch yaitu dengan cara menerima paket data pada suatu port lalu akan melihat MAC *(Media Access Control)* tujuannya dan membangun sebuah koneksi logika dengan port yang sudah terhubung dengan node atau perangkat tujuan, sehingga selain port yang dituju tidak dapat menerima paket data yang dikirimkan dan akan mengurangi terjadinya tabrakan data atau disebut dengan *collision*. Setiap perangkat yang terhubung ke port tertentu, MAC addsernya akan dicatat di MAC address table yang nantinya disimpan pada memori chache switch, itulah bagaimana switch bekerja.

Gambar 2. Swicth

2.2.5 Laptop

Laptop atau komputer jinjing adalah komputer bergerak yang berukuran relatif kecil dan ringan, beratnya berkisar dari 1–6 kg, tergantung pada ukuran, bahan, dan spesifikasi laptop tersebut. Sumber daya laptop berasal dari baterai atau adaptor A/C yang dapat digunakan untuk mengisi ulang baterai dan menyalakan laptop itu sendiri. Baterai laptop pada umumnya dapat bertahan sekitar 2 hingga 6 jam sebelum akhirnya habis, tergantung dari cara pemakaian, spesifikasi, dan ukuran baterai. Laptop terkadang disebut juga dengan komputer notebook atau notebook saja.

Sebagai komputer pribadi, laptop memiliki fungsi yang sama dengan komputer desktop (*desktop computers*) pada umumnya. Komponen yang terdapat di dalamnya sama persis dengan komponen pada desktop, hanya saja ukurannya diperkecil, dijadikan lebih ringan, lebih tidak panas, dan lebih hemat daya.

Laptop kebanyakan menggunakan layar LCD (*Liquid Crystal Display*) berukuran 10 inci hingga 17 inci tergantung dari ukuran laptop itu sendiri. Selain itu, papan ketik yang terdapat pada laptop juga kadang-kadang dilengkapi dengan papan sentuh yang berfungsi sebagai "pengganti" tetikus. Papan ketik dan tetikus tambahan dapat dipasang melalui soket Universal Serial Bus maupun PS/2 jika tersedia.

Berbeda dengan komputer desktop, laptop memiliki komponen pendukung yang didesain secara khusus untuk mengakomodasi sifat komputer jinjing yang portabel. Sifat utama yang dimiliki oleh komponen penyusun laptop adalah ukuran yang kecil, hemat konsumsi energi, dan efisien. Komputer jinjing biasanya harganya lebih mahal, tergantung dari merek dan spesifikasi komponen

penyusunnya, walaupun demikian, harga komputer jinjing pun semakin mendekati desktop seiring dengan semakin tingginya tingkat permintaan konsumen.

Gambar 3. Laptop

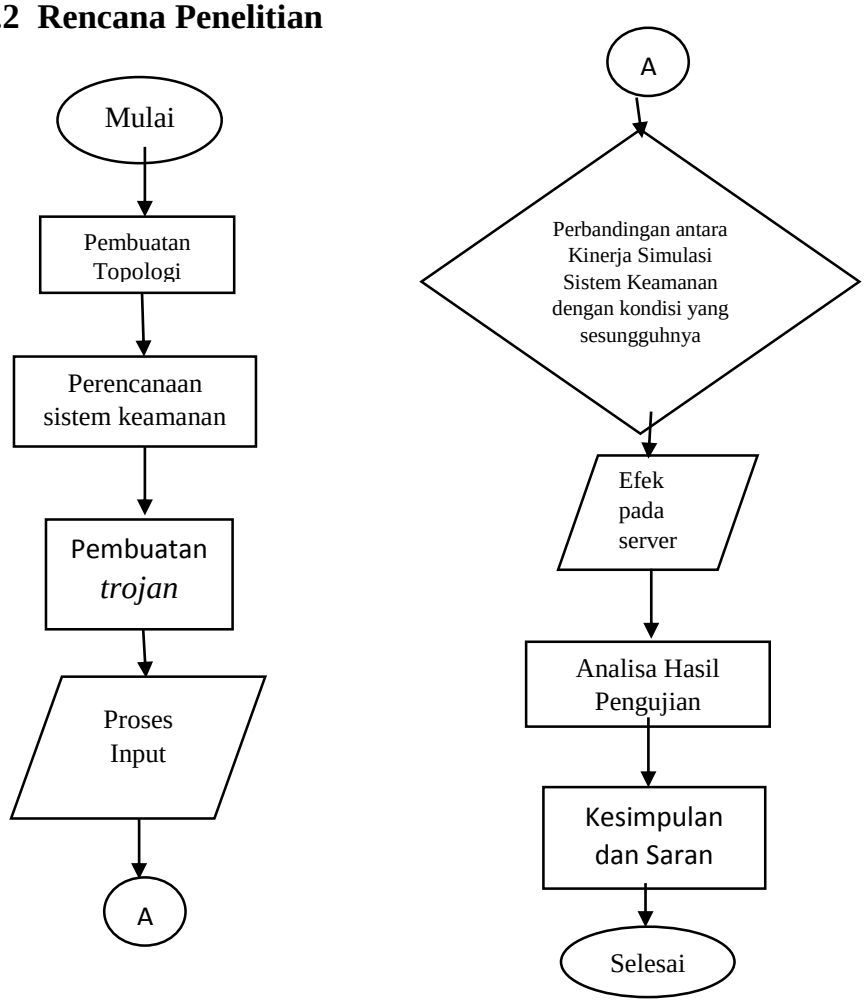
BAB III

Metode Penelitian

3.1 Jenis Penelitian

Metode yang digunakan adalah honeypot yang bekerja dengan menipu penyerang dengan menggunakan server yang palsu, tanpa bisa diketahui bahwa server tersebut juga dapat mengetahui data penyerang yang berhubungan dengan informasi, seperti alamat IP penyerang yang dapat mengetahui menganalisis teknik menyerang, memungkinkan administrator sistem untuk melacak kembali ke sumber serangan jika diperlukan.

4.2 Rencana Penelitian



Gambar 4 Diagram Alir Penelitian

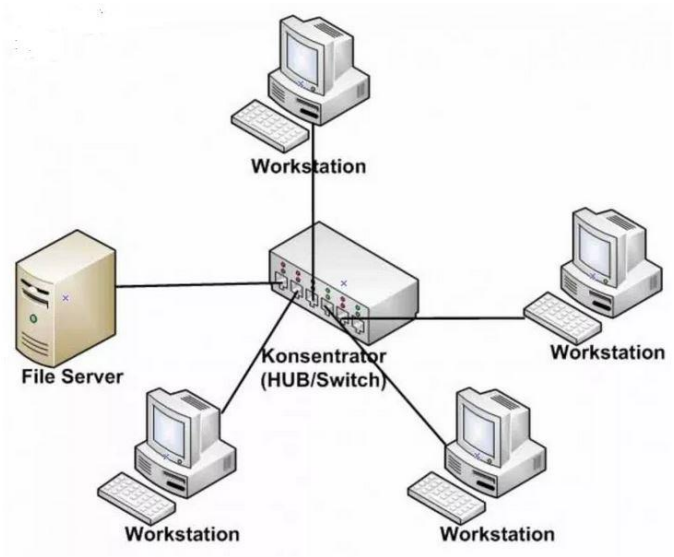
Ditahap penelitian ini yang akan dilakukan dalam pembuatan sistem, dengan penjelasan sebagai berikut :

1. Tahap pertama hal yang dilakukan adalah membuat sebuah topologi Star
2. Tahap kedua membuat progam untuk pengamanan jaringan pada sebuag router
3. Tahap ketiga proses pembuatan
4. Tahap keempat proses bagaimana cara memasukan ke server
5. Tahap kelima pengujian sistem keamana setelah masuk server apakah bisa diamankan baik pada keadaan simulasi atau keadaan sesungguhnya, lalu dibandingkan bagaimana perbedaannya
6. Tahap keenam apa efek yang terjadi pada server, apakah server masih berjalan dengan normal atau tidak
7. Tahap ketuju analisa hasil pengujian pada kedua kondisi pada keadaan simulasi atau keadaan sesungguhnya
8. Tahap kedelapan merupakan sebuah kesimpulan dan saran yang dapat diambil berdasarkan rumusan masalah, pembuatan sistem, serta hasil dan analisa yang telah dilakukan. Sedangkan saran dapat diperoleh dari kekurangan pada pembuatan sistem keamanan apakah dapat ditanbahkan selain *trojan* pada tahap pengujian serangan terhadap server

3.3 Perancangan Alat atau Sistem

Perancangan menjelaskan tentang blok diagram sistem yang digunakan, perancangan sistem dan penjelasan cara kerja sistem yang direpresentasikan ke dalam bentuk flowchart.

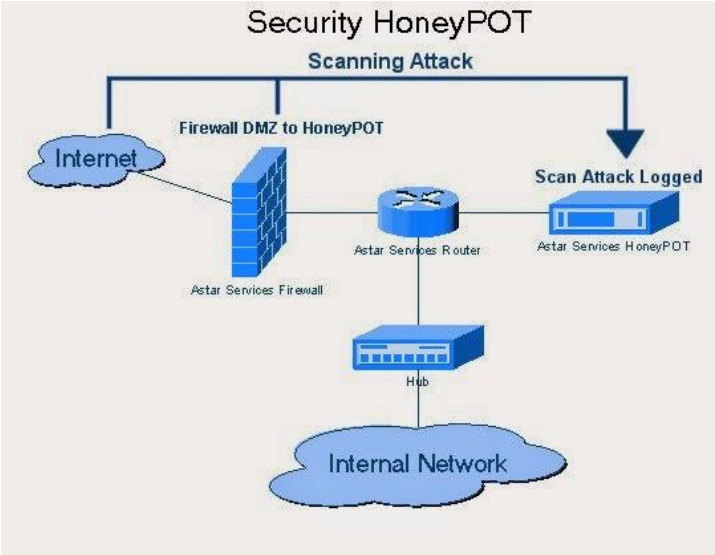
3.3.1 Tahapan Pembuatan Topologi



Gambar 5. Topologi Star

Topologi star merupakan bentuk jaringan yang mana terdapat satu penghubung (Hub/Switch) sebagai pusat dan setiap komputer terhubung ke penghubung tersebut. Hub/Switch ini posisinya ada di central dan berfungsi untuk menghubungkan satu komputer ke setiap komputer yang terhubung dan juga menghubungkan komputer ke File Server.

3.3.2 Pembuatan Sistem Keamanan Jaringan



Gambar 6. Cara kerja HoneyPot

Dari gambar diatas dapat dijelaskan bahwa pertama ada kemungkinan serangan dari lalu akan melewati firewall yang berfungsi untuk memonitring dan mengontrol semua lalu lintas jaringan masuk dan keluar. Lalu dilanjtukan ke sebuah router yang digunakan untuk mengirimkan paket data. Dengan adanya honeypot tidak akan langsung dikirim ke tujuan tapi dilewatkan dulu ke service honeypot untuk mengamati data yang dikirim oleh router aman atau tidak yang bisa disebut juga sebuah sistem yang palsu. Sistem tersebut dibuat agar bertujuan untuk mengelabuhi ha cker ataupun cracker yang dapat berupa dedicated server, virtual server dan lain sebagainya.

3.3.3 Pembuatan *Trojan*

Untuk pembuatannya sendiri kita memakai SDK atau Software Development Kit MS Visual Basic 6.0. Kenapa harus menggunakan Visual Basic, karena sangat popular, maka sangat banyak sumber yang dapat digunakan untuk belajar.

Trojan yang akan kita buat ini nantinya terdiri dari beberapa fungsi atau modul, seperti yang disebutkan di bawah ini:

1. Bisa mengambil informasi, baik ketikan, input atau masukan dari keyboard atau informasi program apa saja yang akan dijalankan oleh user yang telah terinfeksi *Trojan* tersebut. Dalam hal ini Si *trojan* mempunyai tangan untuk mengambil informasi apa saja yang ada di dalam computer korban.
2. Jika sudah bias mengambil informasi, bagian selanjutnya adalah mengirimkan informasi yang telah dikumpulkan ke sebuah web atau ke suatu email. Dalam hal ini *trojan* mempunyai kaki untuk mengantar pesan atau informasi rahasia si pembuat *trojan.*
3. Namanya sebuah program yang dapat mengambil informasi, otomatis kita juga harus tahu tentang apa saja yang dikerjakan oleh si user yang komputernya telah terinfeksi, apakah mereka sedang membuka sebuah program, menyalin file atau membuka file-file video dewasa. Dalam hal ini *trojan* mempunyai mata untuk melihat.
4. Selanjutnya ukuran file *trojan* yang diusahakan sangat kecil, sehingga tidak terlalu menarik perhatian user ketika file tersebut menjadi sangat kecil.
5. Membuat *trojan* mempunyai jadwal untuk membuat aktif hanya bereaksi di waktu tertentu atau *trojan* autorun.

3.3.4 Perbandingan Antara Simulasi dengan keadaan yang Sesungguhnya

Untuk membandingkan antara kedua sistem tersebut, kita harus membuat sebuah topologi yang sama antara simulasi dengan keadaan yang sebenarnya. Dan untuk mengujinya seberapa besar simulasi tersebut dapat menyamai hasil dari sistem yang dibuat dengan router dan switch yang sebenarnya. Apakah data yang dihasilkan simulasi dengan keadaan yang sesunggunhya berbeda jauh atau tidak, ketika hasilnya berbeda jauh apa ada yang salah pengaturan coding antara kedua sistem tersebut.

3.3 Parameter Penelitian

Parameter penelitian yang digunakan adalah sebagai berikut :

1. Pengamatan Bandwith yang keluar dan masuk dari server
2. Perbandingan seberapa jauh perbedaan latency dari hasil antara simulasi dengan keadaan yang sesungguhnya

Daftar Pustaka

[1] Listiorini, "6 Perbedaan Hacker dan Cracker yang Wajib Anda Ketahui," 22 September 2019. [Online]. Available: https://carisinyal.com/perbedaan-hacker-dan-cracker/.

[2] M. Handy Noviyarto, "fasilkom mercubuana," 2016. [Online]. Available: http://www.mercubuana.ac.id.

[3] Yuslianson, "Liputan 6," Liputan 6, 03 Mei 2017. [Online]. Available: https://www.liputan6.com/tekno/read/2938703/peneliti-temukan-malware-*trojan*-pertama-di-macos.

[4] A. Tanujaya, "Inet Detik," Detik, 10 Maret 2014. [Online]. Available: https://inet.detik.com/konsultasi-internet-security/d-2520681/mengenal-lebih-dalam--*trojan*.

[5] A. Ramadhan, "Ardi Hendrawan," 5 September 2015. [Online]. Available: http://ardi17hendrawan.blogspot.com/2015/09/pengertian-gns3-installasi-gns3-dan.html.

[6] S. N, "Pengertian Switch Dan Fungsinya Secara Jelas," Pengertianku, 7 Juni 2015. [Online]. Available: http://www.pengertianku.net/2015/06/pengertian-switch-dan-fungsinya.html.

[7] "Komputer," Wikipedia, 13 Oktober 2019. [Online]. Available: https://id.wikipedia.org/wiki/Komputer.