PENERAPAN IPTABLES FIREWALL PADA LINUX DENGAN MENGGUNAKAN FEDORA

Mizan Syarif Hawari
D3 Manajemen Informatika, Fakultas Teknik, Universitas Negeri Surabaya, mizansyarifhawari@gmail.com

Ibnu Febry Kurniawan
Jurusan Teknik Informatika, Fakultas Teknik, Universitas Negeri Surabaya, ibnufebry@unesa.ac.id

Abstrak

Firewall adalah aplikasi pembatasan paket dalam jaringan. *Firewall* dapat melakukan pemblokiran jaringan paket atau pengaturan *chain* paket jaringan. *IPTables* merupakan salah satu aplikasi yang sudah ada hampir pada semua distribusi linux untuk keperluan *firewall*. *IPTables* dapat melakukan filter terhadap lalulintas data pada komputer pengguna. Pada tugas akhir ini, fitur blok di buat pada *chain forward* dengan mengubah *policy* menjadi DROP, serta membuat 2 *chain* tambahan untuk protokol TCP dan UDP. Hasil dari pengujian ini adalah *iptables* dapat memblokir akses jaringan ke salah satu web dalam protokol HTTP, dan akses ke komputer server online game. Seperti blok web detik.com, *online game* ayo dance dan *online game* steam dota 2.
Kata Kunci : *Iptables, chain, firewall.*

Abstract

Firewall is one of network packet filtering applications. This type of application is able to limit network packet access or packet chain filter. IPtables is one of firewall application that is widely available on almost all Linux distribution. This study attempts to utilize DROP policy on FORWARD chain, and create 2 additional chain for TCP and UDP. Experiments show that IPTables is able to block network access to HTTP website, and online games.
Keywords: *iptables, chain, firewall.*

PENDAHULUAN

Mengatur akses jaringan dan perangkat komputer merupakan faktor yang cukup penting untuk diperhatikan saat ini. Jika beberapa tahun yang lalu mengatur akses jaringan masih sedikit orang yang memperhatikan manfaat dan kegunaannya, namun akhir-akhir ini perilaku tersebut harus segera di perbaiki. Karena akses jaringan, perangkat komputer dan perangkat elektronik lainnya akan meningkat sangat tajam. Hal ini sangat berbeda dengan perkembangan kebutuhan perangkat komputer untuk kehidupan sehari-hari yang juga semakin tinggi. Tidak hanya di dalam kegiatan bisnis dan kehidupan rumah tangga, pendidikan juga sudah membutuhkan jika dilengkapi dengan sebuah komputer. Maka dari itulah, mengapa mengatur akses jaringan komputer menjadi begitu penting untuk diperhatikan saat ini.

Salah satu pelindung yang dibutuhkan untuk mendapatkan akses yang aman ketika berhubungan dengan jaringan komputer, baik dari luar (internet) maupun dari dalam (intranet) dengan cara membuat aturan tertentu pada *firewall*. Salah satu cara *firewall* mengamankan sistem jaringan komputer adalah dengan menerapkan penyaringan port – port web dan game.

Salah satu aplikasi *firewall* yang memiliki fitur untuk dapat melakukannya yaitu aplikasi *iptables* pada linux. Aplikasi iptables merupakan fasilitas *firewall* yang tersedia pada sistem operasi linux.

Tujuan dari penelitian yang berjudul "Penerapan IPTables Firewall Pada Linux Dengan Menggunakan Fedora" yaitu dapat membuat konfigurasi untuk menyamakan port TCP dengan *chain* baru TCP, port UDP dengan *chain* baru UDP serta port TCP dan port UDP dengan *chain* baru TCP dan *chain* baru UDP dengan melakukan blok web dan blok *online game* pada *iptables* linux.

Adapun manfaat yang ingin dicapai dari penelitian yang berjudul "Penerapan IPTables Firewall Pada Linux Dengan Menggunakan Fedora" yaitu dapat memberikan *filtering* terhadap komputer pengguna. *Filtering* pada komputer pengguna antara lain memblok port *online game* dan web yang tidak boleh untuk di buka pada konfigurasi iptables linux Fedora.

Hasil penelitian adalah *iptables* linux Fedora dapat memblokir akses jaringan ke salah satu web dalam protokol HTTP, dan akses ke komputer server online game. Situs yang diblok pada penelitian ini adalah Detik.com, sedangkan online game ialah AyoDance dan Steam Dota 2.

KAJIAN PUSTAKA

Pengertian Jaringan Komputer

Jaringan komputer adalah suatu himpunan interkoneksi sejumlah komputer *autonomous*. Dalam bahasa popular dapat dijelaskan bahwa jaringan komputer adalah kumpulan beberapa komputer (dan perangkat lain seperti *Printer*, *Hub*, dan sebagainya) yang saling terhubung satu sama lain. Melalui media perantara. Media perantara ini bisa berupa media kabel ataupun media tanpa kabel (*Nirkabel*). Informasi berupa data akan mengalir dari satu komputer ke komputer lain, sehingga masing-masing komputer bisa saling bertukar data atau berbagi perangkat keras. (Budi Irawan, 2005)

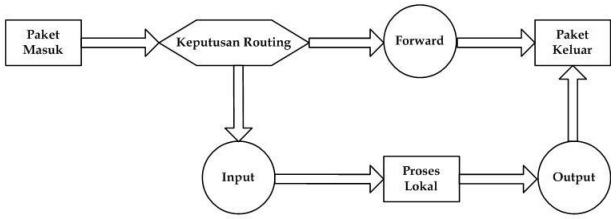
IPTables

Menurut Onno (2008:188) Iptables adalah Firewall, yang default diinstall hampir semua distribusi Linux, seperti, Ubuntu, Kubuntu, Xubuntu, Fedora Core, dan lain. Pada saat menginstall Linux, Iptables memang sudah terinstall, tapi defaultnya mengizinkan semua trafik untuk lewat. Adapun salah satu kelebihan iptables adalah membuat komputer linux menjadi sebuah gateway menuju internet.

Menurut Kai ichinose (2013) iptables adalah suatu tools dalam sistem operasi linux yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalu lintas data. Secara sederhana digambarkan sebagai pengatur lalu lintas data. Dengan iptables inilah akan bisa mengatur semua lalu lintas dalam komputer, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer. IPTables merupakan sistem firewall di sistem open source yang mendukung Layer 3 (Network layer), Layer 4 (Transport layer) dan Layer 7 OSI layer.

Dengan kemampuan tools iptables ini, bisa melakukan banyak hal dengan iptables. Yang paling penting adalah bahwa dengan iptables ini bisa membuat aturan (rule), untuk arus lalu lintas data. Aturan aturan itu dapat mencakup banyak hal, seperti besar data yang boleh lewat, jenis paket/datagram yang dapat diterima, mengatur trafic berdasar asal dan tujuan data, forwarding, nat, redirecting, pengelolaan port, dan firewall.

Iptables menggunakan konsep alamat IP, protokol (TCP, UDP, icmp) dan juga port. Iptables juga menggunakan chain (INPUT, OUTPUT, dan FORWARD) apabila data yang diproses melalui paket ip akan dilewati dalam tabel penyaringan terlebih dahulu.



Gambar 1. Chain IPTables
(Sumber : Skripsi Ahmad Fauzie, 2004)

Pada gambar 1 chain tersebut digambarkan pada lingkaran, jadi saat sebuah paket sampai pada sebuah lingkaran, maka disitulah terjadi proses penyaringan. Chain akan memutuskan nasib paket tersebut apabila keputusannya adalah DROP, maka paket tersebut akan di-drop, tetapi jika chain memutuskan untuk ACCEPT, maka paket akan dilewatkan melalui diagram tersebut.

Firewall

Menurut simarmata (2010:87) Firewall adalah potongan perangkat lunak yang mengatur komunikasi antar jaringan tak aman (insecure), seperti internet dan jaringan aman (secure), seperti LAN perusahaan. Komunikasi ini di atur oleh aturan-aturan akses. Menurut Madcoms (2009:10) Firewall merupakan benteng keamanan dalam internet yang berfungsi melindungi jaringan kecil dari jaringan internet yang luas.

Firewall adalah sebuah sistem yang didesain untuk mencegah akses yang tidak sah ke atau dari jaringan pribadi (Privat Network). Firewall dapat diimplementasikan dalam perangkat keras dan perangkat lunak, atau kombinasi keduanya. Firewall sering digunakan untuk mencegah pengguna Internet. Semua pesan masuk atau keluar dari internet melewati filewall bertindak sebagai pengawas (controller) setiap pesan dan memblok jika tidak memenuhi kriteria keamanan tertentu.

Firewall merupakan perangkat jaringan yang berada di dalam kategori perangkat Layer 3 (Network layer) dan Layer 4 (Transport layer) dari protocol 7 OSI layer. Seperti diketahui, layer 3 adalah layer yang mengurus masalah pengalamatan IP, dan layer 4 adalah menangani permasalahan port-port komunikasi (TCP/UDP). Pada kebanyakan firewall, filtering belum bisa dilakukan pada level data link layer atau layer 2 pada 7 OSI layer. Jadi dengan demikian, sistem pengalamatan MAC dan frame-frame data belum bisa difilter.

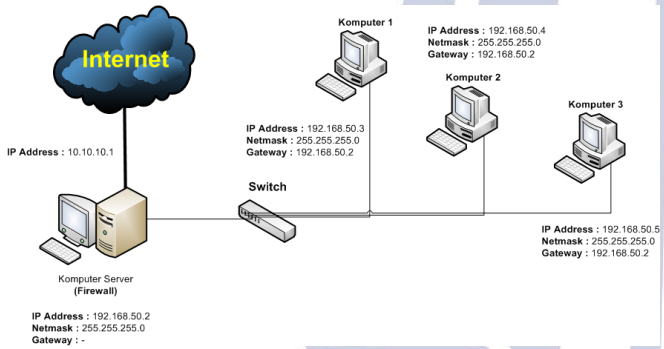
Fungsi firewall sebagai pengontrol, mengawasi arus paket data yang mengalir di jaringan. Fungsi firewall mengatur, memfilter dan mengontrol lalu lintas data yang diizinkan untuk mengakses jaringan privat yang dilindungi.

METODE

Analisis Sistem

Sistem yang akan di buat dalam tugas akhir ini yaitu sebuah sistem *firewall* pada jaringan komputer yang menggunakan *iptables* pada linux Fedora 23. Dengan menggunakan *iptables* pada linux Fedora sebagai sistem pengawasi dan memfilter jaringan komputer. Proses pelaksanaan yang akan dikerjakan yaitu dengan menggunakan *firewall* software yaitu *iptables* linux Fedora 23. Pada *iptables* linux Fedora chain yang di gunakan yaitu forward dengan membuat chain baru yang di beri nama TCP dan UDP. Dengan demikian akan mempermudah dalam mengawasi dan memfilter setiap permasalahan pada jaringan komputer. Berikut arsitektur jaringan yang akan dibuat dalam tugas akhir ini.

a. Topologi *firewall* menggunakan iptables linux Fedora



Gambar 2. Topologi Firewall menggunakan iptables linux Fedora

Berikut penjelasan Topologi *firewall iptables* linux Fedora pada Gambar 2 :

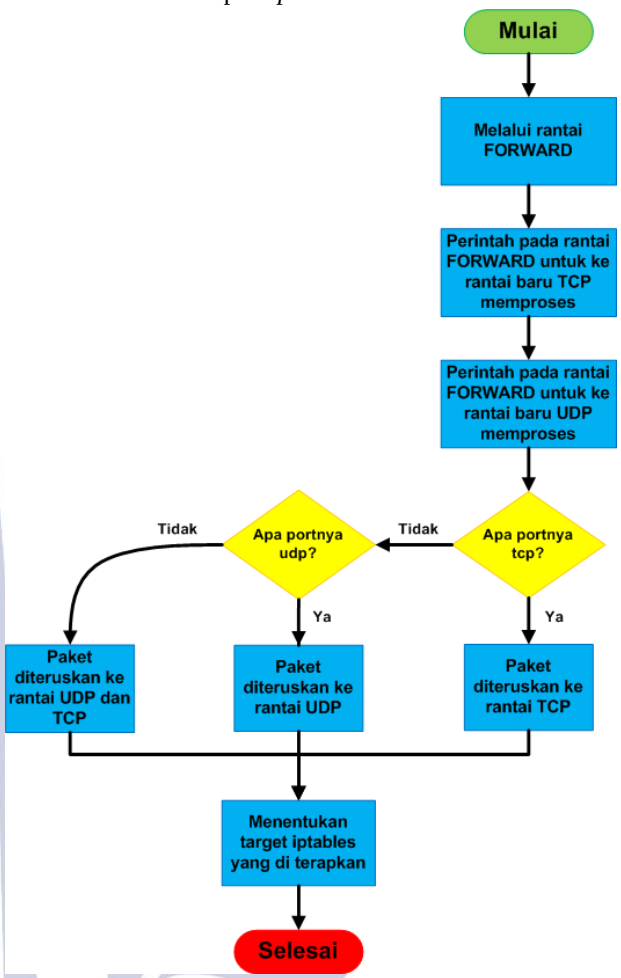
a) Komputer no 1, 2, dan 3
Merupakan alat bantu pengguna untuk mengakses internet.

b) Switch
Merupakan alat untuk menghubungkan antara komputer no 1, 2 ,dan 3 ke komputer server.

c) Komputer Server
Merupakan komputer yang akan di buat untuk mengawasi dan memfilter jaringan komputer no 1, 2 dan 3 dalam tugas akhir ini.

d) Internet
Merupakan jaringan komunikasi global yang terbuka dan menghubungkan miliaran jaringan komputer dengan berbagai jenis dan tipe.

b. Flowchart Penerapan *Iptables* Pada Linux Fedora



Gambar 3. Flowchart *iptables* pada linux Fedora

Berikut Penjelasan Flowchart iptables linux Fedora pada Gambar 3

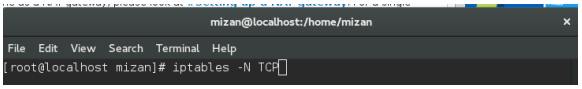
Pada gambar 3 menjelaskan pada proses *iptables* pada linux Fedora bermula dari pengguna komputer no 1, 2 dan 3. Setiap apa saja yang di akses oleh pengguna akan melalui rantai forward pada komputer server yang sudah ada konfigurasi perintah untuk ke rantai baru TCP dan perintah untuk ke rantai baru UDP. Selanjutnya port yang di akses oleh komputer pengguna akan di seleksi. Penyeleksianya yaitu menyamakan port dengan rantai baru, seperti apakah port perintah dari komputer pengguna TCP, jika iya port akan di teruskan ke rantai TCP, jika tidak akan melalui penyeleksian lagi apakah portnya UDP, jika iya port akan masuk ke rantai UDP. Pada penyeleksian akhir jika port perintah dari komputer pengguna TCP dan UDP akan masuk ke rantai TCP dan rantai UDP. Setelah perintah dari komputer pengguna sudah masuk ke rantai baru TCP atau UDP perintah akan di kenakan target yang sudah di terapkan pada konfigurasi di komputer server. Jika sudah di terapkan targetnya semua berhasil dan selesai.

HASIL DAN PEMBAHASAN

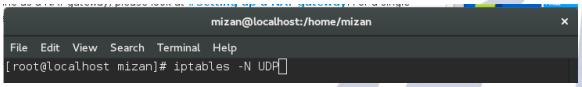
Tahap pengujian dan pembahasan penelitian ini berisi analisa hasil dari pengujian penelitian yang dibuat, berikut analisa hasil dari pengujian sistem**:**

1. **Membuat rantai baru di *iptables***

   Sebelum ke pengaturan blok web, blok *online game* ayo dance dan *online game* steam dota 2. Buat rantai baru di *iptables*. Buat rantai pertama dengan nama TCP dan rantai kedua dengan nama UDP. Berikut hasil gambar membuat rantai baru di *iptables*.



Gambar 4. Perintah untuk membuat rantai baru TCP

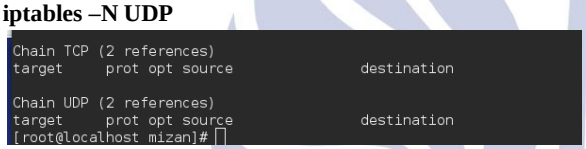


Gambar 5. Perintah untuk membuat rantai baru UDP

Perintah untuk membuat rantai baru dengan nama TCP dan UDP.

iptables –N TCP

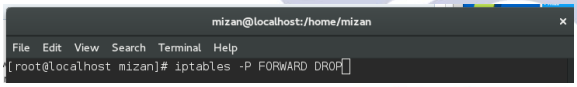
iptables –N UDP



Gambar 6. Hasil membuat rantai baru TCP dan UDP

2. **Mengatur kebijakan rantai**

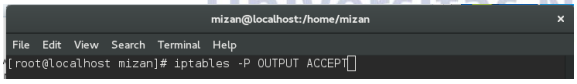
   Setelah membuat dua rantai baru, selanjutnya buat kebijakan pada rantai forward, rantai output, dan rantai input. Berikut hasil gambar mengatur kebijakan rantai.



Gambar 7. Perintah mengatur kebijakan rantai Forward

Perintah membuat kebijakan rantai forward

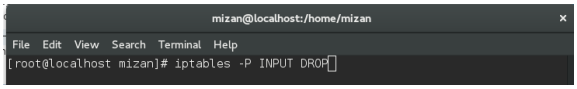
Iptables –P FORWARD DROP



Gambar 8. Perintah mengatur kebijakan rantai Output

Perintah membuat kebijakan rantai output

Iptables –P OUTPUT ACCEPT

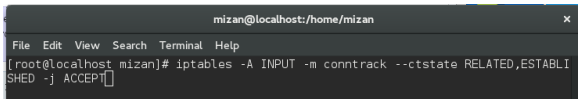


Gambar 9. Perintah mengatur kebijakan rantai Input

Perintah membuat kebijakan rantai output

Iptables –P INPUT DROP

Selanjutnya membuat lalu lintas baru yang berlaku. Pertama menambahkan aturan ke rantai input untuk mengizinkan lalu lintas yang di miliki koneksi yang didirikan.

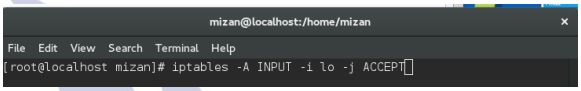


Gambar 10. Perintah mengatur izin lalu lintas yang dimiliki koneksi yang di beri kebijakan rantai Input

Perintah

iptables -A INPUT -m conntrack –-ctstate RELATED,ESTABLISHED -j ACCEP

Selanjutnya yang kedua membuat aturan menerima semua lalu lintas dari loopback.

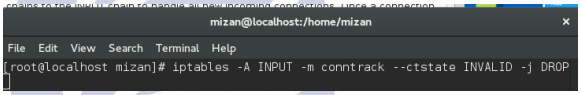


Gambar 11. Perintah menerima semua lalu lintas

Perintah

Iptables -A INPUT -i lo -j ACCEPT

Selanjutnya yang ketiga drop semua lalu lintas dengan header yang tidak valid.

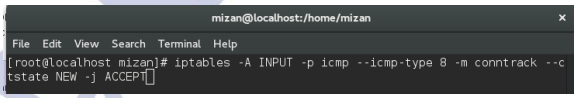


Gambar 12. Perintah drop semua lalulintas dengan header tidak valid

Perintah

iptables -A INPUT -m conntrack --ctstate INVALID -j DROP

Selanjutnya yang ke empat akan menerima permintaan masuk ping.

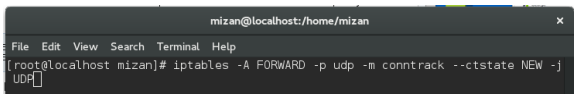


Gambar 13. Perintah menerima permintaan masuk ping

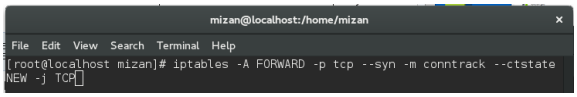
Perintah

iptables -A INPUT -p icmp --icmp-type 8 -m conntrack --ctstate NEW -j ACCEPT

Selanjutnya melampirkan rantai TCP dan rantai UDP ke rantai FORWARD untuk menangani semua koneksi masuk baru.



Gambar 14. Perintah melampirkan rantai UDP di rantai FORWARD



Gambar 15. Perintah melampirkan rantai TCP di rantai FORWARD

Perintah melampirkan rantai UDP di rantai FORWARD pada gambar 14 dan melampirkan rantai TCP di rantai FORWARD pada gambar 15 sebagai berikut.

iptables -A FORWARD -p UDP -m conntrack --ctstate NEW -j UDP

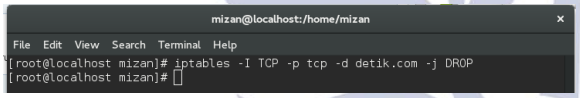
iptables -A FORWARD -p TCP --syn -m conntrack --ctstate NEW -j TCP

UJI COBA

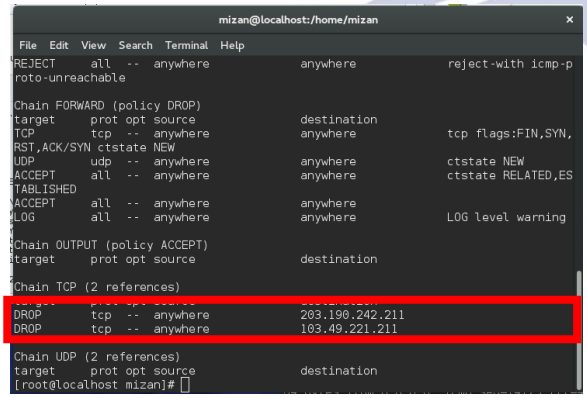
Tahap pengujian dan pembahasan implementasi ini berisi hasil dari instalasi dan konfigurasi yang telah dibuat. Berikut ini hasil pengujian sistemnya.

1. **Pengujian port TCP mengelompokkan pada chain TCP**

   Pertama web detik .com memiliki port TCP untuk di blok dan tidak memiliki port UDP untuk di blok. Berikut hasil pengujian blok web dengan menggunakan salah satu nama web untuk di masukkan dalam pengujian blok ini. Pengujian ini menggunakan nama web **www.detik.com**. Berikut hasil gambar pengujian blok web.



Gambar 16. Perintah IPTables untuk memblokir web

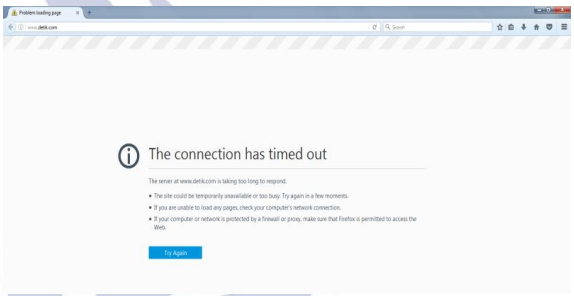


Gambar 17. Tampilan konfigurasi iptables berhasil

Sebelum pc pengguna di blok. PC pengguna masih bisa mengakses www.detik.com .

Gambar 18. Tampilan pc pengguna yang akses di perbolehkan

Sesudah perintah iptables di masukkan dan berjalan. PC pengguna tidak bisa mengakses web www.detik.com .

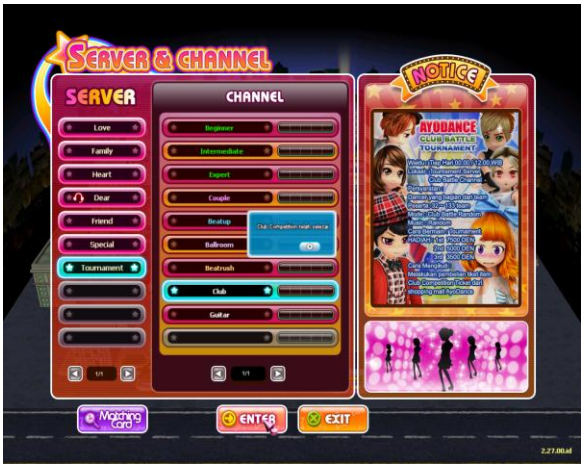


Gambar 19. Tampilan pc pengguna yang tidak di izinkan

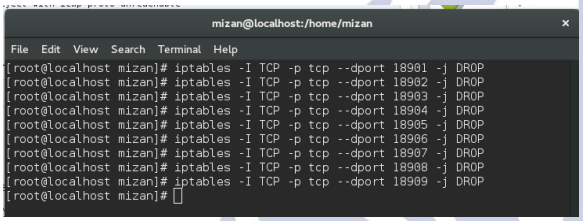
Dari gambar 18 diatas di saat pc server belum memasukkan perintah iptables, pc pengguna masih bisa mengakses web www.detik.com. Di saat pc server memasukkan perintah **iptables –I TCP –p TCP –d detik.com –j DROP** seperti gambar 16 dan perintah berhasil di masukkan seperti gambar 17. Hasil blok web pada pc pengguna berhasil berjalan. Hasil pc pengguna berhasil di blok seperti gambar 19 .

Kedua *online game* ayo dance memiliki port TCP untuk di blok dan tidak memiliki port UDP untuk di blok. Berikut hasil pengujian blok *online game* dengan menggunakan game ayo dance untuk di masukkan dalam pengujian block ini.

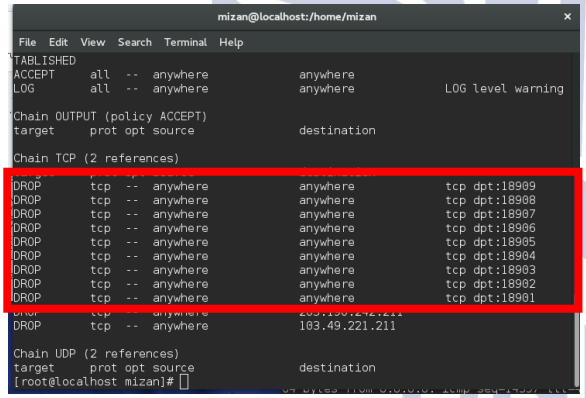
Gambar 20. Tampilan awal masuk game ayo dance



Gambar 21. Tampilan pc pengguna yang akses *online game* di perbolehkan

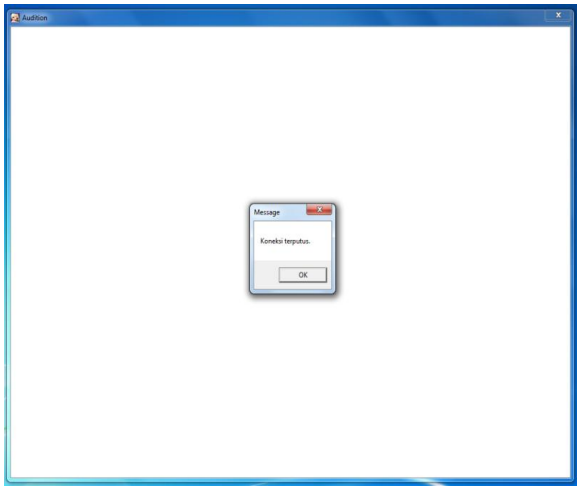


Gambar 22. Perintah IPTables untuk blok *online game* ayo dance



Gambar 23. Tampilan konfigurasi iptables berhasil

Gambar 24. Tampilan awal masuk game ayo dance



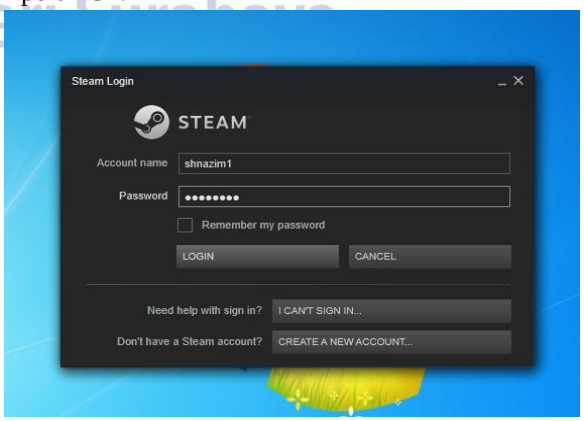
Gambar 25. Tampilan pc pengguna yang akses *online game* ayo dance di blok

Dari gambar 20 dan gambar 21 diatas di saat pc server belum memasukkan perintah iptables, pc pengguna masih bisa mengakses *online game* **ayo dance**. Di saat pc server memasukkan perintah

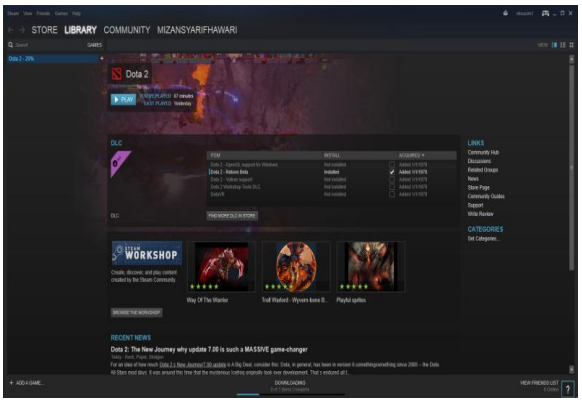
iptables –I TCP –p TCP –-dport 18901 –j DROP
iptables –I TCP –p TCP –-dport 18902 –j DROP
iptables –I TCP –p TCP –-dport 18903 –j DROP
iptables –I TCP –p TCP –-dport 18904 –j DROP
iptables –I TCP –p TCP –-dport 18905 –j DROP
iptables –I TCP –p TCP –-dport 18906 –j DROP
iptables –I TCP –p TCP –-dport 18907 –j DROP
iptables –I TCP –p TCP –-dport 18908 –j DROP
iptables –I TCP –p TCP –-dport 18909 –j DROP

seperti gambar 22 dan perintah berhasil di masukkan seperti gambar 23. Hasil blok *online game* ayo dance pada pc pengguna berhasil berjalan. Hasil pc pengguna berhasil di block seperti gambar 24 dan gambar 25 .

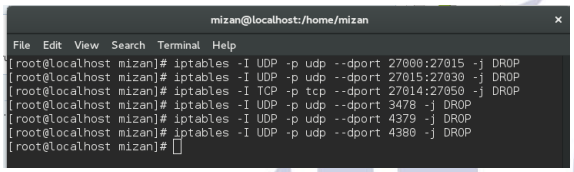
Ketiga game steam dota 2 memiliki port TCP dan UDP untuk di blok. Berikut Hasil pengujian blok *online game* dengan menggunakan game steam dota 2 port TCP.



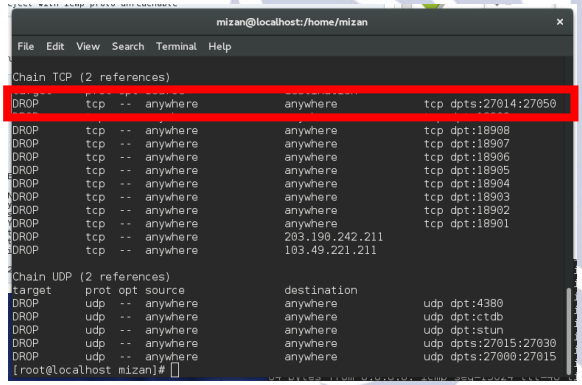
Gambar 26. Tampilan awal masuk game steam dota 2



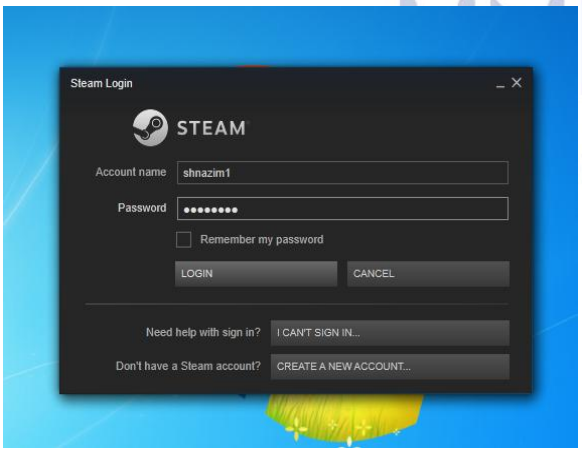
Gambar 27. Tampilan pc pengguna yang akses *online game* steam dota 2 di perbolehkan



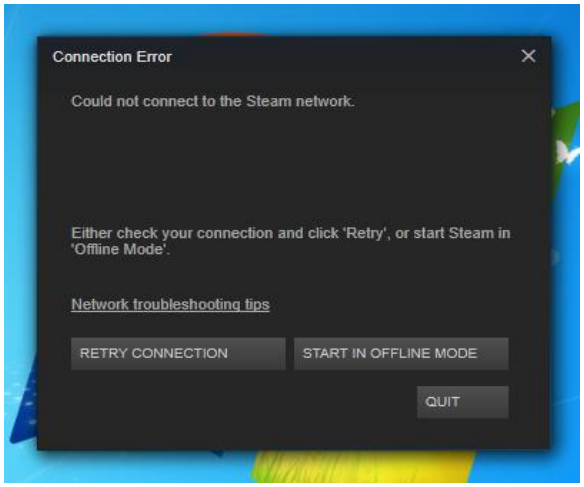
Gambar 28. Perintah IPTables untuk blok *online game* steam dota 2



Gambar 29. Tampilan konfigurasi iptables berhasil



Gambar 30. Tampilan awal masuk game steam dota 2



Gambar 31. Tampilan pc pengguna yang akses *online game* steam dota 2 di blok

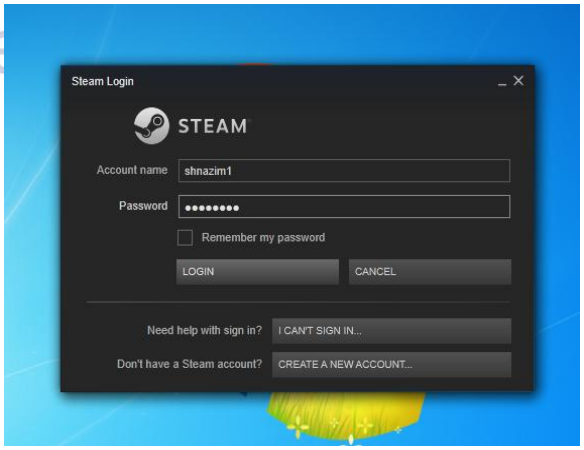
Dari gambar 26 dan gambar 27 diatas di saat pc server belum memasukkan perintah iptables, pc pengguna masih bisa mengakses *online game* **steam dota 2**. Di saat pc server memasukkan perintah

iptables –I UDP –p UDP –-dport 27000:27015 –j DROP
iptables –I UDP –p UDP –-dport 27015:27030 –j DROP
iptables –I TCP –p TCP –-dport 27014:27050 –j DROP
iptables –I UDP –p UDP –-dport 3478 –j DROP
iptables –I UDP –p UDP –-dport 4379 –j DROP
iptables –I UDP –p UDP –-dport 4380 –j DROP

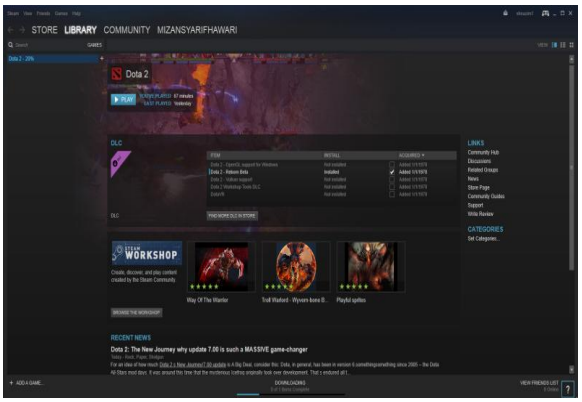
seperti gambar 28 dan perintah berhasil di masukkan seperti gambar 29. Hasil blok *online game* steam dota 2 pada pc pengguna berhasil berjalan. Hasil pc pengguna berhasil di block seperti gambar 30 dan gambar 31 .

2. Pengujian port UDP mengelompokkan pada chain UDP

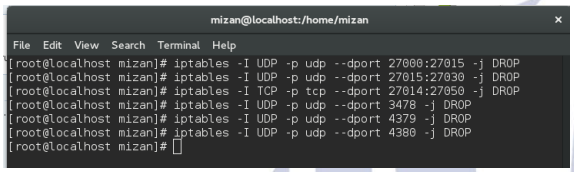
Dalam pengujian ini game steam dota 2 memiliki port TCP dan UDP untuk di blok. Berikut Hasil pengujian blok *online game* dengan menggunakan game steam dota 2 port UDP.



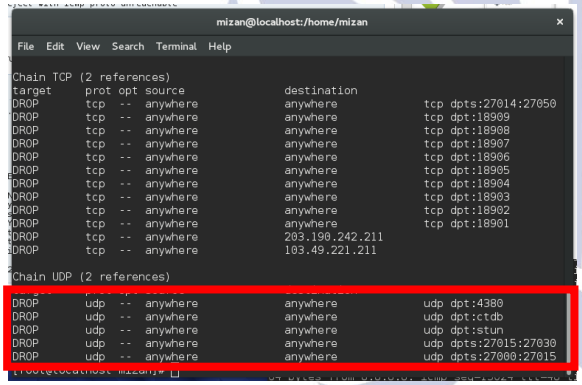
Gambar 32. Tampilan awal masuk game steam dota 2



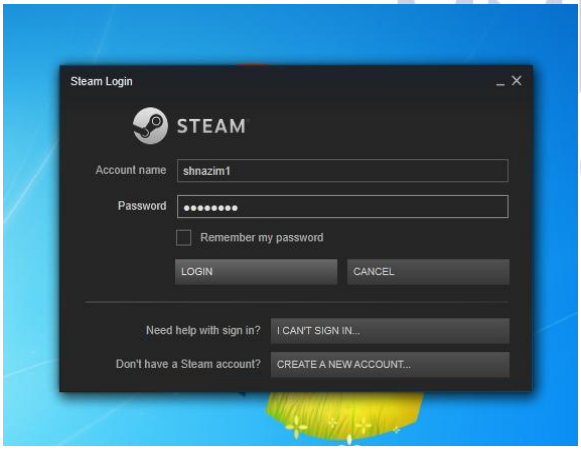
Gambar 33. Tampilan pc pengguna yang akses *online game* steam dota 2 di perbolehkan



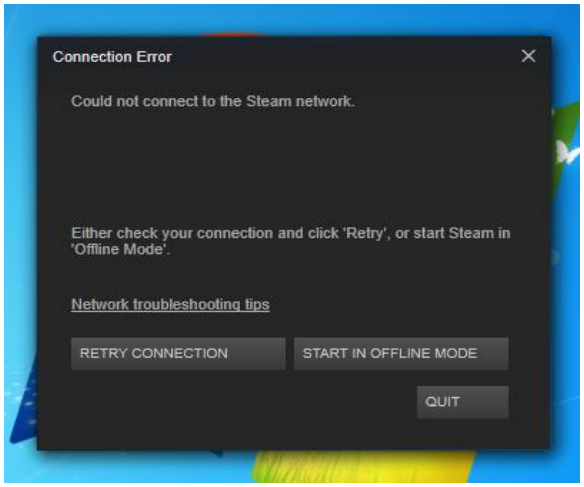
Gambar 34. Perintah IPTables untuk blok *online game* steam dota 2



Gambar 35. Tampilan konfigurasi iptables berhasil



Gambar 36. Tampilan awal masuk game steam dota 2



Gambar 37. Tampilan pc pengguna yang akses *online game* steam dota 2 di blok

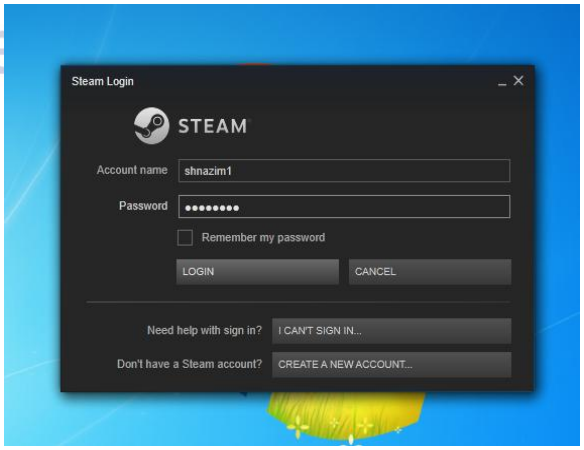
Dari gambar 32 dan gambar 33 diatas di saat pc server belum memasukkan perintah iptables, pc pengguna masih bisa mengakses *online game* **steam dota 2**. Di saat pc server memasukkan perintah

iptables –I UDP –p UDP --dport 27000:27015 –j DROP
iptables –I UDP –p UDP --dport 27015:27030 –j DROP
iptables –I TCP –p TCP --dport 27014:27050 –j DROP
iptables –I UDP –p UDP --dport 3478 –j DROP
iptables –I UDP –p UDP --dport 4379 –j DROP
iptables –I UDP –p UDP --dport 4380 –j DROP

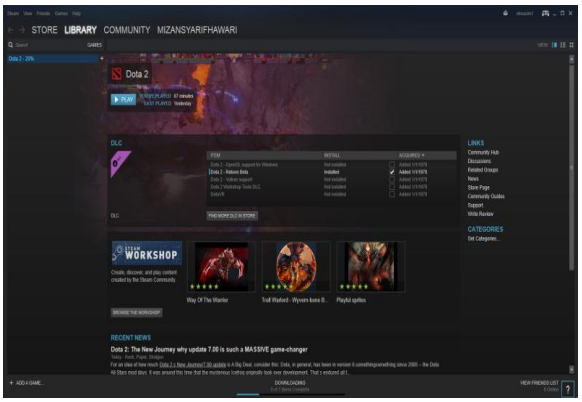
seperti gambar 34 dan perintah berhasil di masukkan seperti gambar 35. Hasil blok *online game* steam dota 2 pada pc pengguna berhasil berjalan. Hasil pc pengguna berhasil di block seperti gambar 36 dan gambar 37 .

3. **Pengujian port TCP dan UDP mengelompokkan pada chain TCP dan UDP**

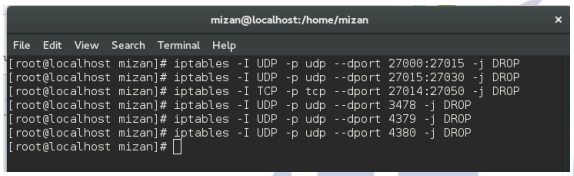
Dalam pengujian ini game steam dota 2 memiliki port TCP dan UDP untuk di blok. Berikut Hasil pengujian blok *online game* dengan menggunakan game steam dota 2 untuk di masukkan dalam pengujian blok ini.



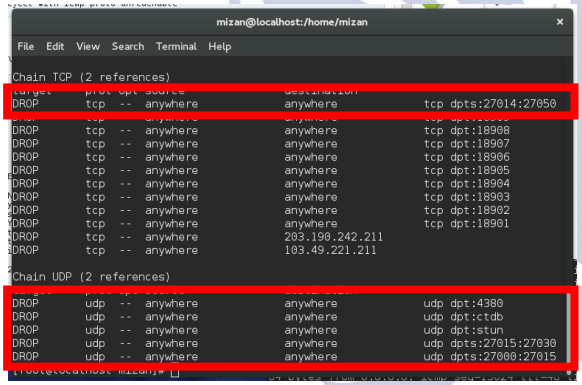
Gambar 38. Tampilan awal masuk game steam dota 2



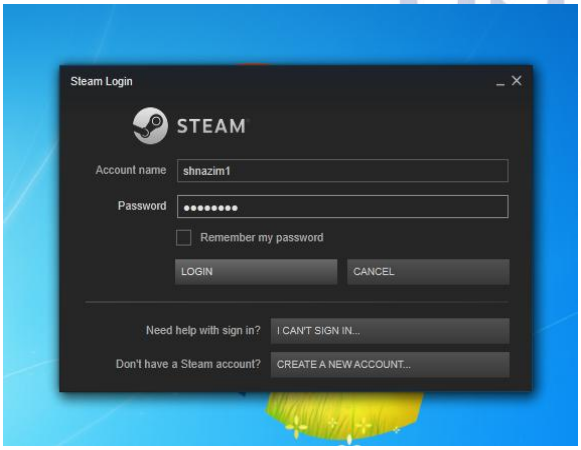
Gambar 39. Tampilan pc pengguna yang akses *online game* steam dota 2 di perbolehkan



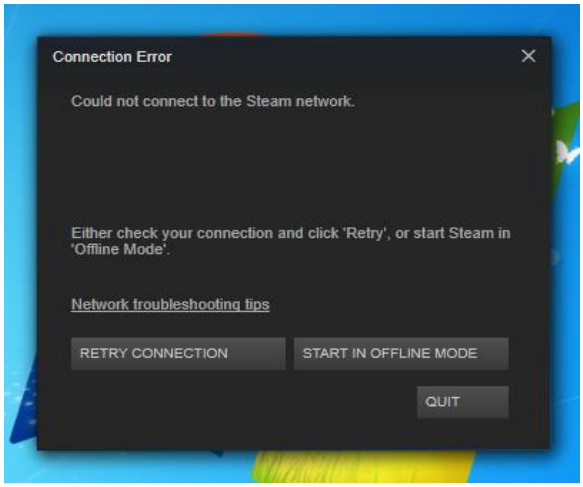
Gambar 40. Perintah IPTables untuk blok *online game* steam dota 2



Gambar 41. Tampilan konfigurasi iptables berhasil



Gambar 42. Tampilan awal masuk game steam dota 2



Gambar 43. Tampilan pc pengguna yang akses *online game* steam dota 2 di blok

Dari gambar 38 dan gambar 39 diatas di saat pc server belum memasukkan perintah iptables, pc pengguna masih bisa mengakses *online game* **steam dota 2**. Di saat pc server memasukkan perintah
iptables –I UDP –p UDP –-dport 27000:27015 –j DROP
iptables –I UDP –p UDP –-dport 27015:27030 –j DROP
iptables –I TCP –p TCP –-dport 27014:27050 –j DROP
iptables –I UDP –p UDP –-dport 3478 –j DROP
iptables –I UDP –p UDP –-dport 4379 –j DROP
iptables –I UDP –p UDP –-dport 4380 –j DROP
seperti gambar 40 dan perintah berhasil di masukkan seperti gambar 41. Hasil blok *online game* steam dota 2 pada pc pengguna berhasil berjalan. Hasil pc pengguna berhasil di block seperti gambar 42 dan gambar 43 .

PENUTUP

Simpulan

1. Membuat konfigurasi port TCP blok web atau blok *online game* di *chain* baru TCP berhasil dalam pengujian ini. Port TCP yang masuk dalam chain TCP yaitu web detik.com, *online game* ayo dance dan steam dota 2.
2. Membuat konfigurasi port UDP blok web dan blok *online game* di *chain* baru UDP berhasil dalam pengujian ini. Port UDP yang masuk dalam chain TCP yaitu *online game* steam dota 2.
3. Membuat konfigurasi port TCP dan UDP blok web dan blok *online game* di *chain* baru TCP dan UDP berhasil dalam pengujian ini. Port TCP dan UDP yang masuk dalam chain TCP dan UDP yaitu *online game* dota 2.

Saran

Iptables pada linux memiliki banyak fungsi yang ber macam-macam sesuai kebutuhan. Dalam laporan tugas akhir ini *iptables* untuk menfilter komputer pengguna dengan membuat table chain baru sendiri, pada pengujian selanjutnya bisa di kembangkan dengan menambahkan marking atau fungsi yang lainya pada *iptables* linux.

DAFTAR PUSTAKA

Amanda, Abdiansyah Rizki. 2014. *Konfigurasi firewall menggunakan metode iptables pada linux ubuntu 12.04*. Tesis tidak di terbitkan

Bambang, Triadi Handaya, Wilfridus, Bernard Renaldy Suteja, Ahmad Ashari. 2015. *Linux System Administrator:* Penerbit Informatika.

Budi Irawan, 2005. *Jaringan Komputer*. Yogakarta: Graha Ilmu.

Farida, Tri. 2016. Implementasi Notifikasi Dengan SMS Pada The Dude Network Monitoring. Tesis tidak di terbitkan. Surabaya: PPs Universitas Negeri Surabaya.

Fauzie, Ahmad. 2004. *Analisis penerapan firewall sebagai sistem keamanan jaringan pada PT. PLN (Persero) penyaluran dan pusat pengaturan beban*. Jakarta. UIN

Ichinose Kai. 2013. *Iptables dan fungsi kode – kodenya*. http://lautankupukupu.blogspot.co.id/2013/01/iptables-dan-fungsi-fungsi-kodenya.html. diakses 18 Desember 2016.

Iksan, Zikhri. 2013. *Program dan struktur dasar system operasi*. http://zicscassanowva.blogspot.co.id/2014/12/sistem-operasi-Fedora-linux.html. diakses 18 Desember 2016

Mahardianto, Himawan. 2015. *Teknik Dasar firewall Dengan IPTables Di Ubuntu Linux Part 2* . http://www.newbienote.com/2015/09/teknik-dasar-firewall-dengan-iptables_27.html. diakses 05 April 2016

Muhar, Syarif. 2008. *Implementasi IPTables sebagai filtering firewall*.

Prasodi, Agung. 2015. *Membuat Jaringan Full Duplex OSPF Wireles Menggunakan Perangkat Mikrotik RB751*. Tesis tidak di terbitkan. Surabaya: PPs Universitas Negeri Surabaya.

Prakoso, Samuel. 2015. *Jaringan Komputer Linux*: Penerbit Andi.

Purbo, W onno. 2008. *Workshop Onno : panduan mudah Merakit Dan Menginstall Server Linux*. Jakarta.

Rusmanto, Henry Saptono, Efrizal Zaida. 2006. Fedora Core 5 Jakarta:Dian Rakyat.

Simamarta, Janner. 2010 *Rekayasa Perangkat Lunak***.** Yogyakarta: Andi.

Sondakh, Glend. 2014. *Perancangan filtering firewall menggunakan iptables di jaringan pusat teknologi informasi Unsrat*. Manado. Unsrat

2014. *Pedoman Tugas Akhir Fakultas Teknik,* Unesa University Press: Surabaya.