ANALISIS KEAMANAN SERVER MENGGUNAKAN IDS DAN ROUTER FIREWALL SERVER DARI SERANGAN DDOS

Disusun dan Diajukan untuk Memenuhi Salah Satu Syarat Guna Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA	**: JUANDA SIDABUTAR**
N.P.M	**: 1614370321**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

ABSTRAK

JUANDA SIDABUTAR

Analisis Keamanan Server Menggunakan IDS dan Router Firewall Server Dari Serangan DDOS

2020

Snort adalah sistem pendeteksi open source yang digunakan untuk memonitor lalu lintas jaringan. Dalam pengembangan snort tidak hanya digunakan sebagai *Intrusion Detection System* (IDS), dengan sedikit pengembangan dan penambahan *netfilter queue* dan *iptables* sehinngga *snort* dapat bekerja dengan sebagai pencegahan. Keterbatasan seorang administrator dalam memonitor server diluar ruangan menjadi snort IDS untuk mendeteksi bila adanya serangan.

Kata Kunci: *Iptables ,Distributed Denial Of Service (DDOS),Snort.*

ABSTRACT

JUANDA SIDABUTAR

Analisis Keamanan Server Menggunakan IDS dan Router Firewall Server Dari Serangan DDOS

2020

Snort is an open source detection system that is used to monitor network traffic. Snort development is not only used as an Intrusion Detection System (IDS), with little development and addition of netfilter and iptables queues so snort can work with prevention. The limitation of the administrator in monitoring the server outside the room is snorting IDS to detect if there is an attack.

Kata Kunci:*Iptables,Distributed Denial Of Service (DDOS), Snort.*

DAFTAR GAMBAR

Halaman

DAFTAR ISI

Halaman

BAB III METODE PENELITIAN

BAB IV IMPLEMENTASI DAN HASIL

DAFTAR TABEL

Halaman

KATA PENGANTAR

Puji syukur Tuhan yang Maha Esa karena dengan berkat dan kasih anugerah-Nya penulis masih diberikan kesehatan sehingga akhirnya penulis dapat menyelesaikan Skirpsi dengan judul : **"ANALISIS KEAMANAN SERVER MENGGUNAKAN IDS DAN ROUTER FIREWALL SERVER DARI SERANGAN DDOS".**

Dalam penyusunan Skirpsi ini penulis menyadari banyak mengalami kesulitan namun berkat bantuan dan dorongan dari berbagai pihak, akhirnya Skirpsi ini dapat juga diselesaikan. Penulis dengan segala kerendahan hati menyampaikan terima kasih kepada:

1. Ayah dan Ibu beserta keluarga yang telah berjasa dalam memberikan dukungan moril dan materil.
2. Bapak H.M. Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Rektor I, Bapak Ir. Bhakti Alamsyah, M.T, Ph.D
4. Bapak Hamdani, ST., MT, selaku Dekan Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan
5. Bapak Eko Hariyanto, S.Kom., M.Kom, selaku Ketua Program Studi Sistem Komputer Fakultas Sains Dan Teknologi Universitas Pembangunan Panca Budi Medan.
6. Dosen Pembimbing 1, Bapak Dian Kurnia S.Kom.,M.Kom
7. Dosen Pembimbing 2, Bapak Hafni S.Kom.,M.Kom
8. Seluruh Dosen dan Staf Pegawai Fakultas Sains Dan Teknologi yang telah banyak membantu dalam kelancaran seluruh aktivitas perkuliahan.
9. Staf Perpustakaan Universitas Pembanguan Panca Budi yang telah berjasa memberikan pinjaman buku-buku yang ada.
10. Teman-teman yang telah memberikan berbagai saran, inspirasi, dorongan, doa, motivasi dan moril maupan materil yang diperlukan sehingga penulis dapat menyelesaikan Skirpsi ini.

Penulis juga menyadari bahwa penyusunan Skripsi ini belum sempurna baik dalam penulisan maupun isi disebabkan keterbatasan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang membangun dari pembaca untuk penyempurnaan isi Skripsi ini.

Medan, Juni 2020
Penulis,

JUANDA SIDABUTAR
NPM : 1614370321

BAB I

PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi internet membawa dampak positif untuk berbagai industri, perkembangan ini dapat membantu pertumbuhan industri, dan seiring berkembangnya teknologi komputer, komputer tidak luput dari suatu-suatu serangan atau kejahatan sistem diluar kendali firewall yang dapat memantau kejahatan atau serangan diluar kendali dari pemilik komputer tersebut.

Ada beberapa cara untuk menanggulangi serangan *cyber*, yang pertama adalah dengan menggunakan *Intrusion Detection System* (IDS) dan yang kedua dengan menggunakan *Router Firewall Server*. IDS merupakan salah satu komponen keamanan jaringan yang melindungi data dan informasi keamanan, dengan memantau lalu lintas pada paket data untuk mendetesi intrusi. IDS berfungsi untuk melindungi sistem komputer dengan mendeteksi dan mendiagnosis semua aktivitas berupa pelanggaran integritas sistem maupun hak akses. *Router Firewall* merupakan sistem yang bekerja untuk filter semua lalu lintas paket dan menganalisanya dengan mengizinkan atau memblokir lalu lintas berbahaya dari port atau aplikasi.

DDOS *(distributed denial of service)* adalah jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (*resource*) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung

mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang tersebut.

Pada penelitian ini, penulis memanfaatkan serangan DDOS untuk melihat sejauh mana pengukuran dari kinerja dari keamanan data dari suatu simulasi *web server* yang kita buat pada OS Ubuntu *Server*. Penulis mencoba melakukan serangan DDOS terhadap *server* yang akan dibangun dan akan dilakukan dengan menggunakan beberapa *host* agar dapat memaksimalkan pengujian serangan terhadap *web server* ini dan mengetahui ketahanan *server* dari serangan DDOS. Maka dari itu penulis tertarik mengajukan skripsi dengan judul: **"Analisis Keamanan *Server* Menggunakan IDS Dan Router *Firewall Server* Dari Serangan DDOS".**

1.2 Rumusan Masalah

Setelah menguraikan latar belakang di atas maka dapat disimpulkan masalah yang akan di selesaikan yaitu sebagai berikut:

1. Bagaimana cara memberikan *alert* saat ada serangan *DDOS* di *web server* ?
2. Bagaimana kinerja *web server* saat normal dan saat ada serangan yang menuju ke *server*?
3. Bagaimana pengaruh *router firewall* pada topologi jaringan yang dirancang ?

1.3 Batasan Masalah

Agar penelitian mendapatkan hasil yang di inginkan sesuai dengan rencana, Berikut adalah batasan masalah yang akan dibahas dalam penelitian ini, yaitu:

1. Dalam melakukan remote ke *server* hanya menggunakan *software snort* sebagai *instrusion detection system* (IDS).
2. Serangan yang di ambil adalah menggunakan jenis serangan *ping of the dead*.
3. Operasi sistem yang akan digunakan yaitu ubuntu server 12.04.5
4. Pengujian serangan menggunakan *firewall*
5. Membangun anti DDOS untuk paket ICMP (Internet Control Message Protocol)

1.4 Tujuan Penelitian

Ada pun tujuan penelitian ini adalah sebagai berikut:

1. Tujuan penelitian ini memberikan *alert* berupa *console* pada saat ada serangan *DDOS (Distributed Denial of Service) attack.*
2. Mengidentifikasi adanya serangan *DDoS* pada *web server* dengan *intrusion detection system* dan *router firewall server.*
3. Mengetahui bagaimana kinerja server saat keadaan server normal dan saat ada serangan.

1.5 Manfaat Penelitian

Berikut adalah manfaat penelitian:

1. Membangun *intrusion detection system* dapat mencegah kerugian akibat serangan yang terjadi membuat *server down*.
2. Mengetahui kinerja *server* yang sedang berjalan agar dapat memberikan layanan yang baik kepada *client.*
3. Mengetahui menajemen jaringan internet yang terhubung yang dilakukan dengan baik dan efisien.

BAB II

LANDASAN TEORI

2.1 Pengertian Keamanan Jaringan

Keamanan jaringan adalah proses mencegah dan mengidentifikasi pengguna yang tidak sah dari komputer yang bertujuan untuk mengantifikasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logik. Ancaman fisik adalah seseorang pengganggu yang berniat untuk merusak bagian fisik komputer sedangkan ancaman *logic* adalah ancaman yang berupa pencurian data atau pembobolan terhadap akun seseorang.

Keamanan biasanya diartikan sebagai suatu yang bebas dari bahaya dan bagaimana menjadikan suatu hal bebas dari bahaya ataupun ancaman dari berbagai hal, keamanan juga termasuk hal yang luas.

Keamanan jaringan dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan dari kelima point ini.

Keamanan komputer adalah berhubungan dengan pencegahan dini dan deteksi terhadap tindakan pengganggu yang tidak dikenali dalam sistem komputer yang mana sistem bekerja sesuai dengan yang diperintahkan oleh pengguna komputer tersebut dan keamanan komputer juga bergantung pada sistem yang dibangun (Muhammad Suyuti Ma’sum, 2017).

2.1.1 Aspek-Aspek Keamanan Jaringan komputer

Ada beberapa aspek keamanan jaringan komputer harus dilindungi dan dijaga dari orang yang tidak bertanggungjawab, yaitu :

1. *Privacy*

   Dengan menjaga informasi tentang jaringan komputer yang kita punya agar tidak bisa di akses oleh orang lain dan orang lain tidak bisa melihat data-data kita.

2. *Integrity*

   Integrity adalah informasi yang tidak boleh diubah tanpa seijin pemilik informasi, contohnya seperti e-mail yang di *intercept* dan diubah isinya kemudian diteruskan ke alamat awal yang dituju.

3. *Authentification*

   Authentication ini memberikan keyakinan bahwa informasi yang dimiliki masih benar-benar asli, atau orang yang mengakses informasi itu benar-benar mendapat informasi yang memang miliknya tanpa diubah oleh orang lain.

4. *Availibility*

   Dibagian ini dimana ketersediaan informasi ketika dibutuhkan, dan ketika ada hambatan contoh nya diserang oleh *denial of servive attack (DoS Attack)*. Dimana *server* dikirim permintaan yang diluar perkiraan sehingga server tidak dapat melayani permintaan lain bahkan sampai server *hang, down, crash.*

5. *Access control*

   Accses control adalah pemberi ijin terhadap sebuah ojek tertentu secara spesifik. Akses control sendiri membatasi orang orang yang akan mengakses objek tersebut. Tanpa adanya akses control, kemungkinan sesuatu (termasuk data) dapat di curi lebih meningkat. (Cindy Nataliana, 2019).

2.1.2 Syarat-Syarat Keamanan Jaringan

Ada beberapa syarat keamanan jaringan yang bisa diterapkan untuk mengurangi adanya ancaman, yaitu:

a. *Prevention*

   Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi *snort* IDS yang berjalan dengan hati-hati.

b. *Observation*

   Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. *System IDS* dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi *log* yang disediakan.

c. *Response*

   Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu sistem telah berhasil disusupi,maka personil perawatan harus segera

mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi *system* dan apabila di -*shutdown* akan menyebabkan lebih banyak kerugian daripada membiarkan sistem yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu sistem telah berhasil disusupi dari luar.(Fuad Jauhari, 2008).

2.2 Pengertian *Server*

Server merupakan sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer. *Server* tersebut didukung dengan prosesor yang bersifat *scalable* dan RAM yang besar, dan juga dilengkapi dengan sistem operasi khusus, yang disebut dengan sistem operasi jaringan.

Server juga menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya, seperti halnya berkas atau alat pelacak (*printer*), dan memberikan akses kepada *workstastion* anggota jaringan (Indrat Susilo dan Gesang Kristiyanto Nugraha, 2012).

2.2.1 Jenis-Jenis *Server*

Ada beberapa jenis *server* yang banyak digunakan antara lain sebagai berikut :

1. *Web server*

   Web server adalah sebuah perangkat lunak yang dipasang pada *server* yang berfungsi untuk menyediakan layanan permintaan data dengan *protocol* https atau http yang dapat diakses dengan menggunakan *browser*.

2. *Proxy server*

   Proxy server adalah sebuah server yang dapat berfungsi sebagai komputer lainnya untuk melakukan permintaan dari sebuah intranet atau internet.

3. *Domain Name Server* (*DNS*

   Server ini berfungsi untuk menerjemahkan informasi nama *host* atau domain menjadi sebuah alam at Internet *Protocol* (IP).

4. *Database server*

   Sebuah layanan untuk menyimpan database server biasanya 3306 (*Mysql)* dan 5432 (PqSQL).

5. *Mail server*

   Mail server memiliki fungsi untuk melayani *client* khususnya dalam hal mengirim surat.

6. *File Transfer Protocol (FTP) server*

   Server ini memiliki *protocol* FTP yang dapat dilakukan sebagai i untuk transfer data.

7. *Fax server*

   Server ini digunakan untuk melayani kebutuhan *fax* bagi *client* dan membuat sistem penerimaan dan pengiriman *fax* dengan menggunakan modem.

8. *File server*

   File server merupakansebuah komputer yang berfungsi untuk menampung sejumlah data yang dimiliki oleh *client* yang bersangkutan.

9. *Print server*

   Print server merupakan sebuah pusat layanan untuk kegiatan percetakan atau *print* untuk *client* (Habib Ahmad Purba, 2010).

2.2.2 Fungsi *Server*

Adapun secara umum fungsi *server* adalah sebagai berikut :

a. Menyediakan beraneka macam *resources* sehingga bisa dimanfaatkan oleh komputer klien yang terhubung dengan jaringan
b. Melayani permintaan data dari komputer klien
c. Menyimpan berbagai data dan file yang nantinya bisa diakses bersama-sama oleh komputer kilen menggunakan protocol FTP
d. Mengatur lalu lintas data

e. Menyediakan aplikasi maupun database yang bisa dijalankan oleh semua komputer klien yang terhubung ke jaringan

f. Mengatur hak akses komputer klien di dalam semua jaringan

g. Melindungi komputer klien dengan menyediakan layanan anti *malware* maupun pemasangan *firewall* di komputer klien (DimensiData, 2017).

2.2.3 Cara Kerja *Server*

Adapun cara kerja *server* adalah untuk memenuhi permintaan *client*. Misalnya pada *web server*, ketika mengakses sebuah alamat *website* menggunakan browser, maka komputer yang dipakai berperan sebagai komputer klien dan komputer kilen meminta informasi *website* kepada *web server*. *Web server* kemudian akan mengirimkan informasi atau data berupa *website* ke komputer sesuai dengan permintaan sehingga isi halaman *website* bisa diakses.

Cara kerja *server* jenis lainnya sedikit berbeda, namun prinsipnya tetap sama yakni melayani permintaan data dari klien yang terhubung dalam satu jaringan. Namun jenis permintaan data maupun informasi yang diminta klien berbeda sesuai dengan jenis *server* nya (Hermawan, 2013).

2.3 Ubuntu *Server*

Ubuntu *server* adalah ubuntu yang didesain untuk di install di server. Perbedaan mendasar, di ubuntu *server* tidak tersedia GUI.Jika anda menggunakan ubuntu *server* artinya harus bekerja dengan perintah di layar hitam yang disebut konsole.

Penggunaan Ubuntu *Server* sudah termasuk dalam *linux Stable*, intinya pada *linux* bila dipakai untuk *server proxy* pun akan berjalan stabil dan untuk pemasukan aplikasi-aplikasi di dalamnya seperti *squid* bisa langsung dipakai atau biasanya istilah ini disebut *compatible* (Priyono et al., 2013)

Sistem operasi ubuntu adalah salah satu distribusi dari *linux* yang berbasiskan debian dan didistribusikan sebagai *open source* dan operasi sistem ubuntu ini juga merupakan sistem operasi yang lengkap dan memiliki dukungan yang baik dari para ahli profesional dan juga komunitas. Ubuntu merupakan proyek andalan debian dan sasaran awalnya adalah menciptakan sistem operasi *desktop linux* yang mudah untuk digunakan, dan ubuntu juga dijadwalkan untuk *update* dan merilis setiap 6 bulan sehingga ubuntu bisa terus diperbaharui.

Sistem operasi adalah program utama yang dijadikan sebagai penghubung *software* aplikasi yang digunakan oleh pengguna dengan *hardware.*Sehingga program aplikasi dapat berjalan dan dikontrol oleh *user*. Sistem operasi secara umum ialah pengelola seluruh sumber daya yang terdapat pada sistem komputer dan menyediakan sekumpulan layanan *(system calls)* yang sering disebut *tools atau utility* sehingga memudahkan dan menyamankan penggunaan ketika memanfaatan sumber daya sistem komputer tersebut.

Sistem operasi juga mengatur sumber daya dari perangkat keras dan perangkat, pengguna tidak bisa menjalankan program aplikasi pada komputer yang tidak memliliki sistem operasi kecuali menjalankan program *booting*.

2.3.1 Perkembangan Ubuntu

Ubuntu pertama kali keluarkan pada 20 Oktober 2004.sejak itu, canonical telah merilis versi Ubuntu yang baru setiap 6 bulan sekali. Setiap rilis didukung selama 18 bulan untuk *update system*, *security*, dan *error*. Ubuntu *12.04* yang dirilis pada April 2012 mendapatkan *update* sistem selama 5 tahun. Ini bertujuan untuk mengakomodasi bisnis dan pengguna IT yang bekerja pada siklus panjang dan pertimbangan biaya untuk memperbarui sistem.paket *software* ubuntu berasal dari paket debian, ubuntu memakai *format* paket dan manajemen paket debian. Paket debian dan ubuntu sering kali tidak cocok.

Paket debian sering kali perlu dibuat ulang dari *source* agar dapat dipakai di ubuntu, begitu juga dengan debian. Ubuntu bekerja sama dengan debian untuk berusaha agar perubahan sistem di ubuntu agar bisa digunakan di debian, namun tak terlaksana karena paket ubuntu berpotensi mengarah terlalu jauh sistem operasi debian. Sebelum setiap keluaran ubuntu, paket diambil dari paket tidak stabil di *debian* dan digabung dengan modifikasi pada ubuntu. Sebulan sebelum perilisan, pengambilan paket dihentikan dan kerja selanjutnya adalah memastikan paket yang sudah diambil bekerja dengan baik.

Ubuntu sekarang dibiayai oleh Canonical Ltd. Mark Shuttleworth mendirikan ubuntu *foundation* dan memberikan pendanaan awal sebesar US$10 juta. Tujuan dari pendirian yayasan ini yaitu untuk memastikan pengembangan dan dukungan semua versi ubuntu dapat terus berjalan dengan lancar.(Mahardani & Asmunin, 2017).

2.3.2 Kelebihan Ubuntu

Pada dasarnya sistem operasi adalah sebuah perangkat lunak yang berfungsi sebagai sistem dasar sebuah perangkat, berikut kelebihan ubuntu *server* (Pratama & Dharmesta, 2018) :

1. *Freeware*, yaitu *software* yang bersifat *free* tanpa ada tuntutan dari hak cipta.
2. *Start / shutdown* cepat.
3. Tahan virus.
4. Performansi bagus.
5. Tidak membutuhkan *hardware* yang terlalu besar kapasitasnya maupun biaya.
6. Akses data mendapat proteksi penuh dari pengguna.

2.3.3 Kekurangan Ubuntu

Sistem operasi ubuntu juga memiliki beberapa kekurangan sama seperti sistem operasi lainnya, yaitu (Pratama & Dharmesta, 2018) :

a. Proses pemasangan agak lama karena paket yang di *install* harus *update* secara *online*.
b. Belum *userfriendly,* dikarenakan sebagian besar pengguna ubuntu berasal dari migrasi *windows*.

Tak semua aplikasi *windows* anda kompatibel dengan *wine* sehingga aplikasi yang diperlukan yang biasanya digunakan dioperasi sistem lain mungkin tidak bisa digunakan di ubuntu.

2.3.4 Ubuntu Edisi *Server*

Ubuntu juga memberikan sistem operasinya dalam edisi server. Pembaruannya akan meliputi keamanan, *hardware*, dan pembaruan ubuntu *stack*. Ubuntu menggunakan keamanan *AppArmor* untuk *linux* kernel, dan *firewall* sudah dikembangan dari yang digunakan oleh sistem operasi. Direktori *home* dan *private directories* juga dienkripsi.

Ubuntu *12.04 LTS Server Edition* mendukung arsitektur Intel x86 dan AMD 64. Edisi *server* menyediakan fitur seperti *file/print services, web hosting, email hosting,* dan lain-lain. Terdapat beberapa perbedaan antara edisi *server* dan edisi *desktop* walaupun keduanya menggunakan *repository apt* yang sama. Perbedaan adalah, pada edisi *server window environment* tidak dipasang secara standar, walaupun *interface* grafik dapat dipasang secara manual seperti ubuntu desktop. Ubuntu *server edition* juga memiliki pilihan untuk menginstall ubuntu *enterprise cloud* (*SISTEM OPERASI ubuntu,* 2017).

2.3.5 Syarat dan Pemasangan Ubuntu

Ada beberapa spesifikasi minimum dan persayaran untuk memasang sistem operasi ubuntu, yaitu (Priyono et al., 2013) :

1. Memiliki prosesor dengan kecepatan proses 300 MHz.
2. Memiliki minimal RAM 64 MB.
3. Minimal memiliki 4 GB *disk space* untuk penginstalan.
4. Memiliki *VGA graphics card* dengan resolusi 640x480 *pixels*.
5. PC mendukung CD-ROM *drive* atau juga *network interface card*.

Agar kinerja dari *server* lebih maksimal dalam melakukan pekerjaannya ada spesifikasi minimal yang direkomendasikan untuk memasang operasi sistem ubuntu, yaitu:

a. Memiliki prosesor dengan kecepatan proses 700 MHz.
b. Memiliki 1024 MB RAM.
c. Minimal memiliki 10 GB *disk space.*
d. Mendukung VGA *graphical card* dengan resolusi 1024x768 *pixels*.
e. Dan juga PC mendukung untuk koneksi internet.

2.4 Pengertian *Intrusion Detection System* (IDS)

Intrusion Detection System (IDS) adalah sebuah sistem yang dapat mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan. Jika ditemukan kegiatan-kegiatan yang mencurigakan berhubungan dengan *traffic* jaringan, maka IDS akan memberikan peringatan kepada sistem atau *administrator* jaringan (Sutarti et al., 2018).

Intrusion detection system dapat di kalsifikasi menjadi 3 bagian yaitu :

1. *Host Intrusion Detection System* (HIDS)

   Jenis ini ditempatkan pada satu perangkat seperti *server* atau *workstation*, dimana data dianalisis secara lokal kemesin dan mengumpulkan data ini dari berbagai sumber. HIDS dapat menggunakan sistem deteksi anomali dan penyalahgunaan.

2. *Network Intrusion Detection System* (NIDS)

   NIDS dikerahkan pada titik strategis dalam jaringan infrastruktur.NIDS dapat menangkap dan menganalisis data mendeteksi serangan yang diketahui dengan membandingkan pola atau tanda dari database atau deteksi aktivitas ilegal dengan memindai lalu lintas untuk aktivitas anomali. NIDS juga disebut sebagai "*Packet-sniffer*", karena ini menangkap paket yang lewat melalui media komunikasi.

3. *Hybrid Intrusion Detection System*

   Manajemen dan memperingatkan dari kedua perangkat deteksi intrusi jaringan dan berbasis host, dan menyediakan pelengkap logis untuk NID dan HID - manajemen deteksi intrusi pusat (Ashoor dan Gore, 2011).

Dalam kebanyakan IDS adalah sistem yg bersifat pasif yang mana tugas dari IDS ini hanyalah mendeteksi intrusi yang bila terjadinya penyerangan dan memberikan peringatan kepada admin jaringan bahwa terjadinya penyerangan (Sutarti et al., 2018).

2.5 Jenis Serangan

Denial of Service (DOS) adalah serangan yang menyerang *server* dalam jaringan internet atau intranet dengan cara mengirimkan permintaan informasi dengan membanjiri sumber daya yang dimiliki oleh *server* tersebut sampai server tidak dapat menjalankan kinerjanya dengan benar dan secara tidak langsung menghambat kinerja *server* dalam pengoperasiannya secara normal.

Serangan DoS memiliki beberapa jenis penyerangan dengan beberapa cara yaitu :

a. *Syn Flood*

   Pada saat keadaan normal penyerang akan mengirimkan paket TCP SYN dalam melakukan hubungan dengan *server*, dengan melalui cara ini penyerang akan membanjiri *server* berupa banyaknya paket TCP SYN

b. ICMP *Flood*

   Penyerangan yang bertujuan untuk membuat *server* menjadi *crash*, yang di sebabkan banyaknya pengiriman paket ke arah target. Penyerangan ini dilakukan dengan mengirimkan suatu perintah ping dengan jumlah yang besar. Hal ini yang membuat *server* menjadi *crash* dan menurunkan kinerja dari *server*.

c. *Remote controled attack*

   Penyerangan dengan mengendalikan beberapa jaringan lain untuk menyerang target. Penyerangan dengan tipe ini biasanya akan berpengaruh besar, karena biasanya *server- server* untuk menyerang mempunyai *bandwith* yang besar.

d. *Buffer Overflow*

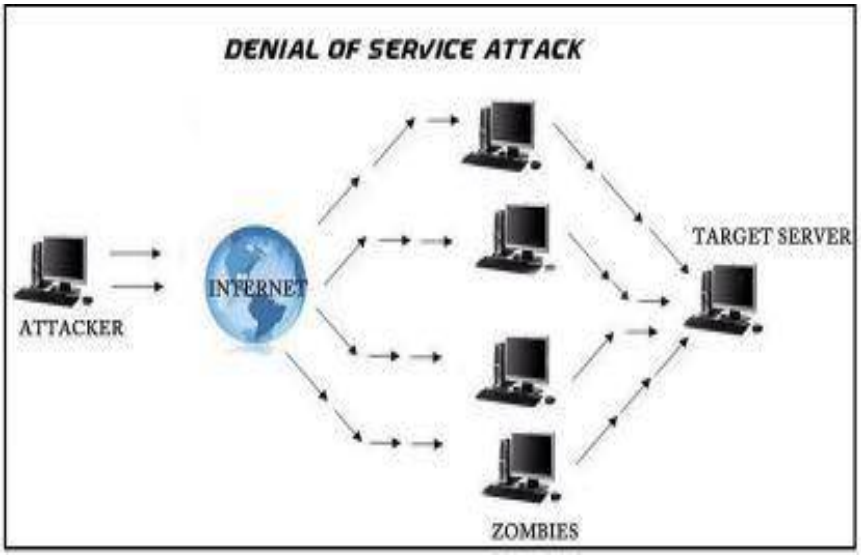
   Penyerang melakukan serangan dengan mengirimkan data yang melebihi kapasitas sistem. TCP Flood dan UDP *Flood*

e. Teardrop

   Penyerang mengirimkan paket terfragmentasi ke server dengan memanfaatkan fitur yang ada pada TCP/IP yaitu paket *fragmentation*.

Hal ini menyebabkan pecahan-pecahan yang terkirim tidak dapat dikumpulkan kembali oleh mesin target (Hermawan, 2013).

Untuk melihat bagaimana DoS bekerja dapat dilihat seperti berikut:



Gambar 2.1 Proses Penyerangan DoS

Sumber: (Digital et al., 2018)

2.6 Pengertian *Router Firewall*

Router firewall adalah sejenis perangkat fisik (*physical device*) yang bertugas mengontrol *incoming traffic* dan *outgoing traffic* koneksi internet. Pengguna yang membeli perangkat ini biasanya ingin membatasi akses pada pengguna lain yang menggunakan koneksi mereka, baik berupa jaringan kabel (*wired*) maupun jaringan *wireless*. Keuntungan *router firewall* lainnya adalah dapat menyembunyikan jaringan komputer dari dunia luar secara efektif, di mana akan memberikan keamanan internet (*internet security*) ketika *browsing* internet.

Cara instalasi *router firewall* terbilang sederhana, di mana merupakan salah satu cara termudah untuk memonitor dan membatasi pengguna ketika terhubung

pada Internet. *Router firewall* menerima koneksi Internet dan melewatkannya melalui sejenis *checkpoint*, atau gerbang khusus. Setelah koneksi melewati *router firewall*, maka *firewall* akan secara efektif menutup akses pada siapa saja yang tidak memiliki identitas dan perizinan yang sesuai. *Administrator* lah yang akan menentukan siapa saja yang mendapatkan akses pada internet, dan siapa yang tidak mendapatkannya (Nurrofiq, 2012).

2.7 Serangan *Distributed Denial Of Service* (DDOS)

Serangan adalah kegiatan yang dilakukan untuk melumpuhkan suatu objek yang dituju dan biasanya serangan akan mengakibatkan kerugian terhadap suatu objek yang diserang, serangan juga bisa digunakan untuk mencuri informasi dari objek yang diserang dan dapat merugikan pemilik objek yang diserang. Biasanya bisa karena alasan persaingan dalam bisnis, dan lain-lain.

Serangan DDoS adalah serangan yang berusaha untuk melumpuhkan komputer yang dituju dan membuat server tersebut menjadi *down*, hang karena disebabkan oleh serangan yang berupa pc *zombie* yang diberikan sangat banyak kedalam *server* tersebut, sehingga *traffic* pada *server* menjadi penuh dan pengguna lain tidak bisa masuk kedalam layanan yang diberikan oleh penyedia.

Suatu serangan yang dilakukan untuk membuat komputer atau jaringan komputer tidak dapat menyediakan layanan secara normal.Pada umumnya serangan DOS menargetkan serangan pada bandwidth jaringan komputer atau koneksi jaringan.*Bandwidth attack* membanjiri jaringan dengan *volume traffic* yang tinggi, sehingga semua *resources* yang ada, tidak dapat melayani *request*

dari *legitimate user*. *Connectivity attack* membanjiri komputer dengan *volume request* koneksi yang tinggi, sehingga semua *resources* sistem operasi komputer yang ada tidak dapat memproses lebih lama *request* dari *legitimate user*(Hermawan, 2013).

Setiap serangan yang ditujukan ke sebuah *server* bisa menyebabkan menyebabkan pemilik komputer mengalami kerugian, dan setiap serangan yang masuk bisa saja dicegah, tetapi pada dasarnya tidak ada komputer yang benar-benar aman dan tidak bisa ditembus keamanannya, setiap komputer pasti mempunyai celah untuk disusupi.

Keamanan jaringan komputer merupakan hal yang tidak bisa dipisahkan dalam jaringan komputer dan keamanan jaringan komputer yang tidak dirancang dengan baik bisa menyebabkan kebocoran data, pelanggaran *privasi*, hingga kerugian finansial (Ramadhan Triyanto Prabowo, 2015).

Karena komputer tidak ada yang aman, maka yang harus dilakukan adalah mengoptimalkan setiap celah-celah keamanan dari komputer tersebut agar komputer tidak dengan mudah diserang oleh orang-orang yang tidak bertanggung jawab atas apa yang dilakukannya untuk menjatuhkan sebuah *server*.

2.7.1 Tipe Serangan DDoS

Penyerang *DDoS* melakukan serangan dengan beberapa cara untuk melumpuhkan *server*, yaitu:

1. Membanjiri lalu lintas jaringan dengan banyak data yang membuat lalu lintas jaringan yang datang dari pengguna lain tidak dapat masuk, ini disebut sebagai *traffic flooding.*
2. Membanjiri jaringan dengan banyak *request* terhadap sebuah layanan yang disediakan oleh sebuah *host* sehingga *request* yang datang tidak terlayani karena *request* yang banyak.
3. Mengganggu komunikasi antara *host* dan *client* nya yang terdaftar dengan banyak cara, dan termasuk juga mengubah informasi konfigurasi sistem atau bahkan merusak fisik terhadap komponen dan *server* (Wikipedia, n.d.).

2.7.2 Penanganan Serangan DDoS

Ada beberapa cara menangani serangan komputer, tergantung pada serangan apa yang ditemukan pada komputer, beda serangannya maka beda pula cara penanganannya, berikut adalah beberapa cara menangani serangan pada komputer server:

1. Penanganan serangan *DDoS*

   Yang bisa dilakukan saat komputer diserang dengan *DDoS* adalah melakukan identifikasi serangan, serangan akan terlihat tanda-tandanya jika mengecek server. Berikut adalah beberapa cara penanganan serangan *DDoS*:

   a. *Syn Flooding*

      Gunakan *firewall* untuk meneruskan paket data yang tidak jelas asalnya.

   b. *Remote Controled Attack*

Block alamat *ip* dan *port* dari penyerang yang masuk sehingga tidak bisa mengirimkan paket data dari ip yang digunakannya saat menyerang komputer tersebut.

c. UDP *Flooding*

Menolak paket trafik yang datangnya dari luar jaringan dan mematikan semua layanan UDP.

d. *Smurf Attack*

Disable broadcast address pada *router* yang digunakan atau *filtering* permintaan ICMP *echorequest* pada *firewall* atau juga membatasi trafik ICMP.

e. Memperbesar *bandwith*

Memperbesar *bandwith* adalah untuk memberikan waktu agar sistem tidak dengan mudah *down* dan cara ini memang kurang ampuh untuk menangani *DDoS* (S et al., 2016).

2.8 *Snort*

Snort adalah *Intrusion Detection System* jaringan *open source* yang mampu menjalankan analisis *real-time* dan paket *logging* pada IP *network*. *Snort* dapat menjalankan analisis *protocol ,content* searching atau *maching,* dan dapat digunakan untuk mendeteksi berbagai serangan dan penyusupan. *Snort* merupakan suatu perangkat lunak untuk mendeteksi penyusup maupun menganalisa paket yang melintasi jaringan *computer* secara *realtime traffic* dan *logging* ke dalam database serta mampu mendeteksi berbagai serangan yang berasal dari luar

jaringan. Snort dapat digunakan pada *platform* sistem operasi Linux, BSD, Solaris,Windows dan sistem operasi lainnya. (Sudradjat, 2017).

Program *snort* dapat dioperasikan dengan tiga mode :

1. Paket *sniffer*

Membaca paket-paket dari jaringan dan memperlihatkan bentuk aliran tak terputus pada konsol (layar). Jika hanya ingin melihat paket-paket *header* dari TCP/IP pada layar menggunakan perintah:

```
./snort –v
```

2. Paket *logger*

Mencatat *log* dari paket-paket ke dalam disk. Jika ingin menyimpan catatan paket-paket ke dalam disk, maka perlu mencantumkan direktori *logging*, yaitu dimana data log disimpan padanya. Melalui perintah berikut *Snort* akan secara otomatis berjalan pada mode pencatatan paket:

```
./snort –dev -1 ./log
```

3. NIDS (*Network Intrusion Detection System*)

Pada mode ini *snort*akan berfungsi untuk mendeteksi serangan yang dilakukan melalui jaringan komputer. Untuk mengaktifkan mode sistem deteksi penyusup jaringan NIDS (*Network Intrusion Detection System*) menggunakan perintah sebagai berikut:

```
./snort –dev -1 ./log –h 192.168.1.0/24 –c snort.conf
```

Snort memiliki komponen yang bekerja saling berhubungan satu dengan yang lainnya seperti berikut ini (Ariyus, 2007):

a. *Decoder* merupakan paket yang di-*capture* dalam bentuk struktur data dan melakukan identifikasi *protokol*, *decode* IP dan kemudian TCP atau UDP tergantung informasi yang dibutuhkan, seperti *port number*, dan IP address. *Snort* akan memberikan peringatan jika menemukan paket yang cacat.
b. *Preprocessors* adalah suatu saringan yang mengidentifikasi berbagai hal yang harus diperiksa seperti *Detection Engine*. *Preprocessors* berfungsi mengambil paket yang berpotensi membahayakan, kemudian dikirim ke *detection engine* untuk dikenali polanya.
c. *Rules File* merupakan suatu file teks yang berisi daftar aturan yang sintaksnya sudah diketahui. Sintaks ini meliputi protokol, *address*, *output plug-ins* dah hal-hal yang berhubungan dengan berbagai hal.
d. *Detection Engine* menggunakan *detection plug-ins*, jika ditemukan paket yang cocok maka *snort* akan menginisialisasi paket tersebut sebagai suatu serangan.
e. *Output Plug-ins* suatu modul yang mengatur format dari keluaran untuk *alert* dan *file logs* yang bisa diakses dengan berbagai cara, seperti *console, extern files, database*, dan sebagainya.

2.9 IP *Address*

Internet Protocol Address atau biasa disebut IP *Address* merupakan suatu deretan angka biner yang disusun dengan kisaran antara 32 bit sampai dengan 128 bit dan digunakan sebagai alat identifikasi *host*/antarmuka pada jaringan dan sebagai komputer jaringan.Dalam ilmu jaringan komputer penggunaan angka dengan 32 bit dipakai pada IP *Address* khusus versi IPv4 sedangkan untuk angka 128 bit untuk yang versi IPv6.

Hadirnya versi IPv6 untuk mengantisipasi jika IPv4 sudah kehabisan daya tampung mengingat kemajuan teknologi yang tentunya mendorong juga semakin berkurangnya persediaan IP *Address* untuk seluruh dunia. Semakin tinggi bit pada IP *Address* komputer anda tentunya akan menghadirkan koneksi yang lebih cepat tentunya (Sitanggang, 2019).

2.9.1 Jenis IP *Address*

a) IP versi 4 (IPv4)

Internet Protocol Version 4 atau IPv4 terdiri dari 32-bit dan bisa menampung lebih dari 4.294.967.296 host di seluruh dunia.contohnya yaitu 172.146.80.100, jika host di seluruh dunia melebihi angka 4.294.967.296 maka dibuatlah IPv6.

b) IP versi 6 (IPv6)

IPv6 diciptakan untuk menjawab kekhawatiran akan kemampuan IPv4 yang hanya menggunakan 32 bit untuk menampung IP Address di seluruh dunia, semakin banyaknya pengguna jaringan internet dari hari ke hari di

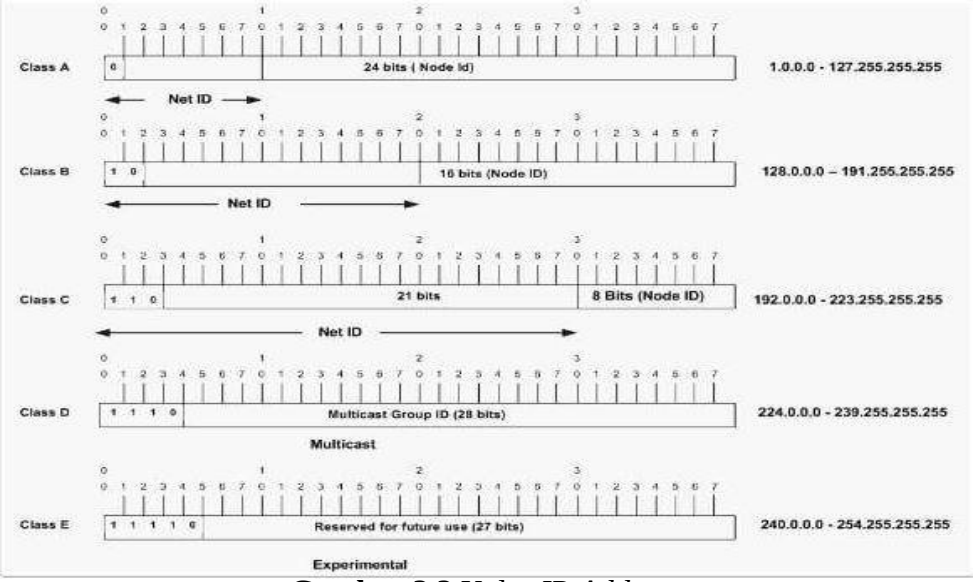
seluruh dunia IPv4 dinilai suatu saat akan mencapai batas maksimum yang dapat ditampungnya, untuk itulah IPv6 versi 128 bit diciptakan. Dengan kemampuanya yang jauh lebih besar dari IPv4 dinilai akan mampu menyediakan IP Address pada seluruh pengguna jaringan internet di seluruh dunia yang semakin hari semakin banyak.

Internet protocol versi 6 atau IPv6 ini terdiri dari 128 bit.IP ini 4 kali dari IPv4, tetapi jumlah host yang bisa ditampung bukan 4 kali dari 4.294.967.296 melainkan 4.294.967.296 pangkat 4, jadi hasilnya 340.282.366.920.938.463.463.374.607.431.768.211.456 (Sitanggang, 2019)

2.9.2 Kelas IP Address

IP *Address* versi 4 terdiri atas 4 oktet, nilai 1 oktet adalah 255. Karena ada 4 oktet maka jumlah IP *Address* yang tersedia adalah 255 x 255 x 255 x 255.IP *Address* sebanyak ini harus dibagi-bagikan keseluruh pengguna jaringan internet di seluruh dunia. Untuk mempermudah proses pembagiannya, IP *Address* harus dikelompokan dalam kelas-kelas.

IP Address dikelompokan dalam lima kelas, yaitu kelas A, B, C, D, dan E. Perbedaannya terletak pada ukuran dan jumlah. IP *Address* kelas A jaringan. IP *Address* Kelas B digunakan untuk jaringan berukuran besar dan sedang. IP *Address* Kelas C untuk pembagian jaringan yang banyak, namun masing-masing jaringan memiliki anggota yang sedikit.



Gambar 2.2 Kelas IP *Address*

Sumber :http://technopark.surakarta.go.id/

2.10 *Virtualbox*

VirtualBox merupakan salah satu produk perangkat lunak yang sekarang dikembangkan oleh *Oracle*. Aplikasi ini pertama kali dikembangkan oleh perusahaan Jerman, Innotek GmbH. Februari 2008, Innotek GmbH diakusisi oleh Sun Microsystems.Sun Microsystem kemudian juga diakuisisi oleh *Oracle*.

VirtualBox berfungsi untuk melakukan virtualisasi sistem operasi. *VirtualBox* juga dapat digunakan untuk membuat virtualisasi jaringan komputer sederhana. Penggunaan *VirtualBox* ditargetkan untuk *Server*, *desktop* dan penggunaan *embedded*. Berdasarkan jenis VMM yang ada, *Virtualbox* merupakan jenis *hypervisor type* 2.

Oracle VM VirtualBox adalah perangkat lunak *virtualisasi*, yang dapat digunakan untuk mengeksekusi sistem operasi tambahan di dalam sistem operasi utama. Sebagai contoh, jika seseorang mempunyai sistem operasi *Microsoft*

Windows yang terpasang di komputernya, maka yang bersangkutan dapat pula menjalankan sistem operasi lain yang diinginkan di dalam sistem operasi *Microsoft Windows* tersebut. Fungsi ini sangat penting jika seseorang ingin melakukan ujicoba dan simulasi instalasi suatu sistem tanpa harus kehilangan sistem yang ada.

Fungsi – Fungsi *VirtualBox :*

1) Mencoba *Operation System* apapun. *Virtualbox* dapat memainkan semua sistem operasi baik itu menggunakan Windows, Linux atau turunan Linux lainnya. *Virtualbox* juga dapat dipergunakan untuk menguji coba OS baru.
2) Sebagai media untuk membuat simulasi jaringan. Di dalam *Virtualbox* dapat membuat banyak mesin *virtual* dan memainkannya sekaligus. Dapat menggabungkan semua mesin yang aktif tadi dalam satu jaringan. Seolah-olah mempunyai banyak komputer yang terkoneksi.
3) Sebagai komputer yang fleksibel dan dapat dipindah-pindahkan.

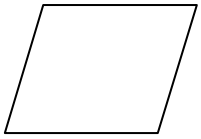
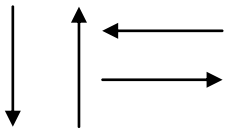
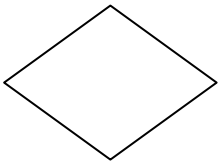
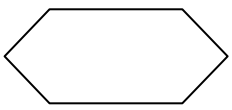
Misalnya saat membuat sebuah *server* antivirus dan *server* absensi sekaligus untuk keperluan kantor dalam bentuk *virtual* di satu komputer. *Server* antivirus dan absensi dapat dipindahkan ke komputer lain dengan memindahkan mesin *virtual* ke komputer lain jika sewaktu waktu komputer utamanya rusak. Biasanya format *file virtualbox* berekstensi .VDI. maka tinggal *copy paste* format .VDInya saja ke komputer lain (Sutarti et al., 2018).

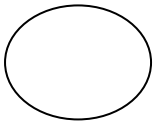
2.11 *Flowchart*

Flowchart adalah bagian-bagian yang memiliki arus dan menggambarkan langkah-langkah penyelesaian suatu masalah. *Flowchart* merupakan suatu cara penyajian dari suatu Algoritma

Flowchart disusun dengan simbol. Simbol ini dipakai sebagai alat bantu menggambarkan proses didalam program. Simbol-simbol yang digunakan dapat dibagi, yakni sebagai berikut:

Tabel 2.1 Simbol *Flowchart*

Simbol	Keterangan
	*Input/Output* Digunakan untuk mewakili data input/output
	Arus/*Flow* Digunkana untuk menunjukkan arah/alir dari suatu proses.
	Proses Digunakan untuk mewakili suatu proses.
	Keputusan/*Decision* Digunakan untuk suatu penyelesaian kondisi dalam program.
	Persiapan/*pendefined* Proses Digunakan untuk memberikan nilai awal dari proses.

	Penghubung/*Connector* Digunakan untuk menunjukkan sambungan dari aliranyang terputus dihalaman yang sama.
	*Predefined* proses Digunakan untuk proses yang detilnya terpisah.
	Awal/akhir (Terminal) Digunakan untuk menunjukkan awal dan akhir dari proses.

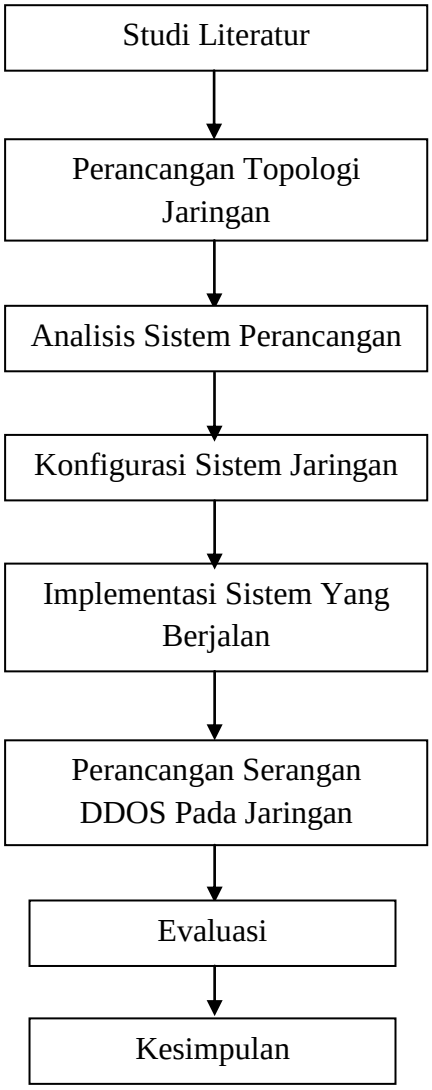
Sumber : (Angga, 2014)

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Metode penelitian yang digunakan yaitu metode eksperimen dimana dilakukan percobaan menggunakan sistem operasi ubuntu. Adapun tahapan penelitian yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar 3.1 Tahapan Penelitian

Dalam menyelesaikan skripsi ini penulis memperoleh data dengan menggunakan beberapa tahapan-tahapan dari gambar 3.1 sebagai berikut :

1. Studi Literatur

   Dengan pengumpulan data-data berupa teori baik dengan dosen pembimbing maupun dengan orang yang berkopeten dalam kasus ini dan pustaka yang mendukung.

2. Perancangan Topologi Jaringan

   Perancangan topologi yang dimaksud adalah untuk topologi yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang hendak dibangun.

3. Analisis Sistem Perancangan

   Perancangan sistem yang akan digunakan untuk merancang suatu sistem yang dapat mendeteksi adanya penyusup ataupun serangan yaitu *Intrusion Detection System*, yang sebelumnya membutuhkan *tools* ataupun komponen yang diperlukan untuk membangun sistem tersebut yang nantinya akan bekerja sama untuk mendapatkan hasil yang maksimal

   a. *Snort*
   b. *WinPcap*
   c. *Virtualbox*

4. Konfigurasi Sistem Jaringan

   Pada tahapan ini, penulis melakukan konfigurasi awal sistem operasi *server*. *Server* yang sudah terinstall akan dilengkapi dengan beberapa aplikasi jaringan yang lain sebagai penunjang sistem. Penulis juga melakukan pemberian ip *address* kepada *network interface server* sesuai dengan rancangan topologi yang telah dibuat. Konfigurasi yang dilakukan selanjutnya adalah melakukan instalasi *snort,* sebelum melakukan instalasi program, penulis telah menyiapkan bebrapa dependensi yang diperlukan untuk keperluan instalasi. Setelah *snort* terinstall dengan baik maka hal selanjutnya yang perlukan adalah menghubungkan database dengan program *snort*, sehingga semua aktivitas paket data dalam jaringan dapat direkam secara baik dan ditempatkan pada database yang telah ditentukan.

5. Implementasi Sistem Yang berjalan

   Kinerja *snort* sangat baik pada pengujian yang dilakukan. Hal ini terkait pada kemampuan mesin mengelola data – data yang masuk dalam jumlah yang banyak dan cepat.

6. Perancangan Serangan DDOS Pada Jaringan

   Ketika serangan DDOS dilancarkan ke suatu *server,* maka akan telihat perilaku *daemon*/komputer yang secara signifikan mempengaruhi jaringan dan terjadi pada waktu bersamaan. Jenis serangan DDOS yang dilakukan adalah jenis *Request Flooding*, dimana penyerang membanjiri jaringan dengan banyak *request* terhadap sebuah *web*

server, sehingga *web server* tidak dapat melayani permintaan dari *client* yang membutuhkan layanan tersebut.

7. Evaluasi

   Apakah *Intrusion Detection System* tersebut sudah dapat untuk menganalisis serangan dari DDOS pada server.

8. Kesimpulan

   a. *Snort* dapat mendeteksi serangan *Distributed Denial of Service* (DDOS) menggunakan metode TCP *Ping Flooding* dengan menangkap ip *address* penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.

   b. Snort dapat mendeteksi serangan *Distributed Denial of Service* (DDOS) menggunakan metode UDP *Ping Flooding* dengan menangkap ip *address* penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.

   c. *Snort* dapat mendeteksi serangan *Distributed Denial of Service* (DDOS) menggunakan metode HTTP *Ping Flooding* dengan menangkap ip *address* penyerang yang menghasilkan respon dan dampak pada CPU komputer yang berlebihan.

3.2 Metode Pengumpulan Data

Untuk mendukung penelitian yang akan dibangun dibutuhkannya metode pengumpulan data. Beberapa teori yang dapat digunakan dalam penelitian ini adalah sebagai berikut :

a) Wawancara

Wawancara yang digunakan dengan teknik pengumpulan data yang dilakukan dengan tatap muka dan tanya jawab secara langsung antara peneliti/penulis dengan narasumber atau Dosen Pembimbing. Peneliti telah mengetahui dengan pasti informasi apa yang hendak digali dari narasumber atau dosen pembimbing. Pada kondisi ini, penulis sudah membuat daftar pertanyaan secara sistematis. Penulis/peneliti juga menggunakan berbagai instrumen penelitian seperti alat bantu *recorder*, kamera untuk foto, serta instrumen lain.

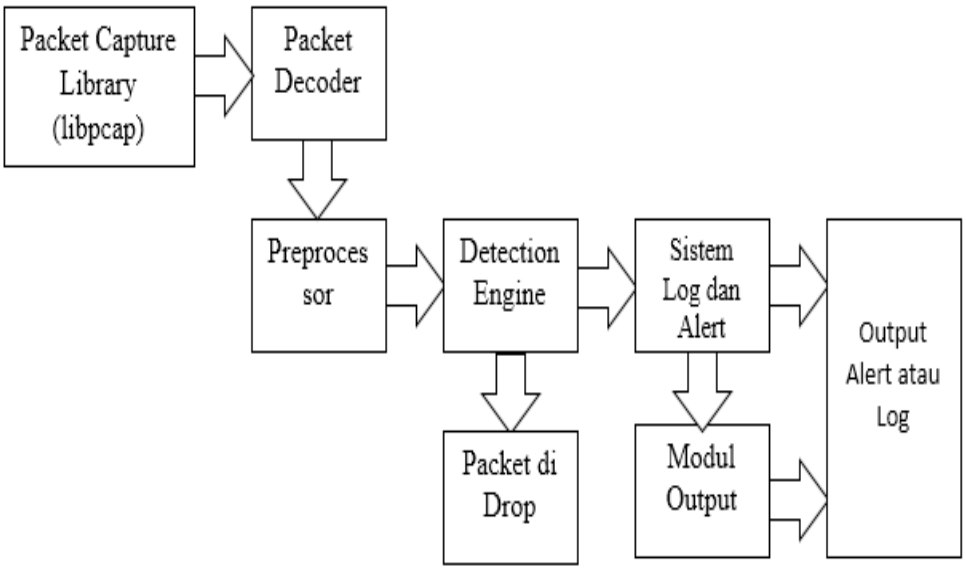
b) Penelitian Pustaka (*Library Research*)

Penulis melakukan penelitian keperpustakaan dengan tujuan agar memperoleh sumber data informasi masalah-masalah yang berkaitan dengan skripsi ini.

3.3 Analisis Sistem Yang Berjalan

Intrusion Detection Prevention System (IDS) merupakan sebuah metode yang dapat mendeteksi aktivitas yang mencurigakan dan mencegah bila adanya serangan yang berbahaya bagi *server*. *Snort* adalah salah satu *tools open source* yang digunakan semula *snort* bekerja sebagai *Intrusion Detection System* (IDS), dengan tambahan paket *filtering iptables* dan didalam snort terdapat modul tambahan DAQ *Net Filter Queue* (NFQ) sebagai *prevention* bagi *snort*.

Komponen kerja *Snort Engine Intrusion Detection System* (IDS)



Gambar 3.2 Komponen Kerja *Snort Engine*

Dari gambar diatas dapat dijelaskan komponen kerja *Snort Engine Intrusion Detection System* (IDS) :

a. *Library Packet Capture* (*Libpcap*)

Libpcap bekerja dalam menangkap dan memisahkan paket data memalui *Ethernet Card* yang selanjutnya akan digunakan *snort*.

b. Packet Decoder

Packet Decoder bekerja dalam mengambil paket dari layer 2 yang dikirim *libpcap*. Dengan memisahkan *Data Link*, *Protocol* Ip, paket TCP dan UDP *snort* memiliki informasi protokol yang akan diproses lebih lanjut.

c. *Preprocesor*

Preprocesor adalah pengubah paket yang berupa data dan untuk mencari tahu bila paket data terjadi serangan.

d. *Detection Engine*

Detection Engine adalah bagian penting *snort*. Bekerja dengan mendeteksi bila terjadinya kegiatan penyerangan pada paket. *Detection Engine* memproses *rule snort* untuk membaca strutur data *internal* yang di cocokkan dengan paket yang ada. Bila paket cocok dengan *rule* yang ada, tindakan yang di ambil berupa *logging* paket atau *alert*, bila tidak paket akan di biarkan saja.

e. Sistem Log dan *Alert*

Telah di dapati oleh *Detection Engine* bila paket cocok dengan *rule* yang ada, tindakan yang di ambil berupa *logging* paket atau *alert* dan log disimpan pada *format* teks didalam penyimpanan.

f. Modul *Output*

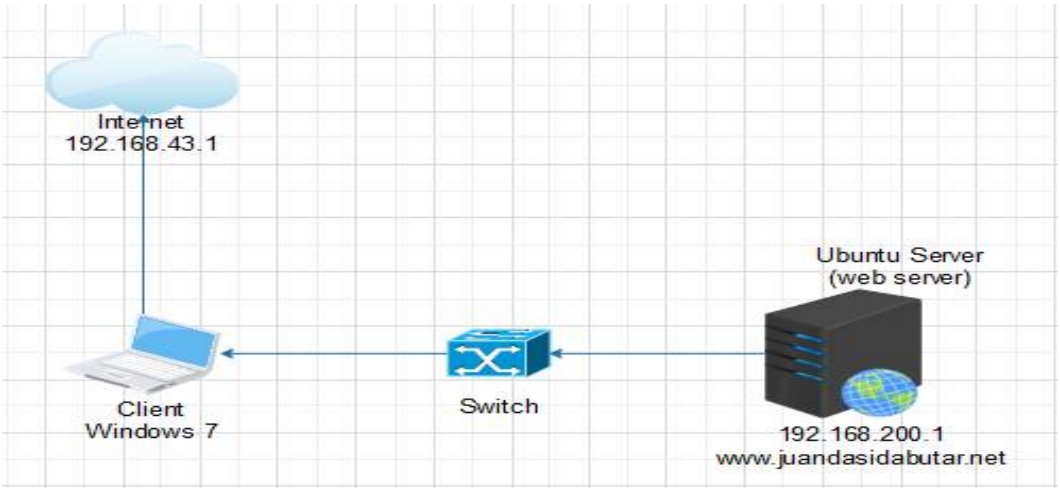
Modul *Output* bekerja bagaimana cara penyimpanan keluaran yang dihasilkan log dan *alert* dari *snort*. Modul ini mengatur jenis keluaran yang dihasilkan oleh sistem log dan *alert*.

3.4 Rancangan Penelitian

3.4.1 *Layout* Jaringan

Layout jaringan atau topologi jaringan dimaksudkan untuk merancang topologi yang kiranya sesuai dengan sistem yang dikembangkan, sehingga gambaran topologi berikut dapat memberikan gambaran secara jelas tentang sistem yang hendak dibangun.

1. Topologi sistem sebelum adanya serangan

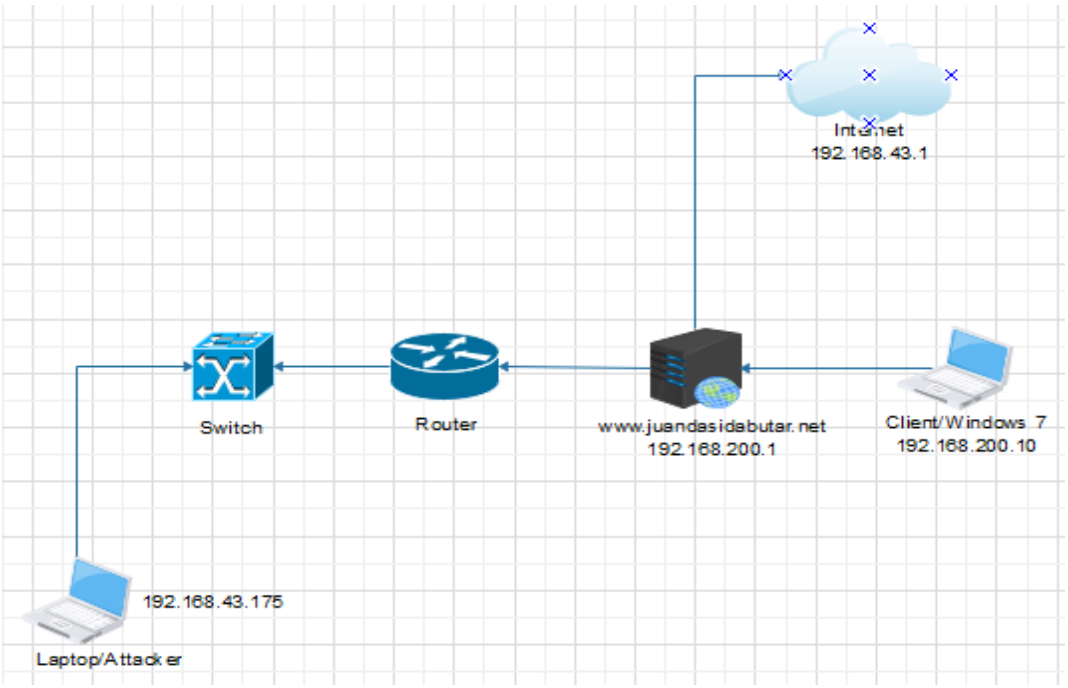


Gambar 3.3 Topologi sistem sebelum diserang

Adapun penjelasan dari topologi sistem jaringan diatas adalah sebagai berikut :

a. Pada *client* adalah tempat pengujian dari hasil konfigurasi *web server*
b. *Switch* merupakan suatu alat penghubung konektivitas pada jaringan menuju ke *web server* dan internet
c. *Server* adalah tempat untuk konfigurasi *web server* dan *snort* (IDS)

2. Topologi sistem setelah diserang



Gambar 3.4 Topologi sistem serangan ddos pada *snort* dan *web server* yang akan dibangun

Adapun penjelasan dari topologi sistem jaringan di atas adalah sebagai berikut :

a. *Client* merupakan tempat pengujian dari konfigurasi *web server*
b. *Switch* sebagai alat penghubung konektivitas pada jaringan langsung menuju ke *web server* dan internet
c. *Server* sebagai tempat untuk mengkonfigurasi *web server* dan *snort*
d. *Attacker* bertujuan untuk melakukan serangan pada *server.*

3.4.2 Anggaran Biaya

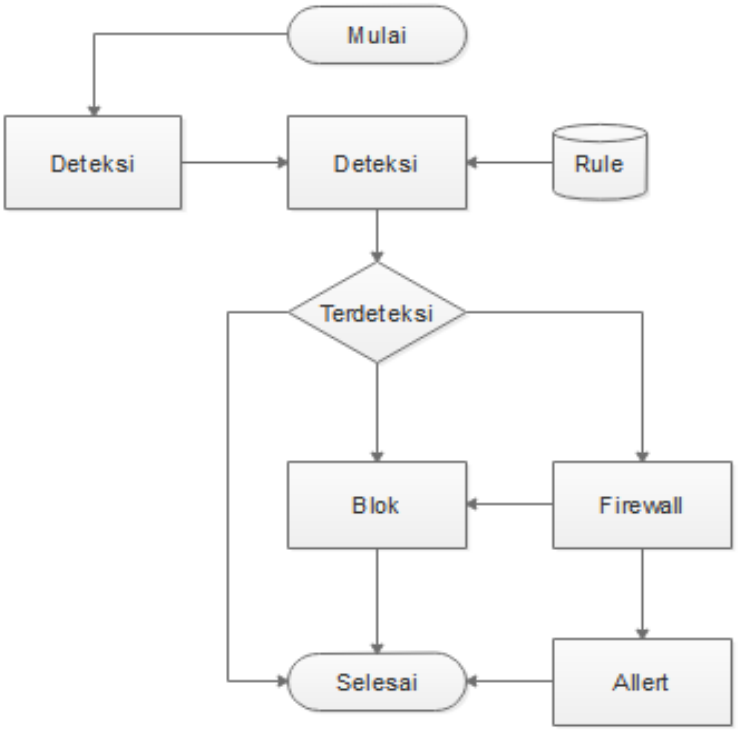
Untuk memenuhi dalam penelitian ini penulis melakukakan pengumpulan biaya yang dikeluarkan untuk penelitian mengenai Analisis Keamanan *Server* Menggunakan IDS dan *Router Firewall Server* Dari Serangan DDOS adalah sebagai berikut :

Tabel 3.2 Anggaran Biaya

NO	Hardware	Spesifikasi	Jumlah	Harga
1.	Laptop untuk Client,Attacker dan Server	LENOVO 320 AMD Radeon R3 Graphics SSD 250 Gb	1	8.000.000
2.	Router		1	
3.	Sistem Operasi : a. Ubuntu *Server* b. Ubuntu Desktop c. Mikrotik OS d. Windows 7	-	1 1 1	Rp. 15.000 Rp. 15.000 - Rp. 15.000

3.4.3 Manajemen Jaringan

Sistem yang akan dibangun pada penelitian ini dapat digambarkan seperti berikut :



Gambar 3.5 Alur Perancangan Sistem yang akan dibangun

Diagram alur atau *flowchart* menggambarkan bagaimana jalannya sebuah sistem dalam melakukan deteksi dan pencegahan. Pada awalnya paket akan di *capture* lalu dideteksi oleh IDS berdasarkan rule yang tersedia. Kemudian apabila tidak terdeteksi maka proses selesai, sedangkan apabila terdeteksi, maka *firewall* akan melakukan blokir terhadap paket dan mengirimkan *alert*.

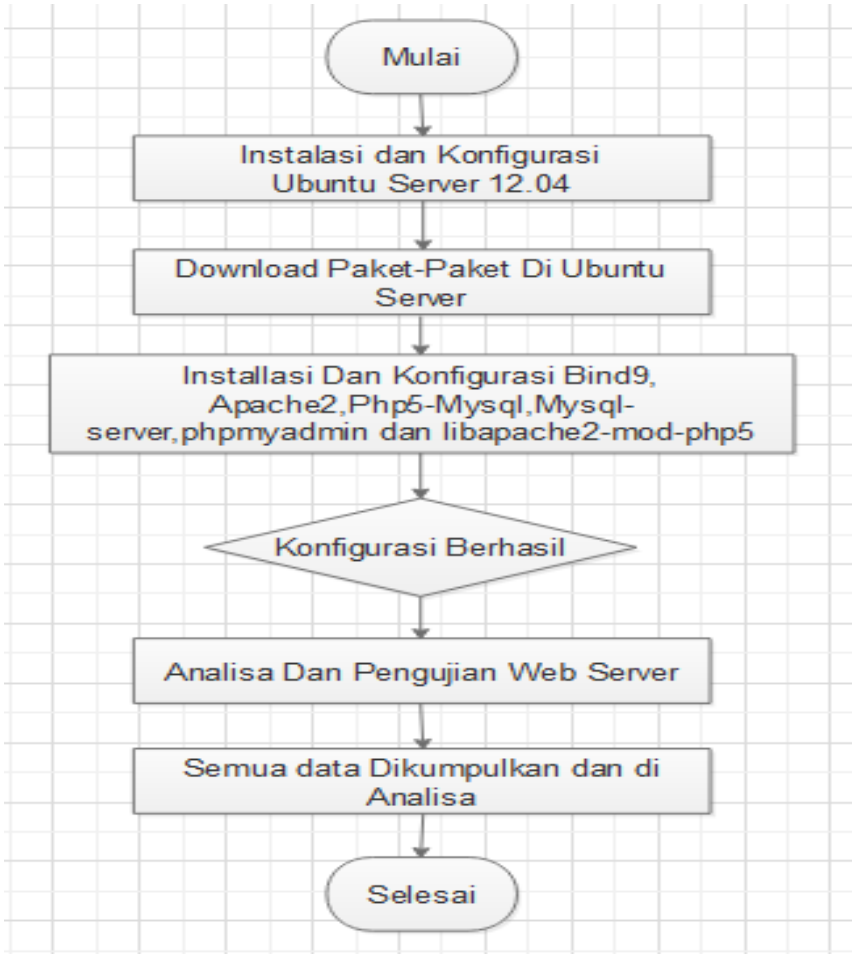
Tabel 3.1 Pengalamatan Ip *Address*

NO	Hardware/Software Network	Port Ethernet	Alamat IP / IP Address
1	Sumber Internet	-	192.168.43.1
2	Ubuntu *Server*	Eth0	*Address* 192.168.43.175 Netmask 255.255.255.0
	Web Server	Eth1	192.168.200.1 255.255.255.0
	Snort (IDS)	Eth0	192.168.100.0/24
3	*Attacker*	Eth1	*Dynamic Host Configuration Protocol* (DHCP)
4	Client Terhubung Jaringan Lokal	Eth0	*Address* 192.168.200.10 *Gateway* 192.168.200.1

Dari tabel 3.1 pengelamatan alamat Ip dapat dijelaskan bahwa sumber internet berasal dari *hotspot* atau menggunakan wifi yang terhubung dengan *server*. Kemudian didalam *server* terinstall sebuah sistem operasi seperti linux ubuntu dengan konfigurasi *snort* IDS, untuk pengelamatan Ip pada *server* dapat melakukan penyetingan jaringan dengan menggunakan beberapa perintah.

3.4.4 Konfigurasi *web server*

Dalam membangun *web server* agar berjalan sesuai dengan apa yang diinginkan dengan baik, maka dari itu dibutuhkan suatu proses yang akan dibuat dalam bentuk diagram alir berikut ini :



Gambar 3.6 *Flowchart* Konfigurasi *Web Server*

Untuk penjelasan pada gambar diatas sebagai berikut :

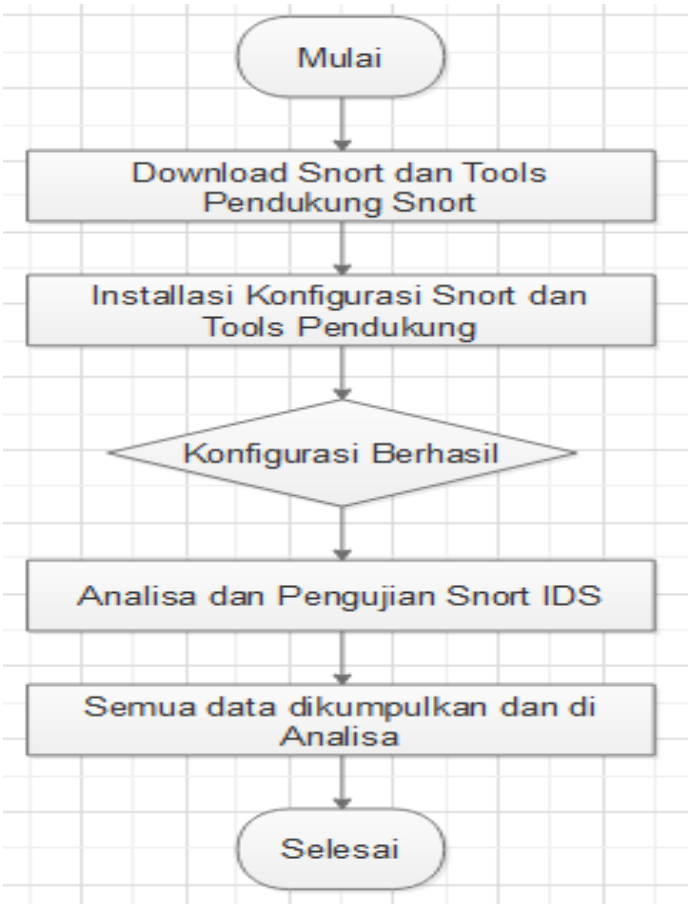
a. Diawali dengan melakukan *installasi Linux Ubuntu 12.04* kemudian mengikuti alur *installasi* hingga selesai penginstallan. Saat telah selesai penginstallan lakukan penyesuaian *IP Address* dan konfigurasi pengroutingan.
b. Setelah selasai dalam penyetingan *IP Address* kemudian mendownload dan penginstallan paket-paket yang dibutuhkan dalam mendukung kinerja *Web Server* agar pembuatan *Web Server* nanti tidak terjadi kesalahan dengan menginstall paket-paket yang di butuhkan berupa *bind9 apache2 php5-mysql mysql-server phpmyadmin libapache2-mod-php5.*
c. Setelah semua paket di install kemudian tahapan mengkonfigurasi *bind9 apache2 php5-mysql mysql-server phpmyadmin libapache2-mod-php5* .

   Bila semua tahap telah berhasil, lakukan tahap akhir yaitu pengujian sistem yang telah dibangun dan pengumpulan data dan menganalisa.

3.4.5 *Security* Jaringan

1. *Security* IDS

Dalam membangun IDS (*Instrusion Detection System*) agar berjalan sesuai dengan apa yang diinginkan dengan baik, dibutuhkannya proses yang akan dibuat dalam bentuk diagram alir berikut :



Gambar 3.8 *Flowchart* Perancangan Konfigurasi IDS

Untuk penjelasan pada gambar diatas sebagai berikut :

a. Setelah selasai dalam penyetingan *IP Address* kemudian penginstallan paket-paket yang dibutuhkan dalam mendukung kinerja *Snort* agar penginstallan *Snort* nanti tidak terjadi kesalahan dengan menginstall paket-paket yang di butuhkan berupa *build-essential, libpcap-dev libpcre3-dev libdumbnet-dev, bison, flex, zlibb1g-dev, liblzma-dev, openssl, libssl-dev, autoconf, libtool. Pkg-config, mysql-server, libmysqlclient-dev, mysql-client, libcrypt-ssleay-perl, liblwp-useragent-determined-perl, apache2, libnetfilter-queue-dev, php5,* dan *tools php5* lainnya.

b. Bila semua tahap telah berhasil, lakukan tahap akhir yaitu pengujian sistem yang telah dibangun dan pengumpulan data dan menganalisa.

2. Serangan DDOS

Bentuk serangan DDOS antara lain adalah :

a. Serangan *Buffer Overflow*, mengirimkan data yang melebihi kapasitas sistem, misalnya paket ICMP yang berukuran sangat besar.

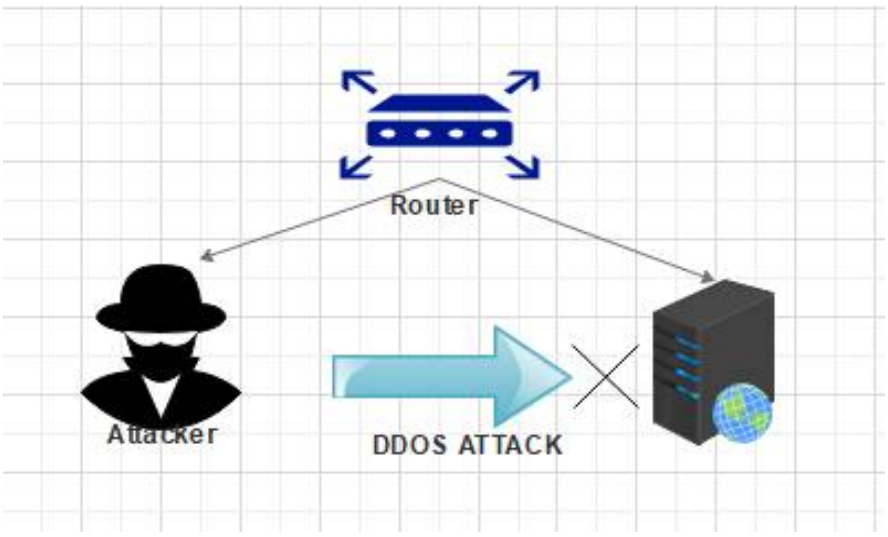
b. Serangan *Smurf*, mengirimkan paket ICMP bervolume besar dengan alamat host lain.

c. ICMP *Flooding*

3. Rancangan Pencegahan Serangan DDOS

a. Menggunakan Router Mikrotik

Sebelum memberikan konfigurasi router ke internet maka sebaiknya memberikan keamanan terlebih dahulu kepada router dengan mengganti *username* dan *password* router, kemudian menutup *service* yang tidak terpakai dan mendisable *Neighboor discovery*.

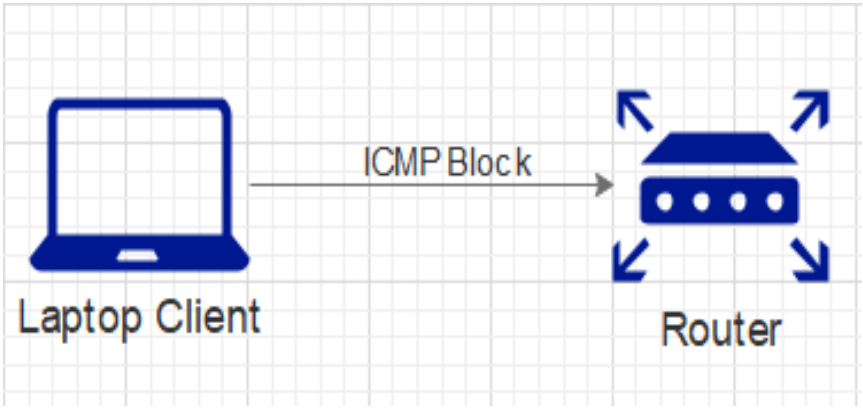


Gambar 3.9 Proteksi serangan DDOS ke *server*

Ketika terdapat paket *new* yang tidak wajar akan dilakukan *grouping* menggunakan *address list* dengan nama *ddosed* dan *ddoser*, setelah alamat IP penyerang dan alamat IP tujuan berhasil ditangkap menggunakan *address-list* maka alamat IP tersebut akan di *drop* oleh *firewall* filter yang dibuat di awal tadi. Dengan begitu perangkat *client* seperti *server* dapat terhindar dari serangan DDOS.

b. ICMP

Internet Control Message Protocol (ICMP) adalah salah satu protocol inti dari keluarga protokol internet. ICMP digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan/ping ke komputer atau *server* tujuan bahwa aksesnya bisa dijangkau.



Gambar 3.10 Blokir Paket ICMP

BAB IV
IMPLEMENTASI DAN HASIL

4.1 Kebutuhan Spesifikasi Minimum Hardware dan Software

Specification Requirement merupakan kebutuhan dalam memenuhi spesifikasi pengaplikasian program agar dapat berjalan dengan baik. *Specification Requirement* terdiri dari dua bagian, yaitu kebutuhan perangkat keras (*hardware requirement*) dan kebutuhan perangkat lunak (*software requirement*).

1. *Hardware Requirement*, dalam program aplikasi ini, penulis menggunakan laptop dan sistem operasi dengan spesifikasi sebagai berikut :
   a. Tipe Laptop : LENOVO IDEAPAD 320
   b. Processor : AMD A4-9120 RADEON R3 CPU 2.20 GHz
   c. Memory : 8,00 GB (7,39 GB usable)
   d. Sistem Operasi : Windows 10 Home Single Language 64 bit
2. *Software* Requirement, adapun perangkat lunak yang dibutuhkan dapat dilihat dengan tabel berikut :

Tabel 4.1 Komponen Perangkat Lunak

No	Perangkat Lunak	Keterangan
1	Sistem Operasi Linux Ubuntu 12.04.5	Bekerja sebagai *server* yang akan menjadi target penyerangan
2	WinSCP	Bekerja upload dan download file melalui protokol ftp
3	PuTTY Configuration	Bekerja sebagai login ubuntu server
4	Sistem Operasi Windows 7	Digunakan pada komputer *Attacker* dan *Client*
5	Mikrotik Router OS 6.33	Digunakan sebagai firewall
6	Winbox	Digunakan sebagai login mikrotik os
7	Torshammer Python Di Ubuntu Desktop	Tools DDOS untuk melakukan serangan

4.2 Pengujian Aplikasi dan Pembahasan

Dalam hal ini sistem yang telah dianalisa dan dikonfigurasi dilanjutkan dengan sistem pengoperasian dan melakukan pengujian untuk melihat hingga sampai mana sistem yang dibuat dapat berjalan dengan baik hingga tujuan.

Dalam proses analisis keamanan *server* menggunakan IDS dan *router firewall server* dari serangan Ddos terdapat bagian utama yang akan berperan yaitu sebagai berikut :

a. Implementasi *Snort*

   Bekerja dalam memonitoring jalur paket data

b. Implementasi *Rule Snort*

   Rule mengelola dan mendeteksi paket data yang melewati *snort* apakah sebuah *attacker* atau paket data tanpa ancaman

c. Implementasi *Web Server*

   Sebagai tempat pengujian serangan DDOS dan notifikasi *snort*

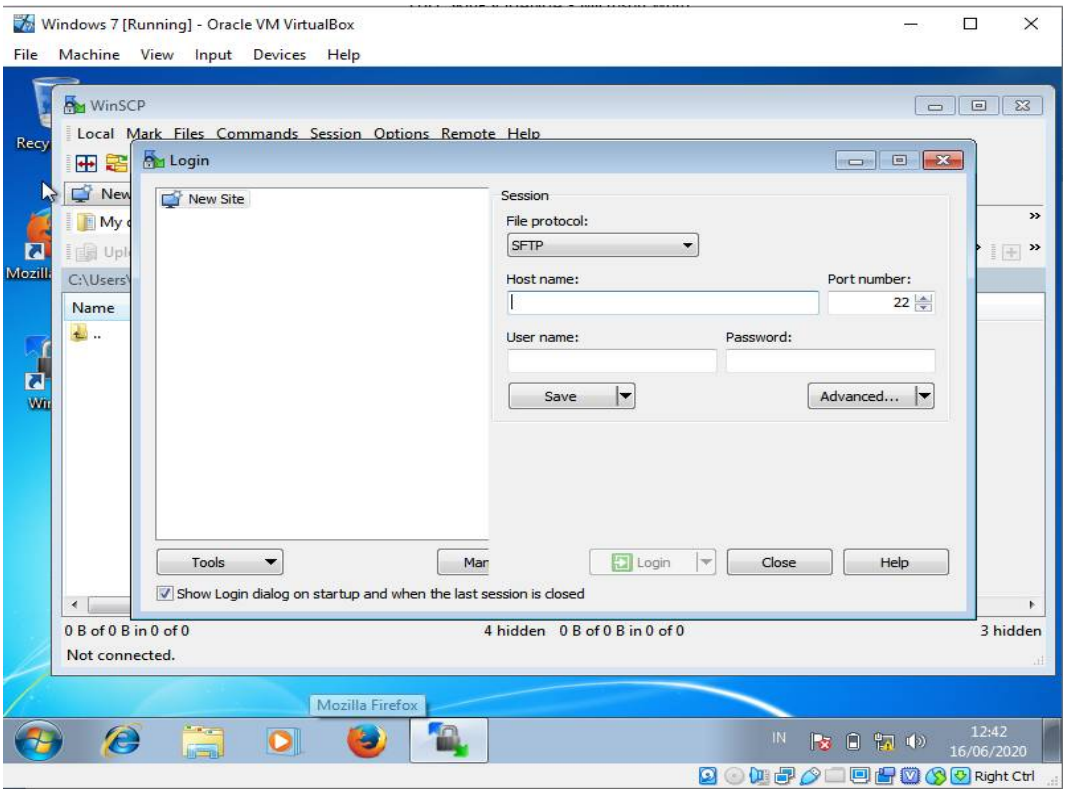
d. Implementasi Serangan DDOS

   Bekerja untuk membanjiri *traffic web server* dengan *request* terus – menerus.

Implementasi serangan ddos menggunakan identifikasi *snort Intrusion Detection System* (IDS) yang nantinya akan mendapatkan hasil dari identifikasi sebuah serangan yang terjadi pada *server* dan menampilkan *output web interface* pada *console terminal*.

1. Upload Web dengan WinSCP, Tampilan Website dan Percobaan FTP Server

Aplikasi WinSCP sudah terinstall di client windows 7, dan dimulai dari tampilan aplikasi WinSCP di Client Windows 7.



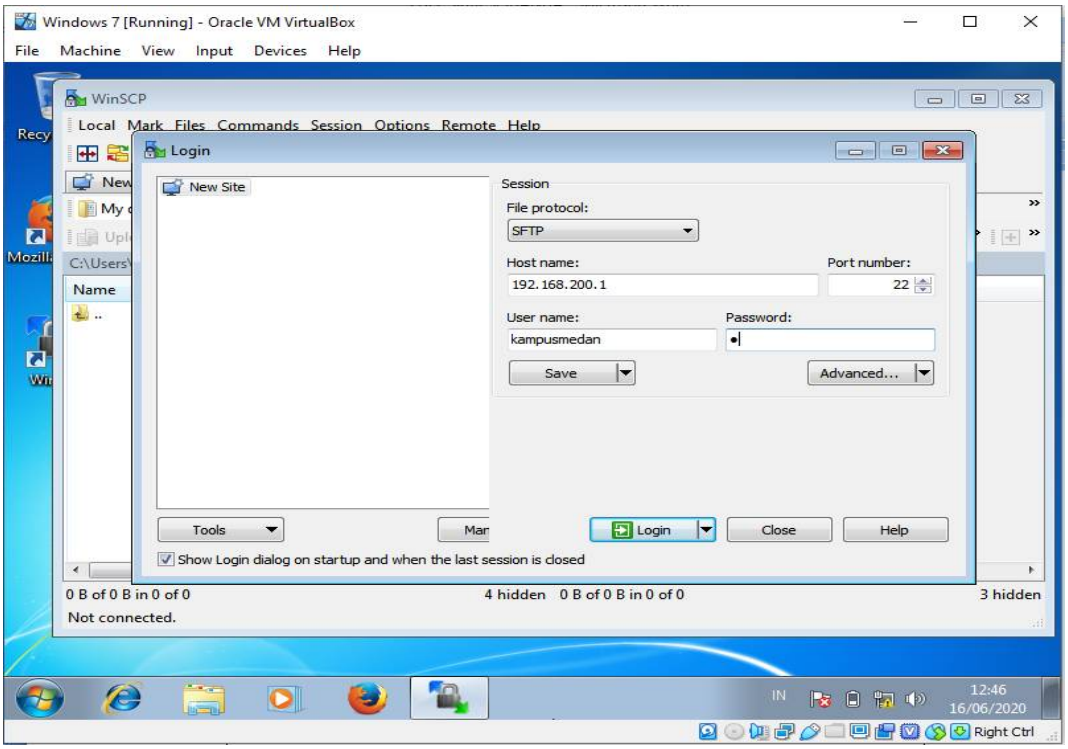
Gambar 4.1 Tampilan aplikasi WinSCP di Client Windows 7

Kemudian login dengan inputan seperti dibawah ini :

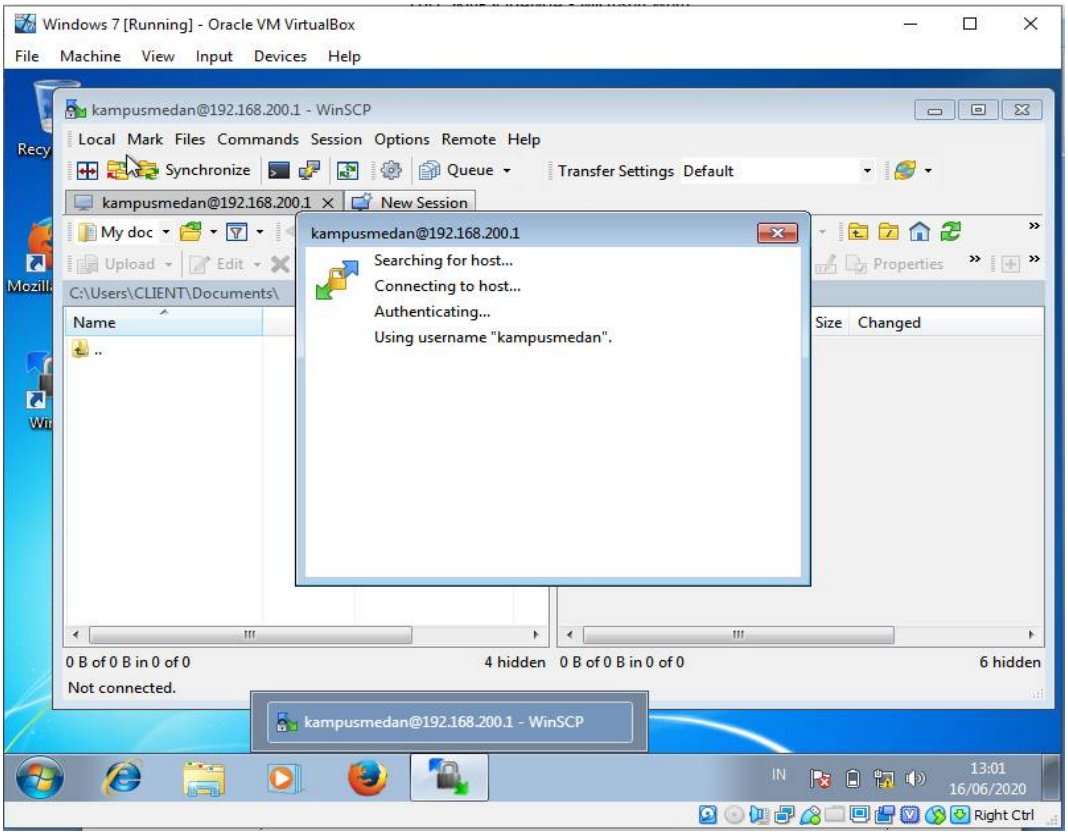
Hostname : 192.168.200.1

Username : kampusmedan

Password : 1

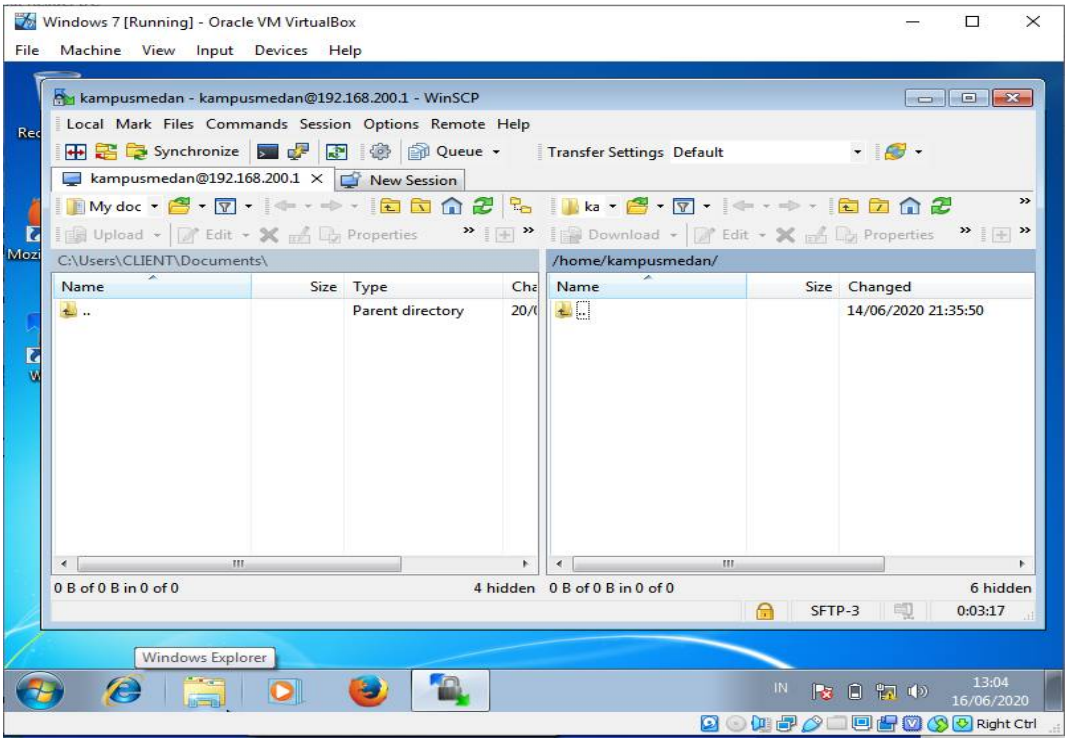


Gambar 4.2 Tampilan Login Di Aplikasi WinSCP

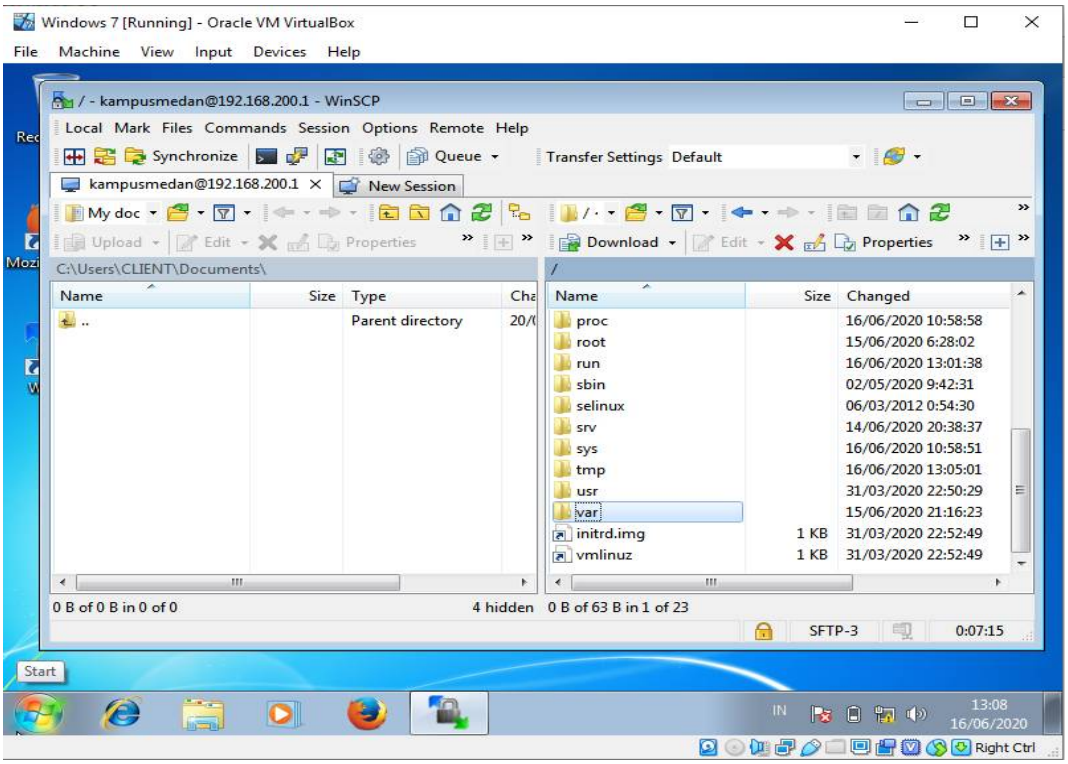


Gambar 4.3 Tampilan Proses Autentikasi, Silahkan tunggu

Tampilan folder pada ubuntu bisa diakses penuh secara GUI pilih folder up

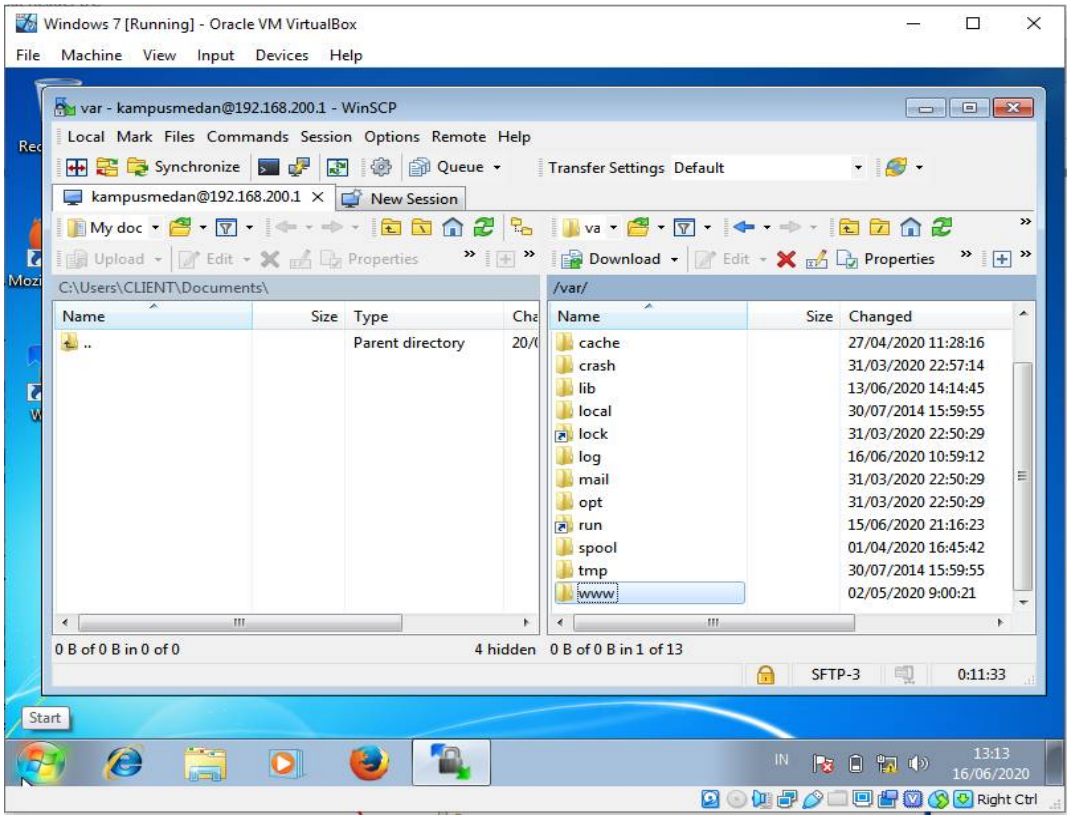


Gambar 4.4 Tampilan WinSCP Folder UP



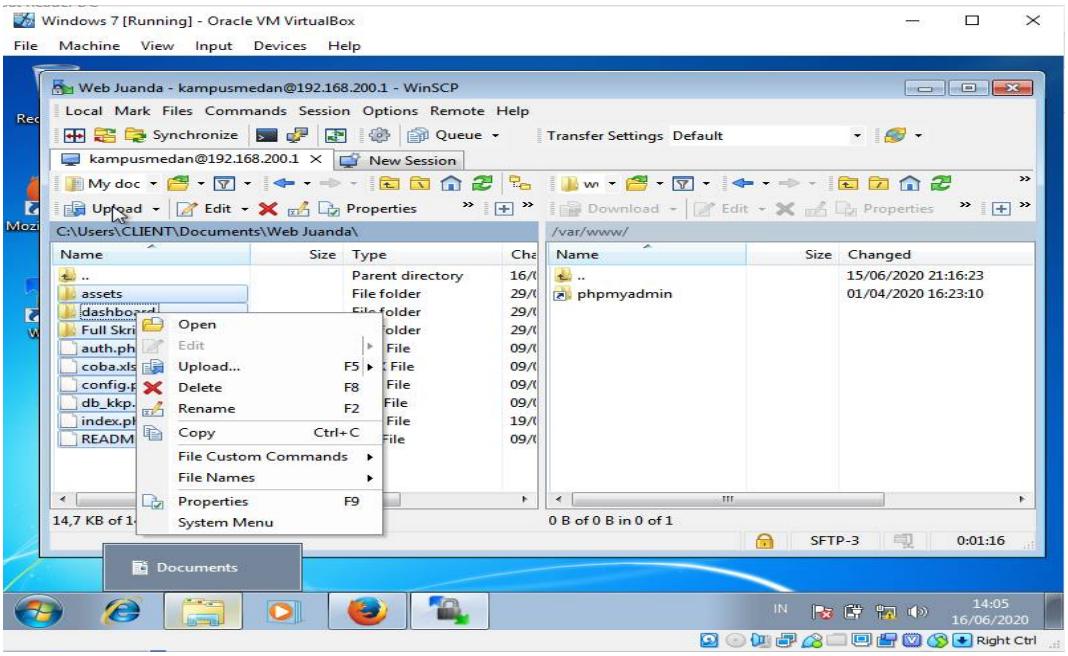
Gambar 4.5 Tampilan WinSCP menuju ke var

Pilih Folder var



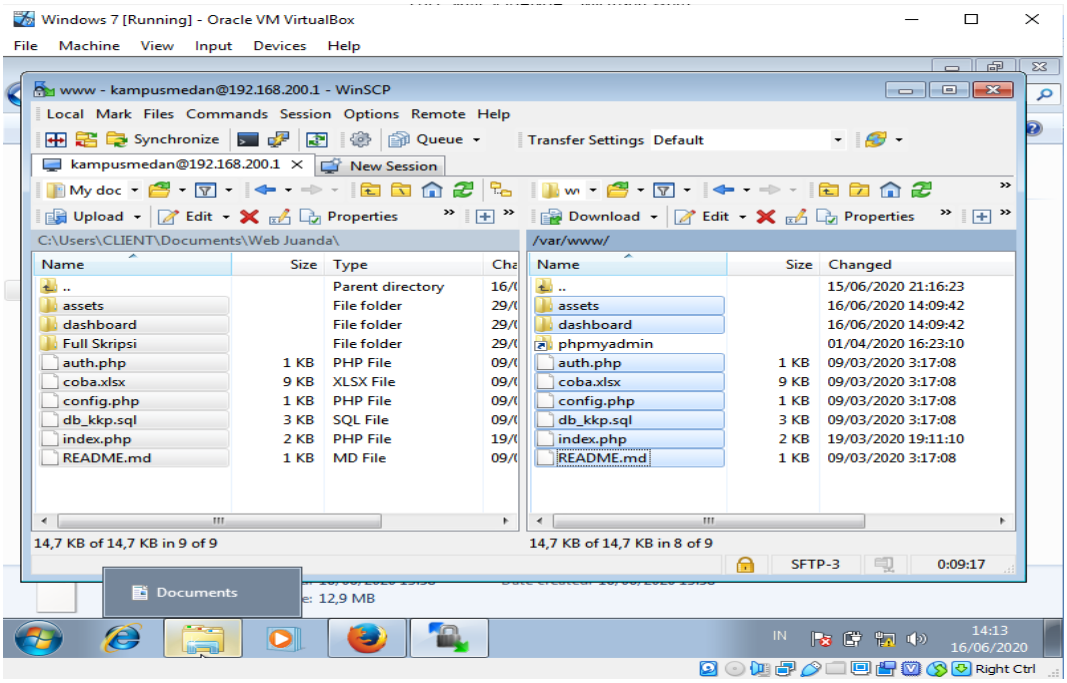
Gambar 4.6 Tampilan WinSCP menuju ke www

Pilih folder www

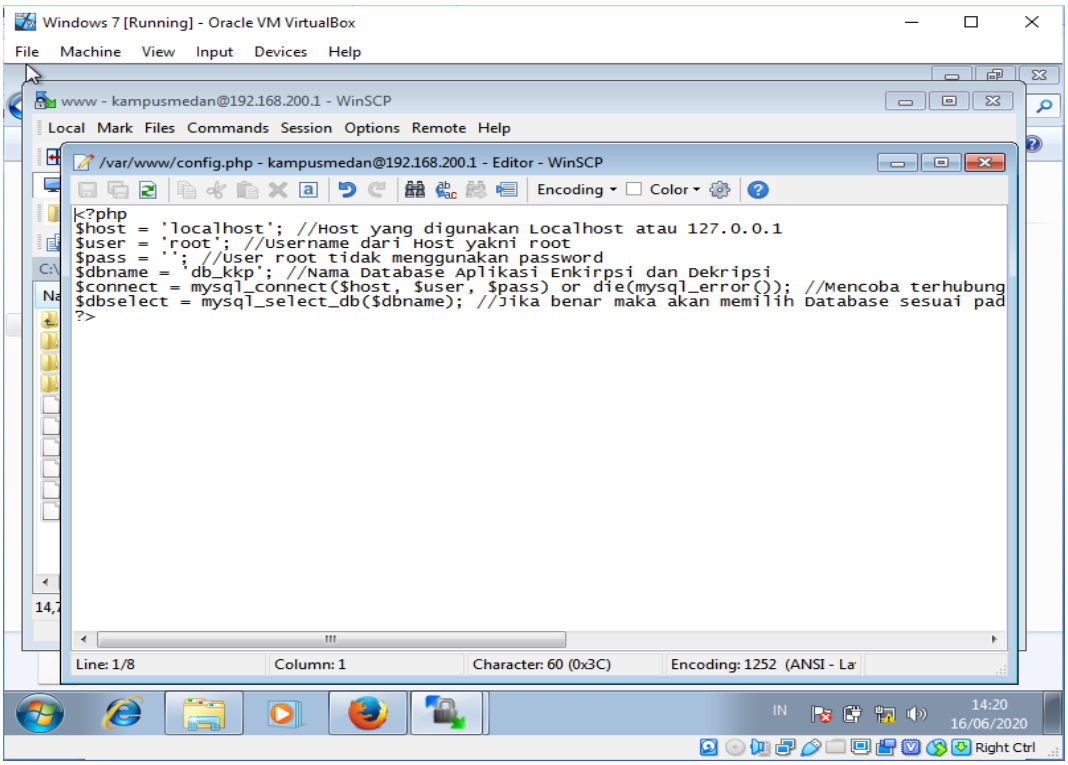


Gambar 4.7 Tampilan Copy File ke WinSCP

Buka folder C\User\Client\Documents\Source Web dan Folder Web copy dan paste \var\www\ WinSCP.

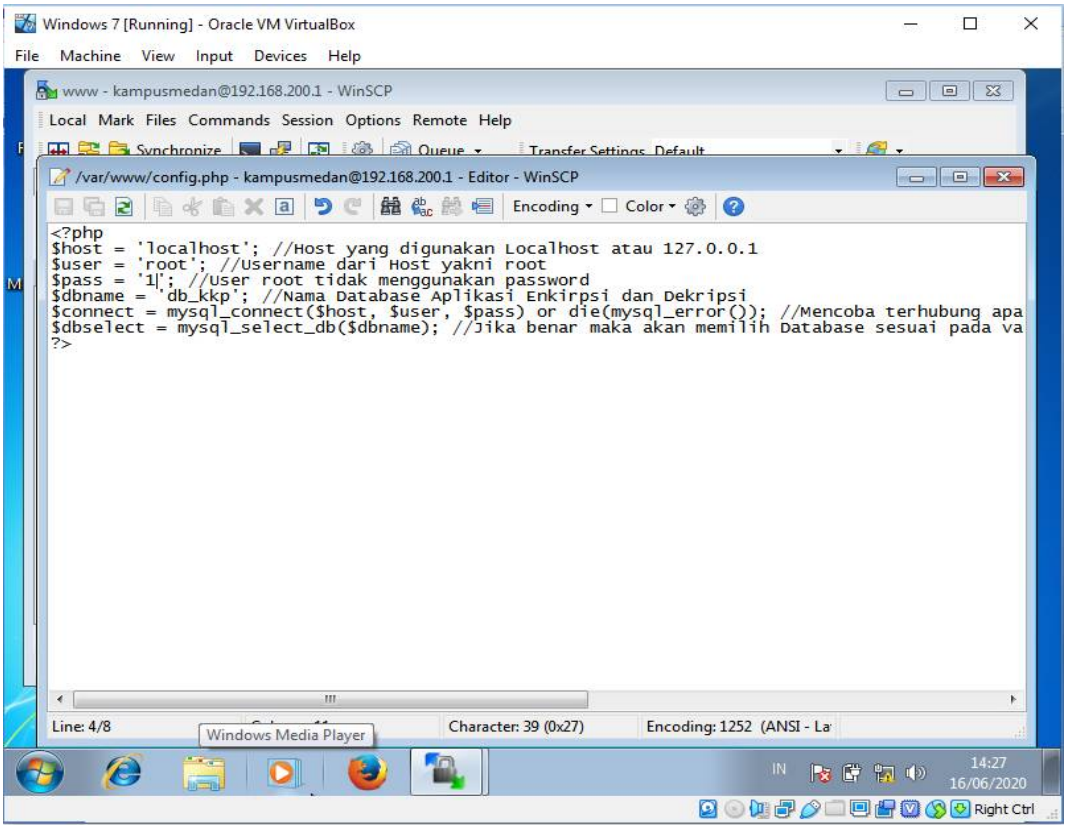


Gambar 4.8 Tampilan WinSCP tersalin

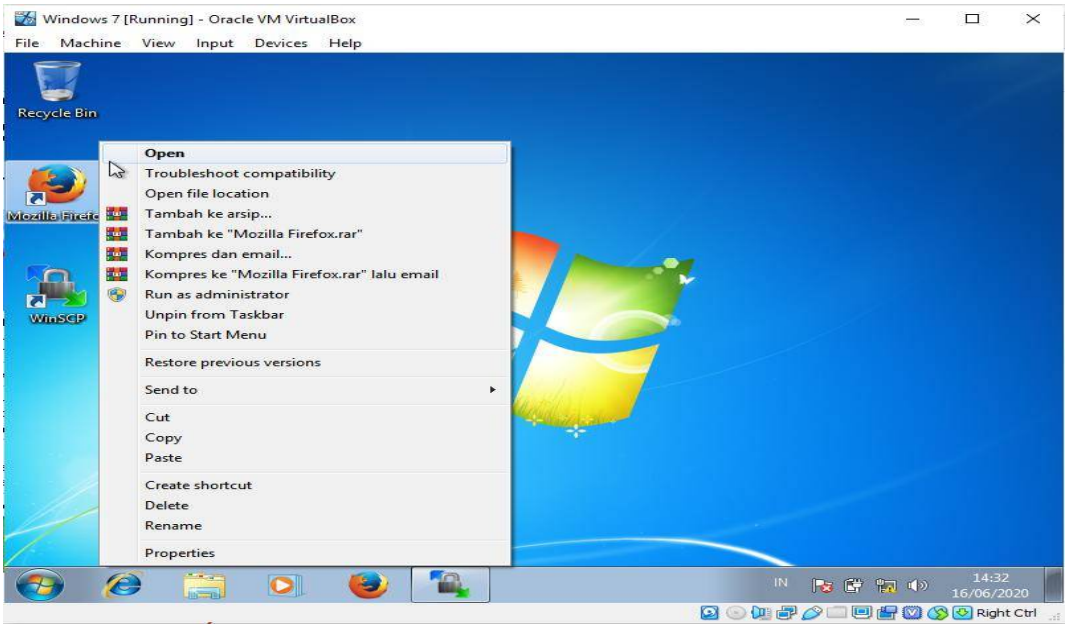


Gambar 4.9 Tampilan default isi Config.php

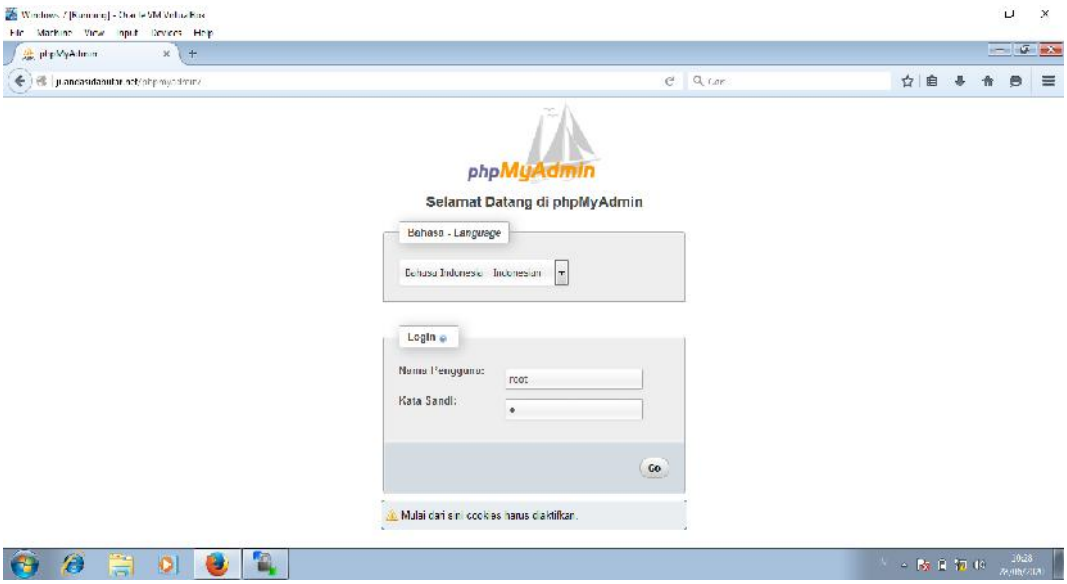
Akan muncul tampilan default seperti ini, bahwa $pass = ‘ ‘ atau masih kosong lalu di isi dengan 1 dan simpan.



Gambar 4.10 Config.php sudah di tambah password

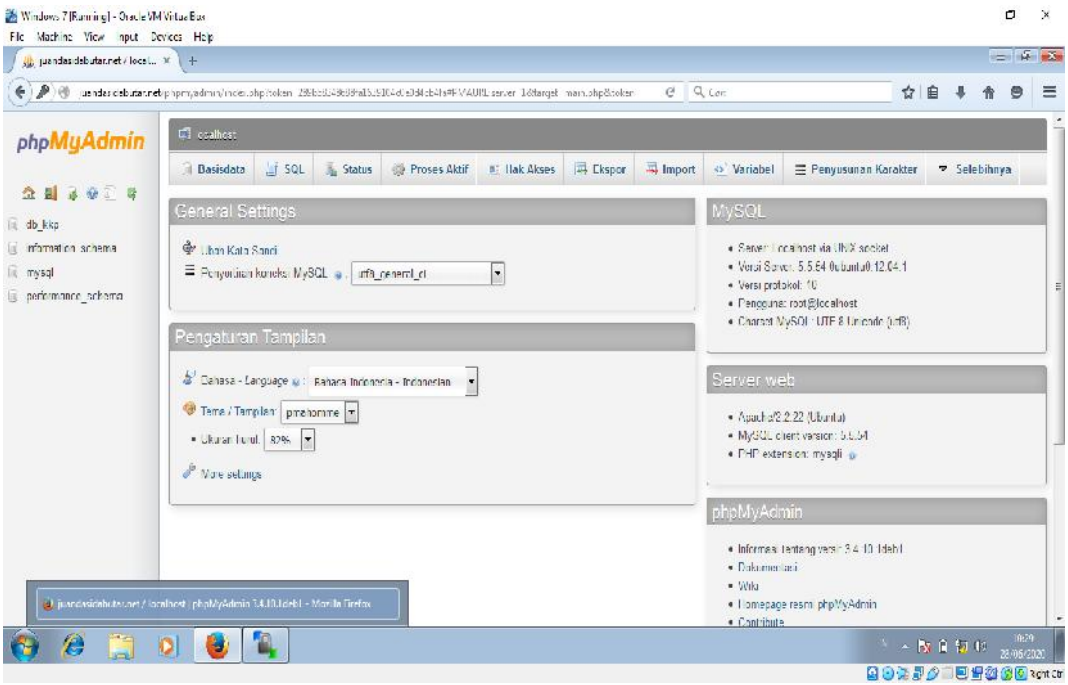


Gambar 4.11 Open Mozilla Firefox di Client windows 7

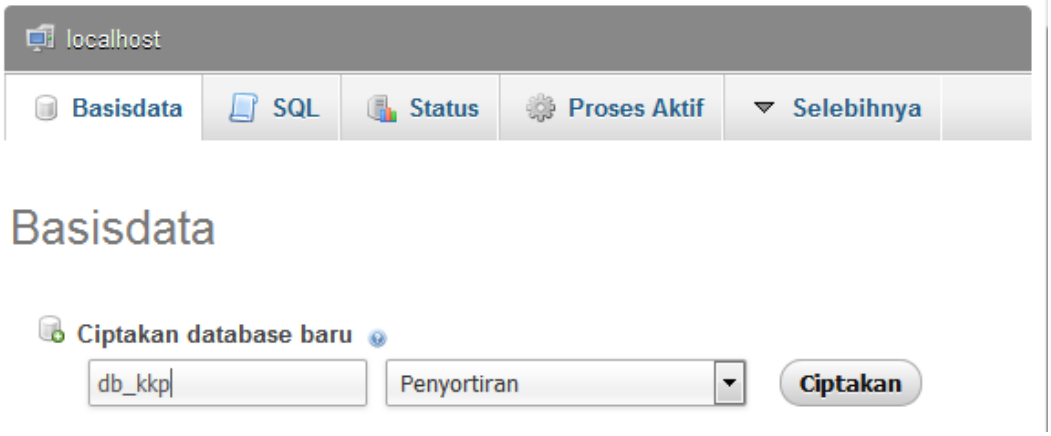


Gambar 4.12 Tampilan login phpmyadmin

Kemudian dengan mengetikkan juandasidabutar.net/phpmyadmin/, lalu mengisi nama pengguna dang root dan password 1.

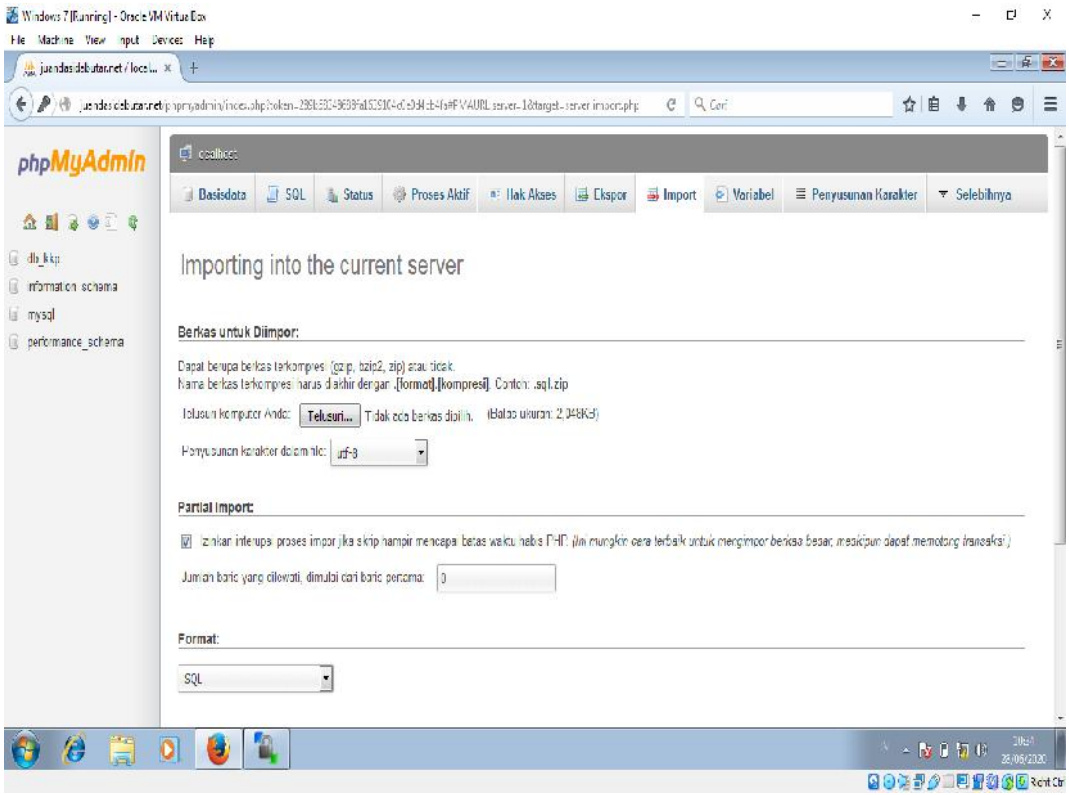


Gambar 4.13 Tampilan login phpmyadmin dari juandasidabutar.net



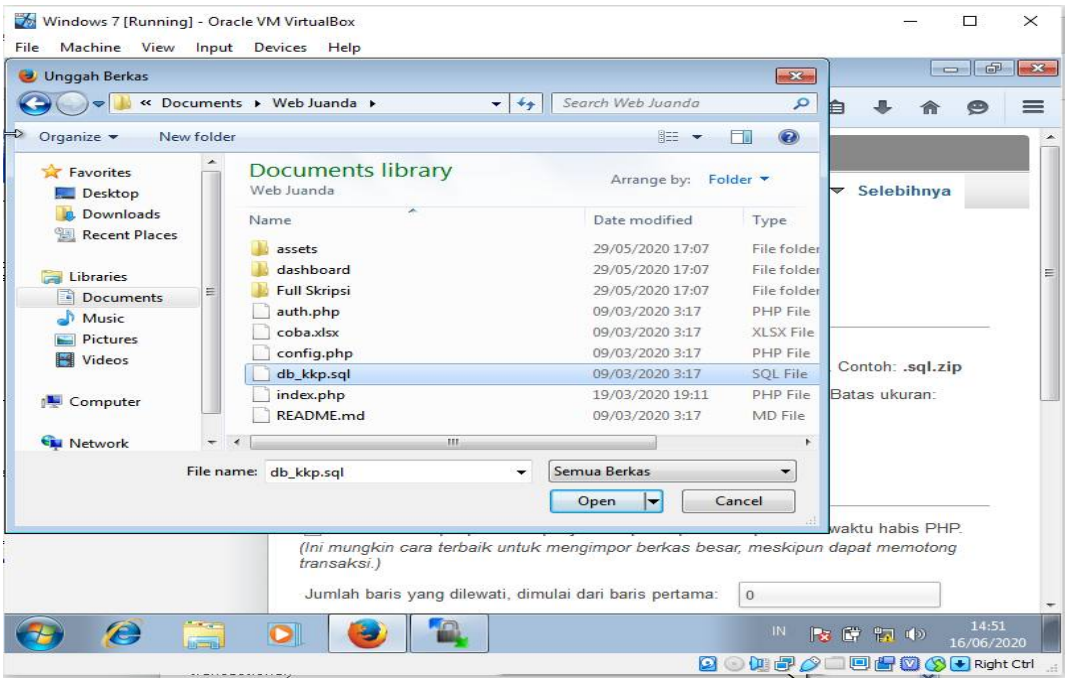
Gambar 4.14 Tampilan membuat database baru

Kemudian diisi pada kolom database = db_kkp kemudian klik ciptakan.

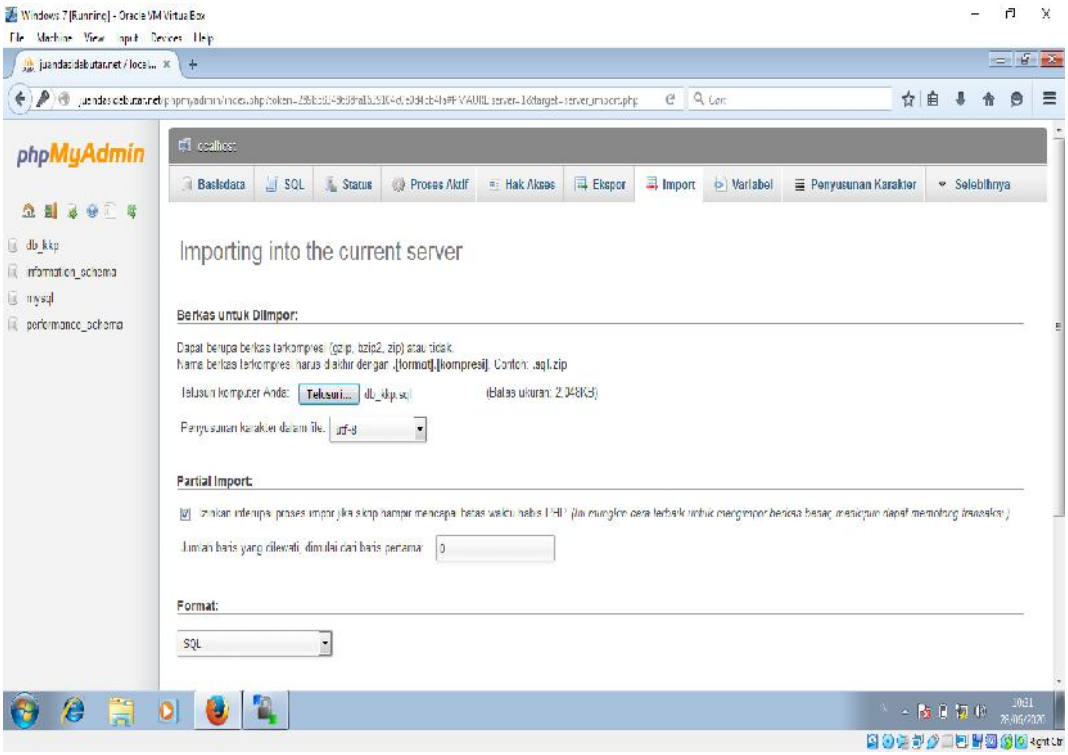


Gambar 4.15 Tampilan menu impor

Kemudian database nya dengan format db_kkp.sql pada folder web juanda, klik open.



Gambar 4.16 Tampilan Impor file db_kkp.sql

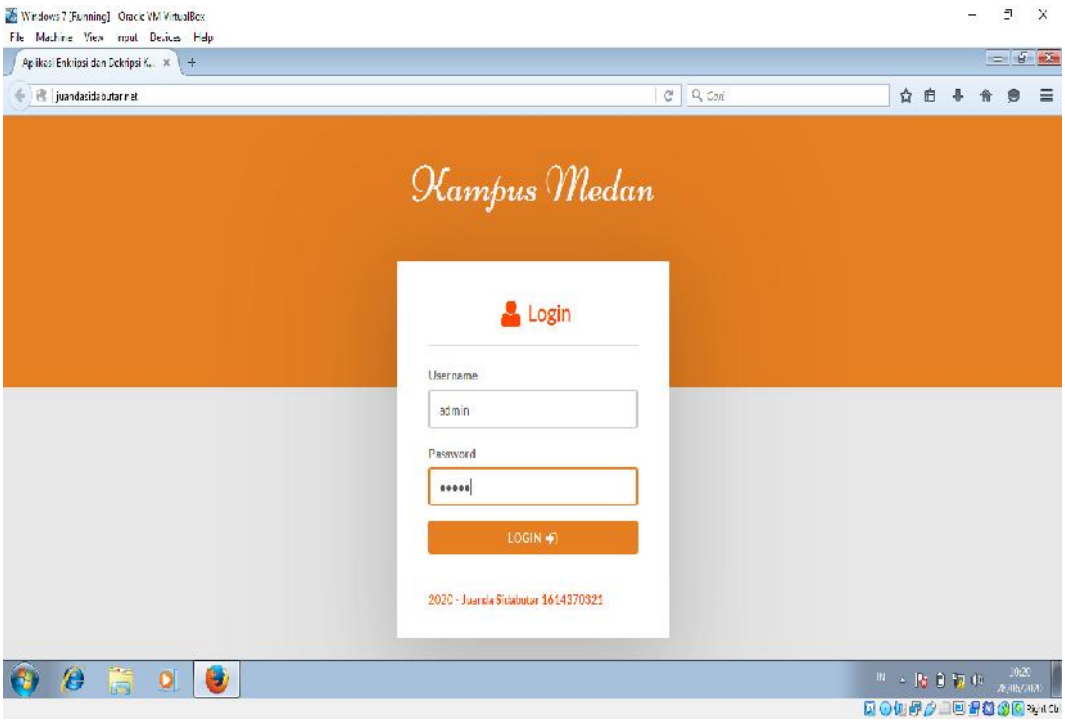


Gambar 4.17 Tampilan sudah diimpor

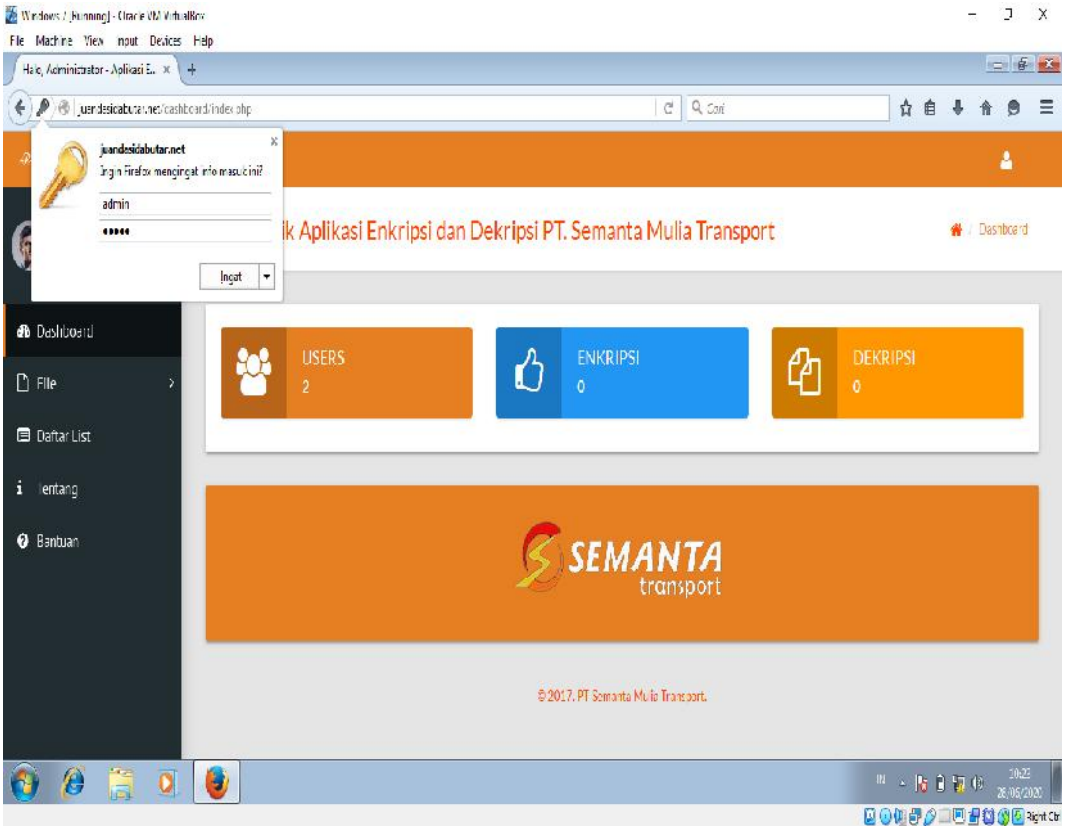
Kemudian klik go, lalu buka juandasidabutar.net di mozila firefox windows 7.

Web server dikenal dapat melayani permintaan pengguna berupa http dari *client* yang terhubung dalam jaringan dan memberikan pelayanan kepada yang meminta informasi berkaitan dengan *website* dan memberikan suatu hasil berupa halaman *web* yang ditampilkan dalam *browser*.

Pada tahap penelitian analisa ini login ke website dengan memasukkan username admin dan password admin, *web server* hanya sebagai tempat pengujian serangan DDOS ke *website* http://www.juandasidabutar.net



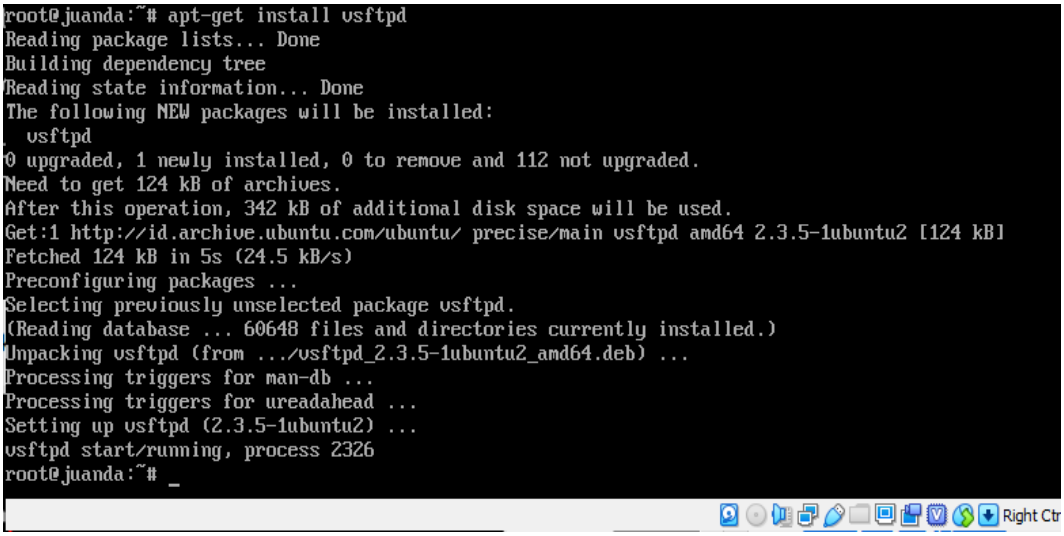
Gambar 4.18 Tampilan *Login Website* di Windows 7 Virtualbox



Gambar 4.19 Tampilan *Website* di Windows 7 Virtualbox

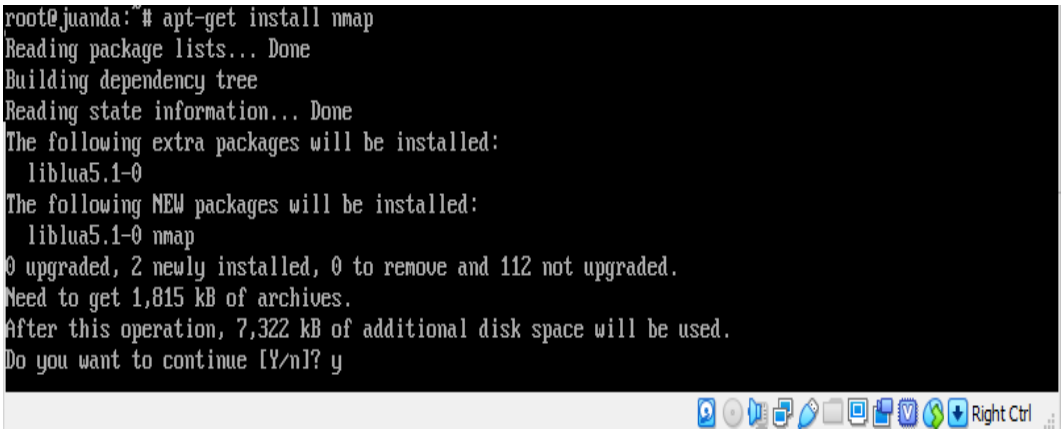
Pada gambar diatas merupakan tampilan dari *website* yang berupa *Hypertext* (HTML) atau *hypermedia* yang dikirimkan ke *user* melalui *World Wide Web*. Untuk menampilkan suatu desain *web* atau isi dari suatu *website*, dibutuhkan sebuah *browser web* atau *software* (perangkat lunak) berbasis *web*. Tujuan dari *web desain* adalah untuk membuat *website* yang meliputi sekumpulan konten online termasuk dokumen dan aplikasi yang berada pada *web server*. Bisa juga sebuah *website* berupa kumpulan teks, gambar, suara dan konten lainnya, serta dapat bersifat interaktif maupun statis. Tampilan web diatas hanya digunakan sebagai target serangan ddos.

Kemudian percobaan FTP Server dengan memulai penginstall vsftpd, yaitu vsftpd merupakan salah satu aplikasi untuk membangun ftp server di lingkungan GNU/Linux dengan lisensi GPL.



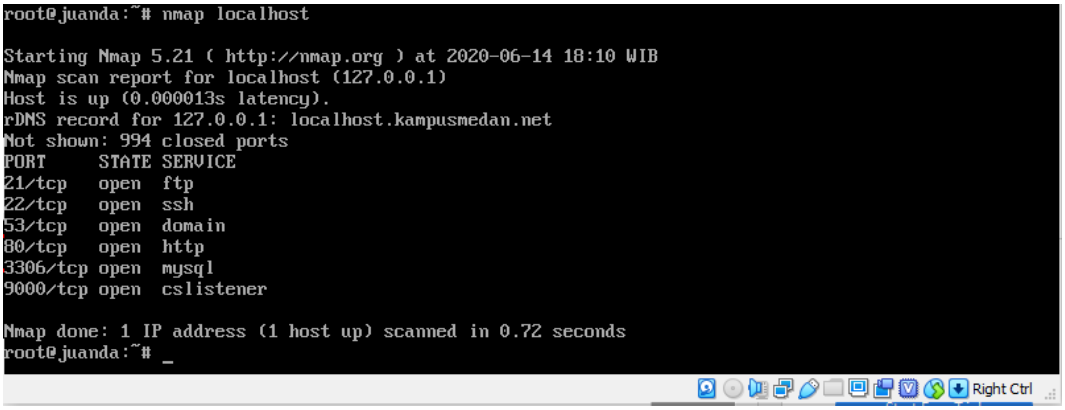
Gambar 4.20 Tampilan installan vsftpd pada linux ubuntu server

Lalu install nmap, dan tekan tombol y kemudian tekan enter.



Gambar 4.21 Tampilan Install nmap

Kemudian mengetikkan perintah dibawah ini untuk menscan port yang terbuka :



Gambar 4.22 Tampilan scan port yang terbuka

Mengecek port FTP apakah sudah bisa listen

Gambar 4.23 Tampilan cek port FTP

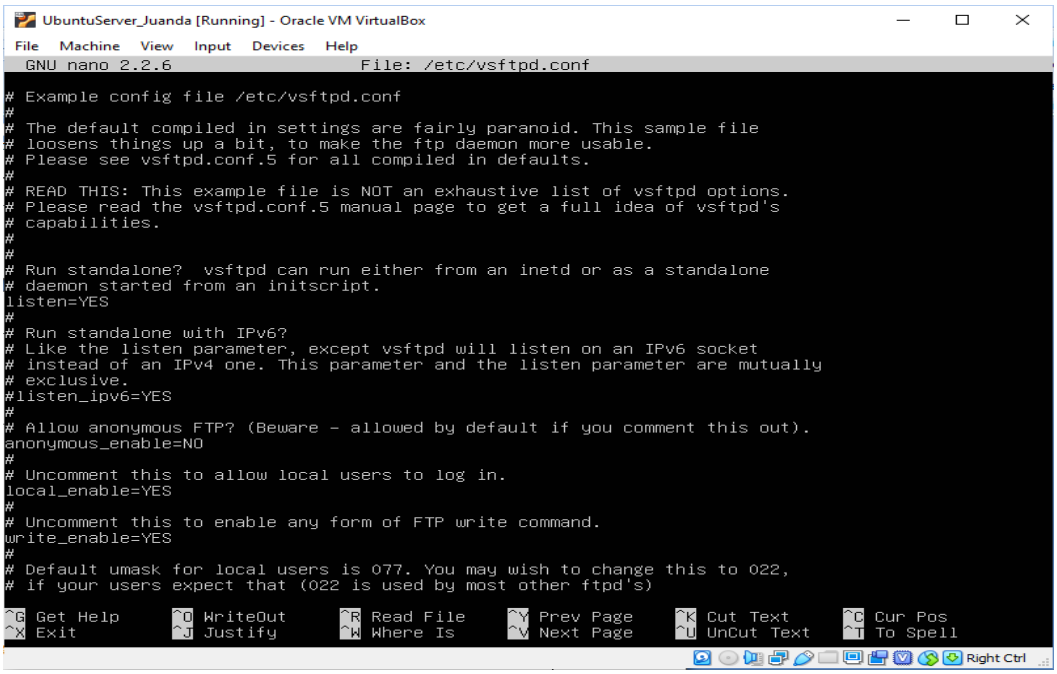
Kemudian membackup file konfigurasi vsftpd original, sebelum melakukan perubahan agar apabila terjadi error pada pengeditan file konfigurasi.Maka tentunya dapat memulai kembali untuk mulai pendeteksian letak kesalahan.

Gambar 4.24 Tampilan backup file vsftpd original

Kemudian dengan mengedit ftp dengan masukkan perintah dibawah

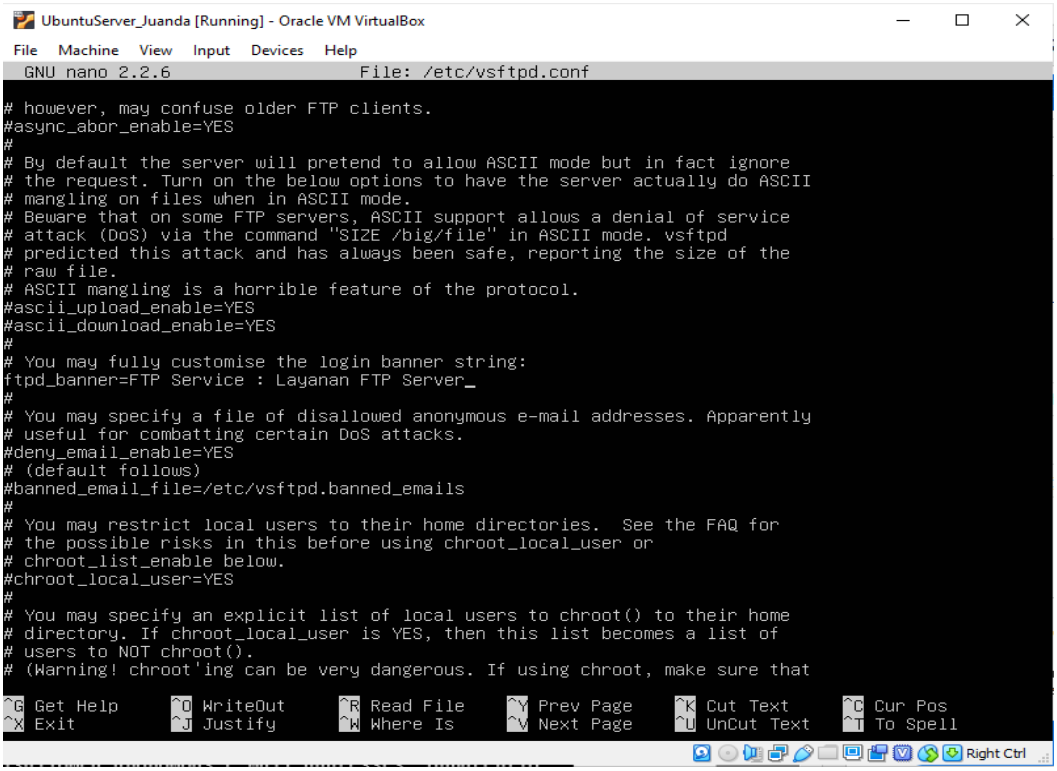
Gambar 4.25 Edit FTP

Lalu anonymous_enable=YES menjadi anonymous_enable=NO dan menghilangkan tanda # pada local _enable=YES dan write_enable=YES.



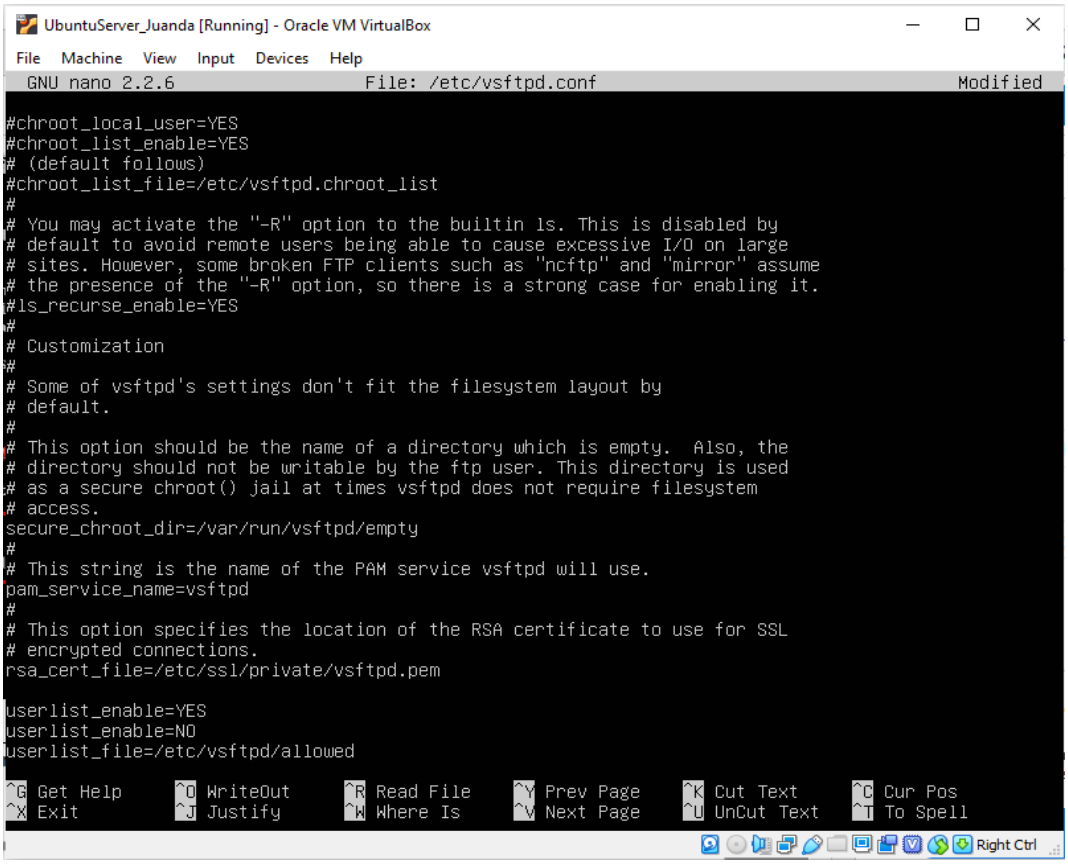
Gambar 4.26 Tampilan Edit FTP

Kemudian turun kursor kebawah,menghapus tanda # dan mengganti perintahnya menjadi seperti dibawah ini.



Gambar 4.27 Tampilan Edit FTP

Kemudian menambahkan perintah paling bawah seperti seperti berikut :



Gambar 4.28 Menambahkan file ftp

Kemudian membuat direktori /etc/vsftpd, lalu nama direktori tersebut dalam hal ini, juanda, sidabutar, kampusmedan.

Gambar 4.29 Membuat direktori di vsftpd

Kemudian memberikan hak akses pada folder tersebut yaitu /etc/vsftpd/allowed dan menambahkan user sesuai directory yang dibuat sebelumnya yaitu juanda, kemudian input dengan password medan.

Gambar 4.30 Memberikan hak akses ke vsftpd

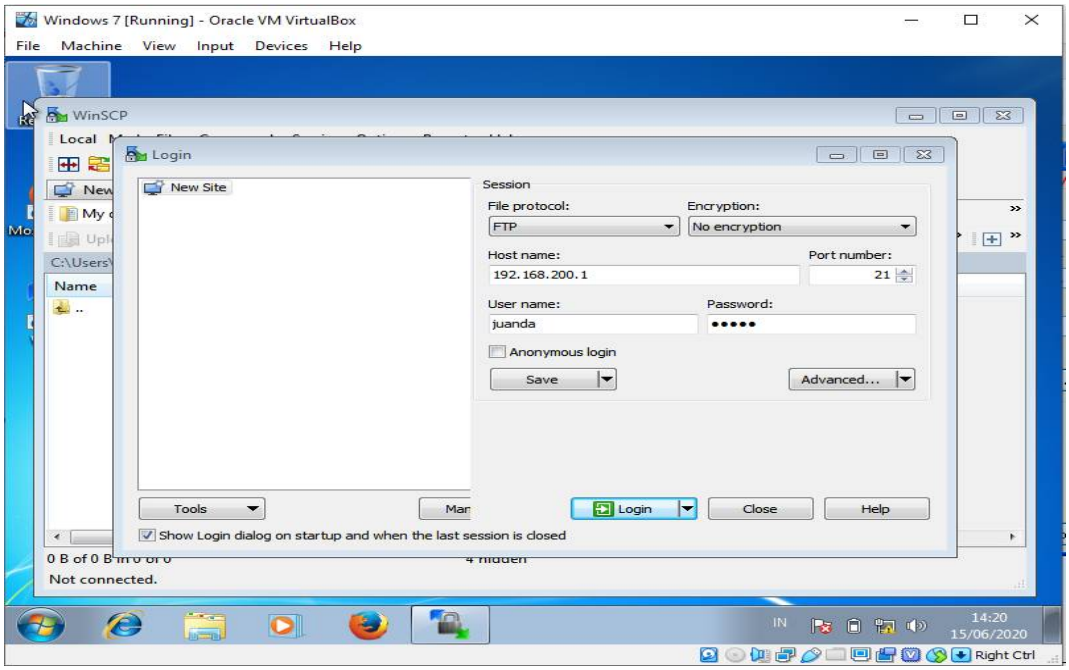
Kemudian restart vsftpd

Gambar 4.31 Restart vsftpd

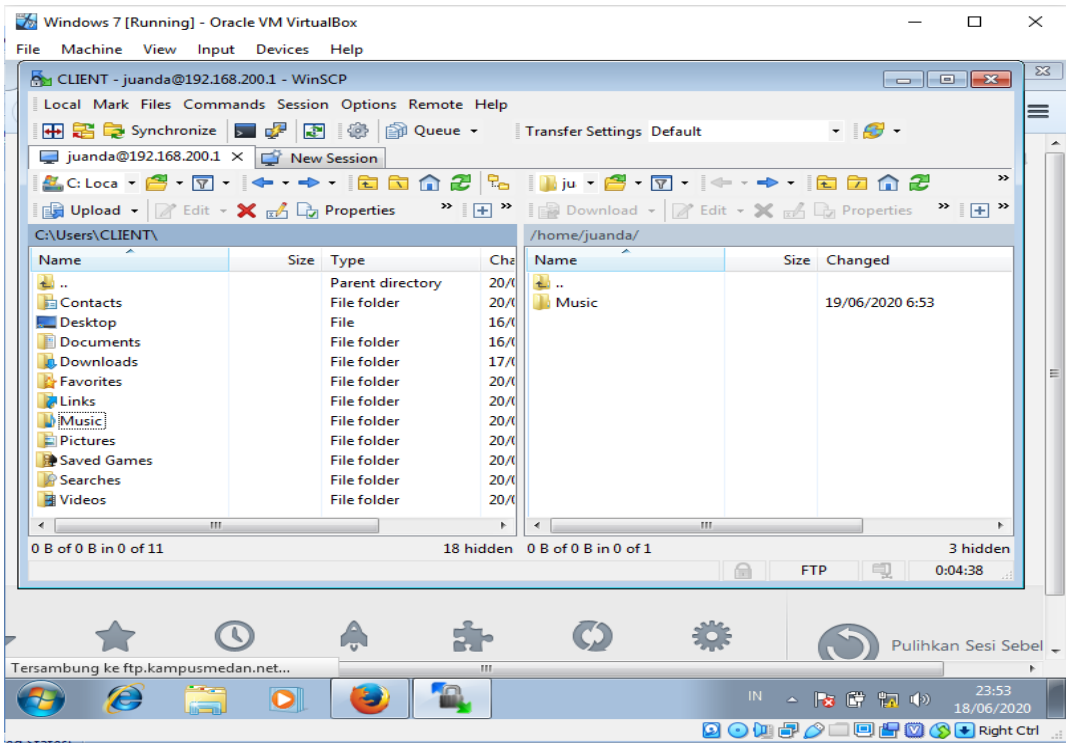
Pengujian FTP Program

Gambar 4.32 Pengujian FTP Server

Pengujian FTP di Client dengan hostname 192.168.200.1, username juanda dan password medan kemudian login.

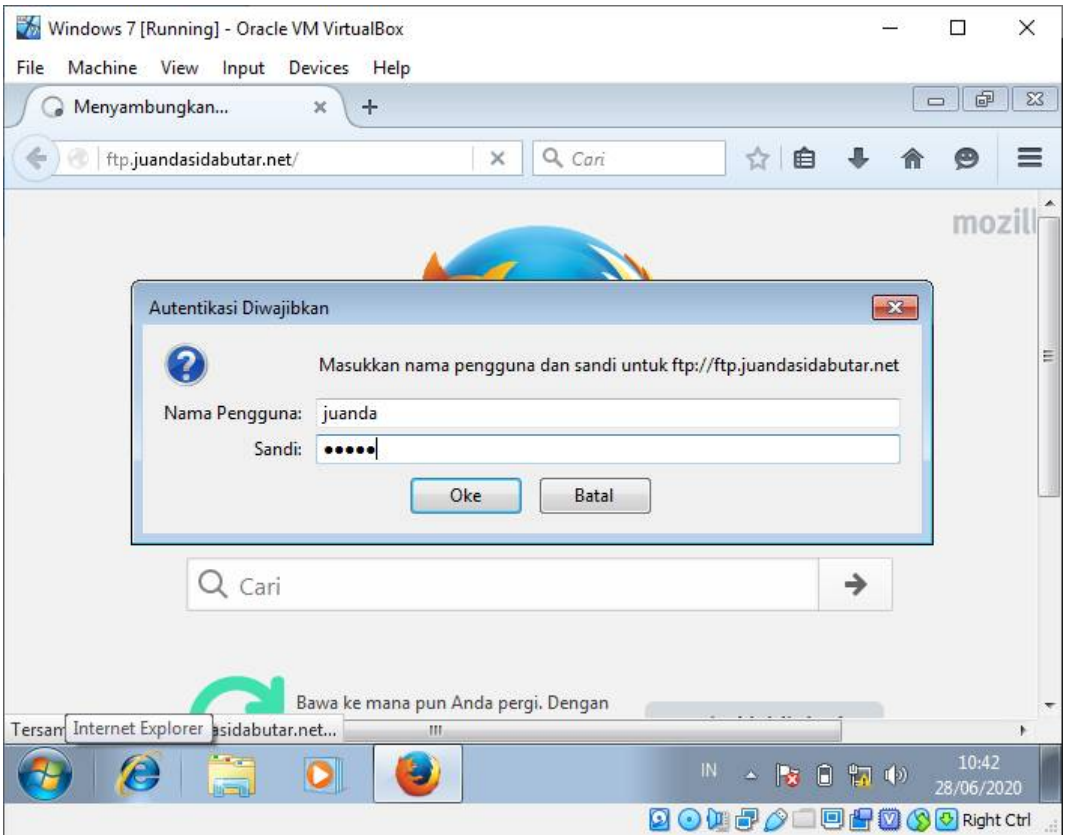


Gambar 4.33 Pengujian Ftp di Client



Gambar 4.34 Copy file dari windows ke directory ubuntu

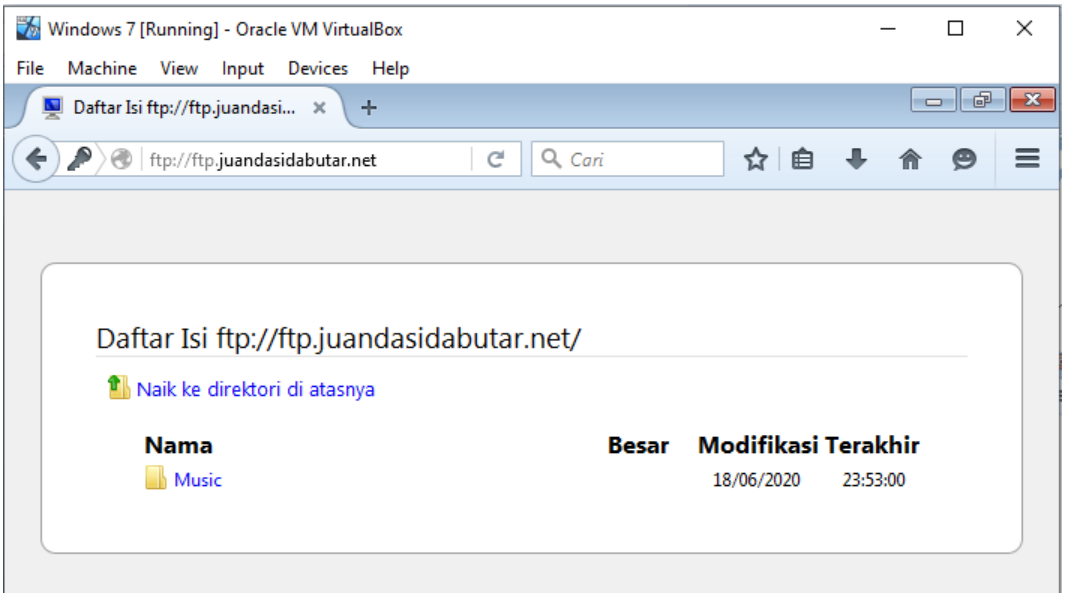
Sehingga tampil seperti gambar 4.34 yang menguji coba copy file my music dari windows ke directory ubuntu, dengan cara mendrag dari kiri ke kanan.



Gambar 4.35 Uji coba login FTP server di browser client

Kemudian pada gambar 4.35 pengujian FTP server pada client dengan browser dengan mengetikkan perintah ftp.juandasidabutar.net lalu memasukkan dengan username juanda dan password medan.

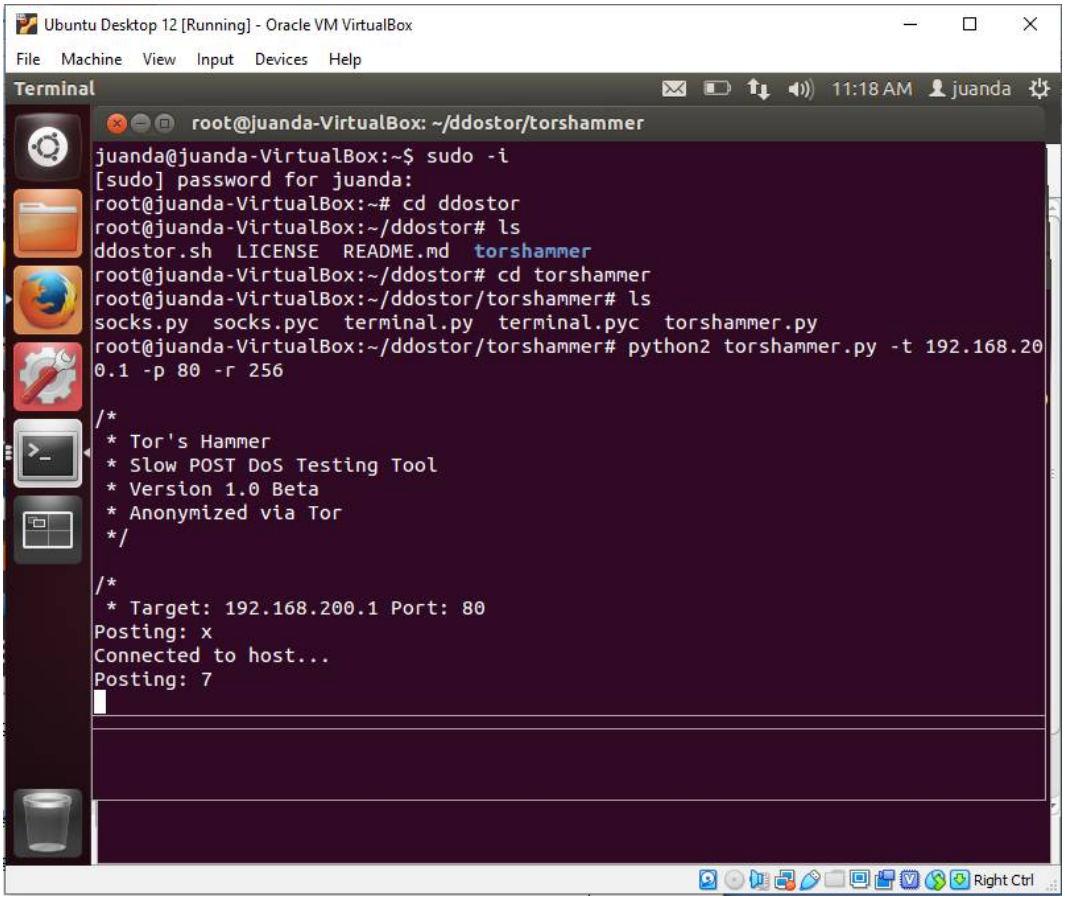
Kemudian hasil tampilan seperti dibawah ini :



Gambar 4.36 Hasil tampilan uji coba ftp server di client

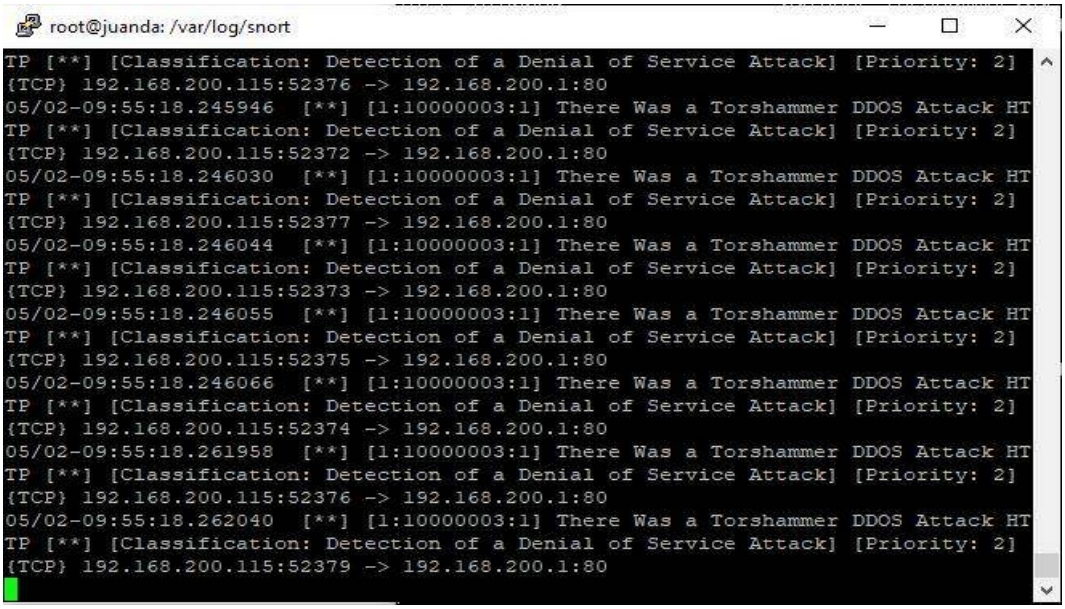
2. Pengujian Serangan *Distributed Denial Of Service* (DDOS) Tanpa *Router Firewall*

Dalam pengujian ini akan menggunakan serangan DDOS yang ada pada sistem operasi Linux Ubuntu Desktop dari beberapa sistem komputer yang menargetkan sebuah *server* agar jumlah *traffic* menjadi terlalu tinggi sampai *server* tidak bisa menghandle *request*nya. Pengujian serangan menggunakan DDOS torshammer python di linux ubuntu desktop. *Script python* yang sudah terinstall otomatis di linux.



Gambar 4.36 Tampilan Serangan DDOS Torshammer di Linux Ubuntu

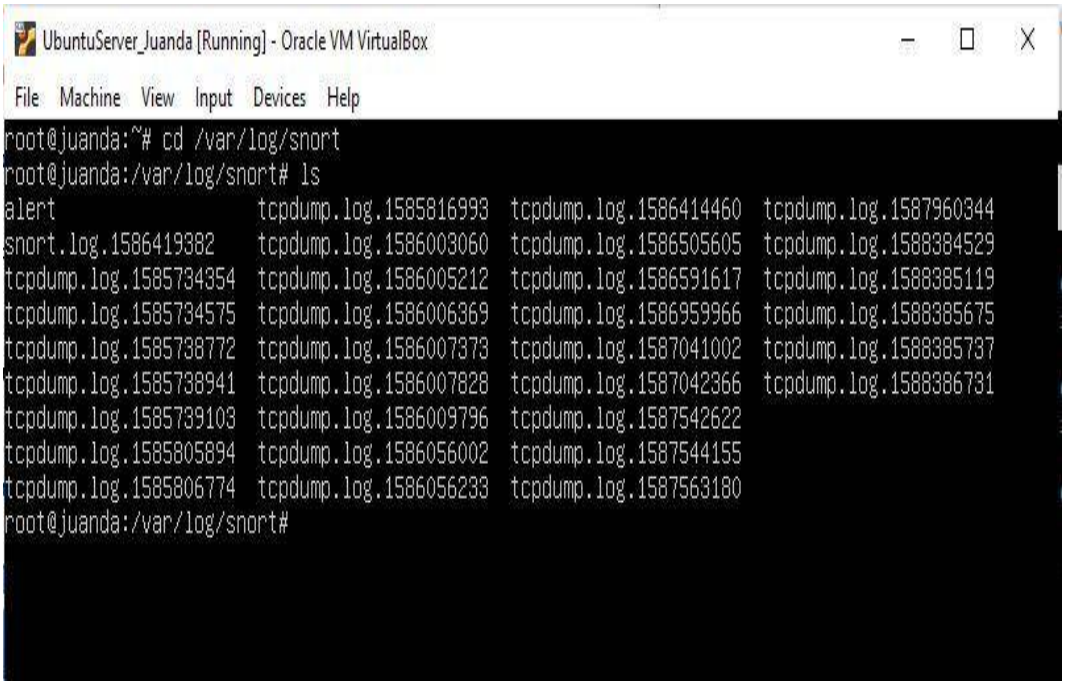
Dalam pengujian diatas dapat dilihat bahwa pengujian menggunakan teknik serangan DDOS torshammer di linux ubuntu dengan teknik kerusakan paling tinggi yaitu dapat memberikan kerusakan pada *server web*.



Gambar 4.37 Hasil Identifikasi Adanya Serangan pada *Mode Console*

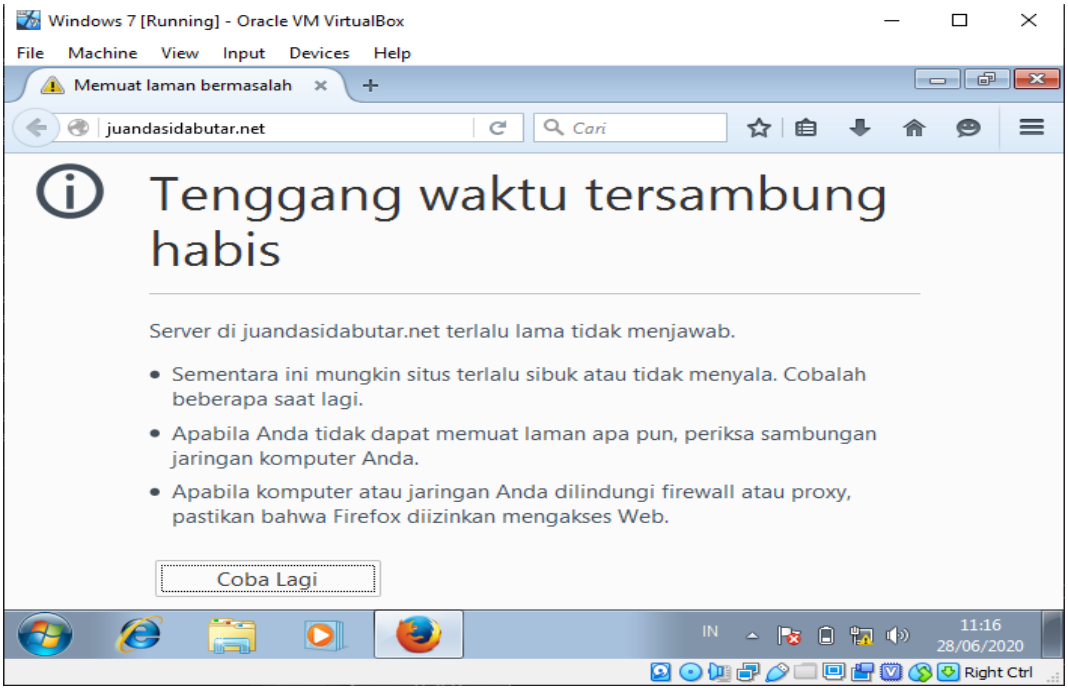
Pada gambar 4.4 dapat dilihat *snort* mendeteksi adanya sebuah serangan DDOS menggunakan tools Torshammmer di ubuntu desktop secara *real time* dalam *mode console*.

Adapun *output snort mode console* seperti berikut :



Gambar 4.38 Tampilan *output snort mode console*

Pada gambar diatas ditampilkan mode *console* hanya memantau suatu serangan dengan menghasilkan *ouput log file*.



Gambar 4.39 Tampilan Web Down di Windows7 Virtualbox Setelah Dilakukannya Serangan

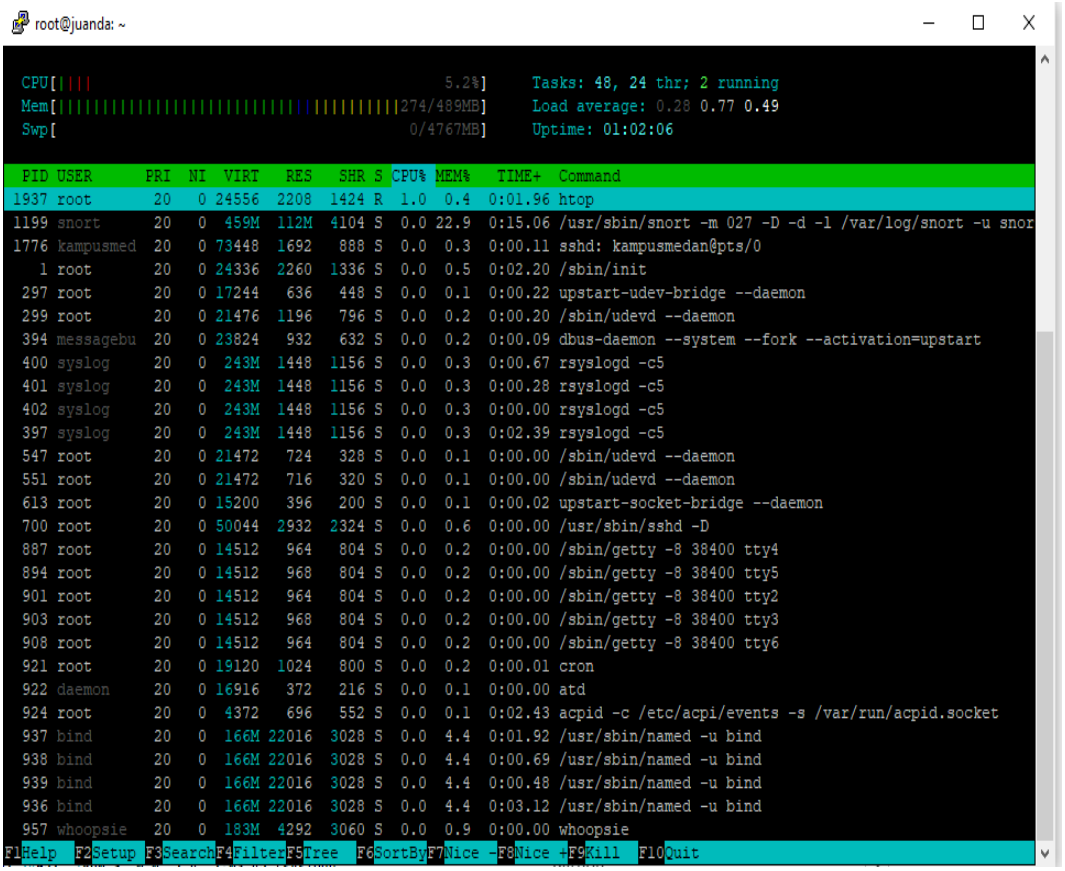
Pada gambar diatas dapat dilihat gejala serangan DDOS sebagai berikut :

a. Kinerja jaringan menurun. Tidak seperti biasanya saat normal atau tidak ada serangan, membuka file atau mengakses situs menjadi lebih lambat.

b. Fitur-fitur tertentu pada sebuah website hilang

c. Website sama sekali tidak bisa diakses.

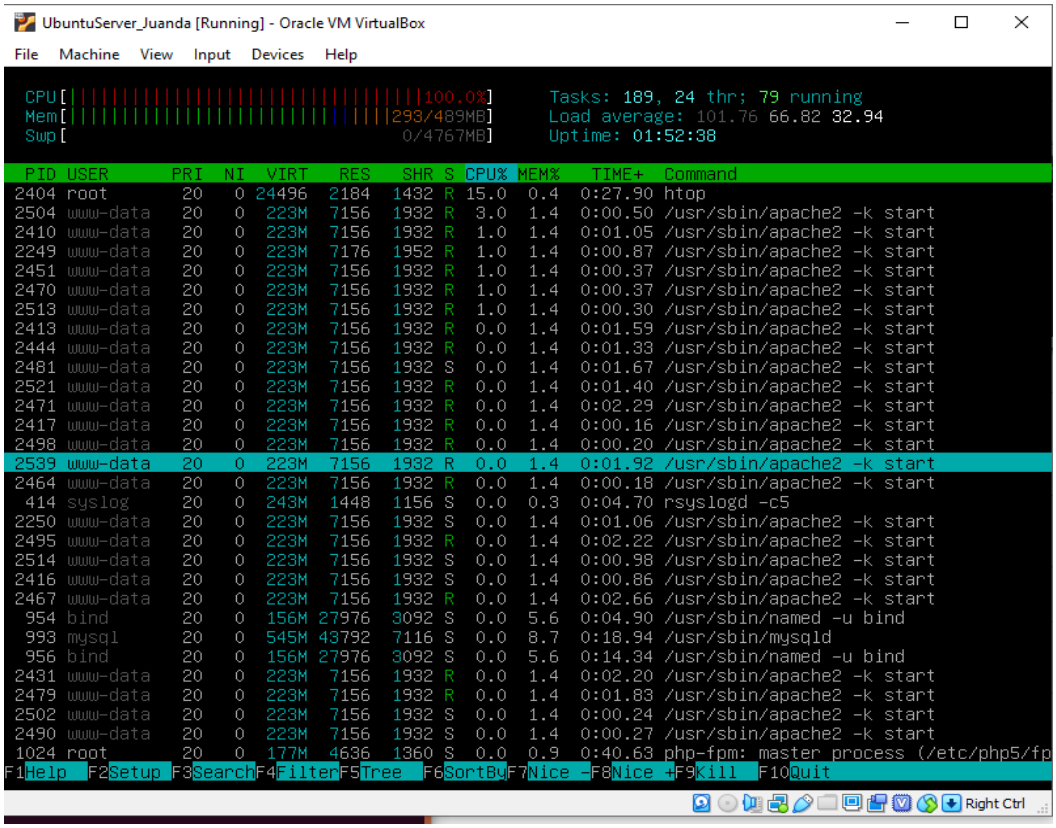
Dari pengujian penyerangan dengan DDOS Torshammer kinerja server dapat diukur menggunakan *system monitor* HTOP untuk dapat dimonitor kinerja jaringan, CPU, dan memori yang berjalan pada server, dapat dilihat dengan tampilan berikut :



Gambar 4.40 Tampilan monitoring kinerja server web saat keadaan normal

Pada gambar 4.7 kinerja CPU, Memory, dan Swap pada system monitoring server ubuntu hanya menunjukkan kinerja CPU yang bekerja menjalankan sistem server dan tak menunjukkan adanya tanda serangan apapun dalam menjalankan kinerja server, sehingga dapat dikatakan kondisi server berjalan dengan keadaan normal, sebab server bekerja dengan normal dan belum adanya serangan DDOS pada server.

Ketika terjadinya sebuah serangan DDOS pada server, system monitoring server ubuntu akan menunjukkan perubahan seperti gambar berikut :



Gambar 4.41 Tampilan monitoring server web saat ada serangan DDOS

Pada gambar 4.8 dapat dilihat monitoring HTOP pada server memiliki 3 core yaitu CPU, Memory, dan Swap, pengujian serangan pada server dapat mempengaruhi kinerja server dengan meningkatnya kinerja pada CPU 100 % yang secara terus menerus dibebani oleh serangan DDOS dan lamanya berjalan dapat dilihat di bagian uptime 01:52:38 dengan kinerja yang berjalan sebanyak 189 serta running sebanyak 79.

Tabel 4.2 Analisa Server Dalam Keadaan Normal

No	Name Core	Nilai
1	CPU	5.2 %
2	Memory	274/489 MB
3	Swap	0/4767 MB
4	Load Average	0.28 0.77 0.49
5	Task	48, 24 thr; 2 running
6	Uptime	01:02:06

Saat keadaan normal kondisi CPU secara realtime kondisi normal hanya 5.2% kemudian pemakaian memory 274MB dalam kurun waktu 01:02:06 tidak ada serangan.

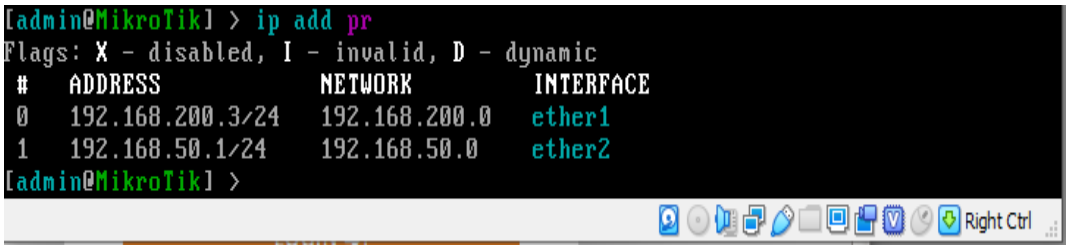
Tabel 4.3 Analisa Kondisi Server saat ada serangan

No	Name Core	Nilai
1	CPU	100 %
2	Memory	293/489 MB
3	Swap	0/4767 MB
4	Load Average	101. 76 66.82 32.94
5	Task	189, 24 thr; 79 running
6	Uptime	01:52:38

Pengujian serangan pada server dapat mempengaruhi kinerja server saat ada serangan menuju ke server service dengan meningkatnya kinerja pada CPU 100 % yang secara terus menerus dibebani oleh serangan DDOS dan lamanya berjalan dapat dilihat di bagian uptime 01:52:38 dengan kinerja job yang sedang berjalan sebanyak 189 serta running sebanyak 79.

3. Pengamanan Web Block Paket ICMP Pada Mikrotik Os Dengan Login Menggunakan Winbox

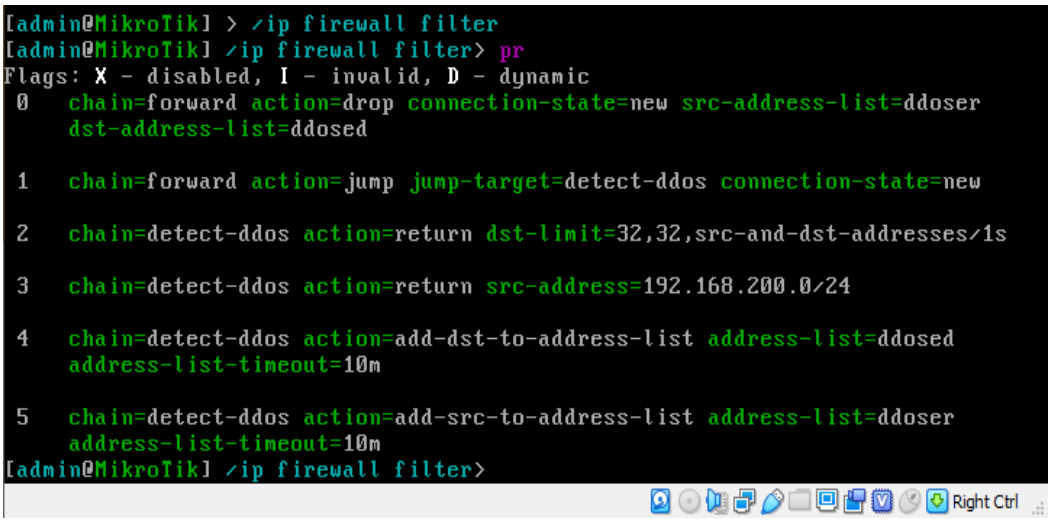
Mikrotik OS sudah diinstall di virtualbox dan di ceklis address sebagai berikut :



Gambar 4.42 Setting IP Interface mikrotik

Untuk ether1 menggunakan ip 192.168.200.3/24 dan ether2 menggunakan ip 192.168.50.1/24 yang diatur secara manual DHCP

Kemudian melakukan konfigurasi dengan membuat *rule firewall filter* dengan *action drop* terhadap alamat ip asal ddoser dengan tujuan alamat ip ddosed.



Gambar 4.43 Konfigurasi IP Firewall Filter

Dari gambar 4.43 diatas imputan sebagai berikut :

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

Kemudian menangkap semua koneksi *new* dan membuat *chain* baru yaitu *detect-ddos*

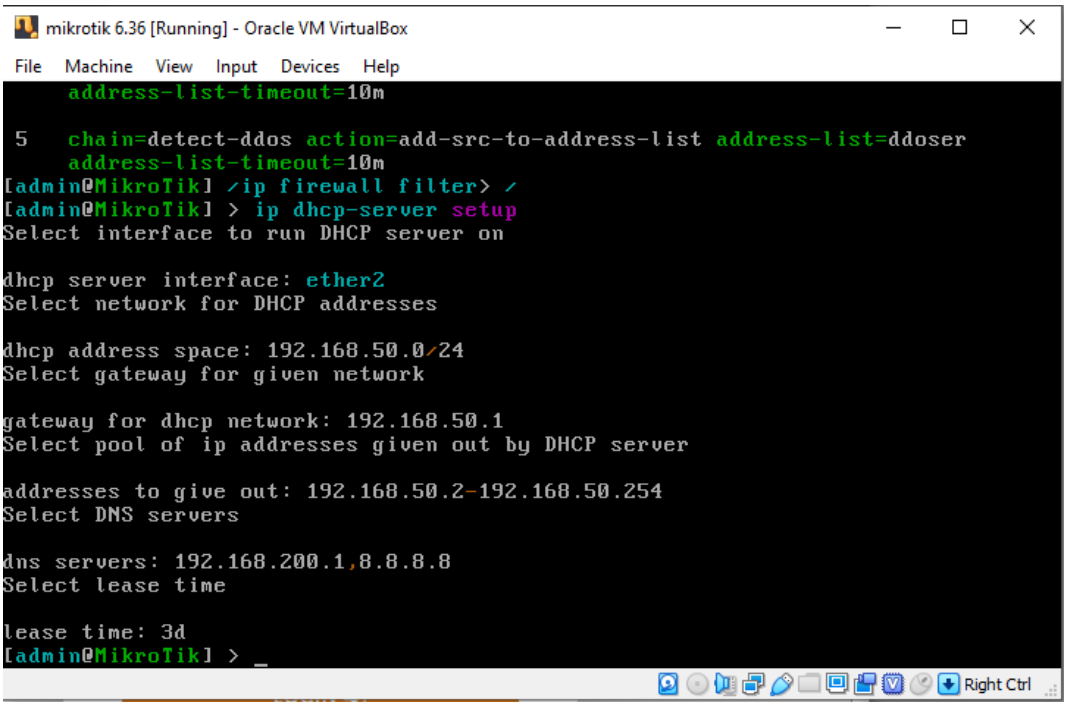
```
/ip firewall filter
add chain=forward connection-state=new action=jump-
target=detect-ddos
```

Kemudian membuat *rule firewall* sebagai berikut :

```
/ip firewall filter
add chain=detect-ddos dst-limit=32,32,src-and-dst-
addresses/1s action=return
add chain=detect-ddos src-address=192.168.200.0/24
```

Dengan *rule firewall* diatas, maka ketika terdapat paket *new* yang tidak wajar, misalnya diatas 32 paket selama 1 detik, maka *firewall* akan melakukan penandaan terhadap alamat asal dan alamat tujuan menggunakan *address list*. Alamat ip penyerang akan melakukan grouping dengan nama ddoser kemudian untuk alamat ip target maka akan dilakukan *grouping* dengan nama ddosed.

```
/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
```

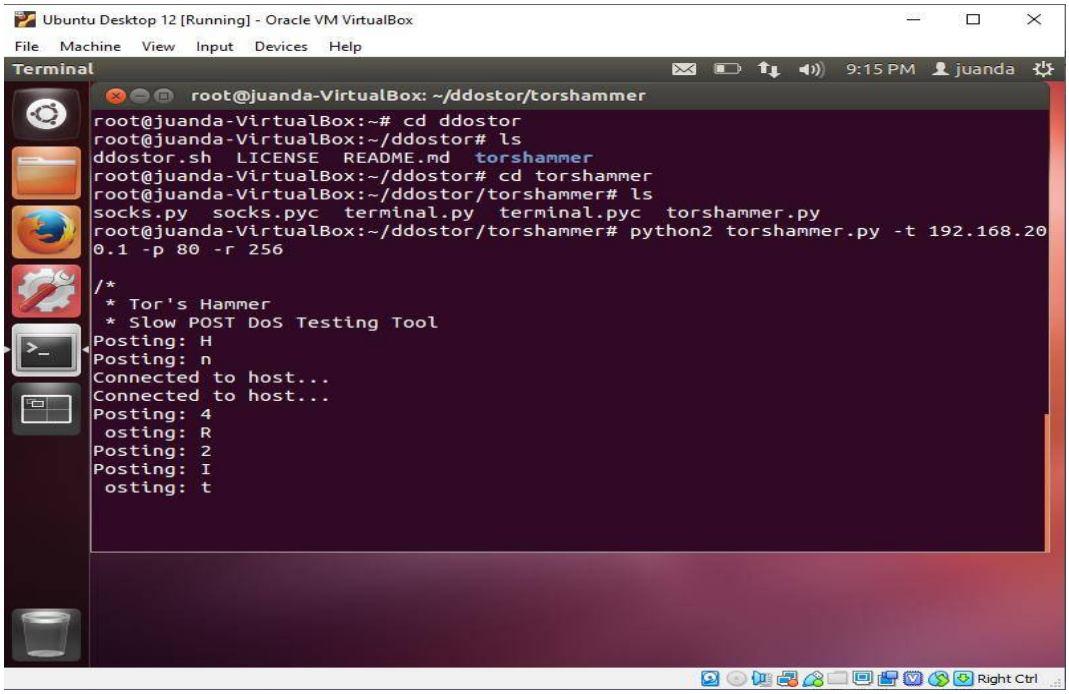


Gambar 4.44 Sistem Firewall Filter dengan DHCP Setup on

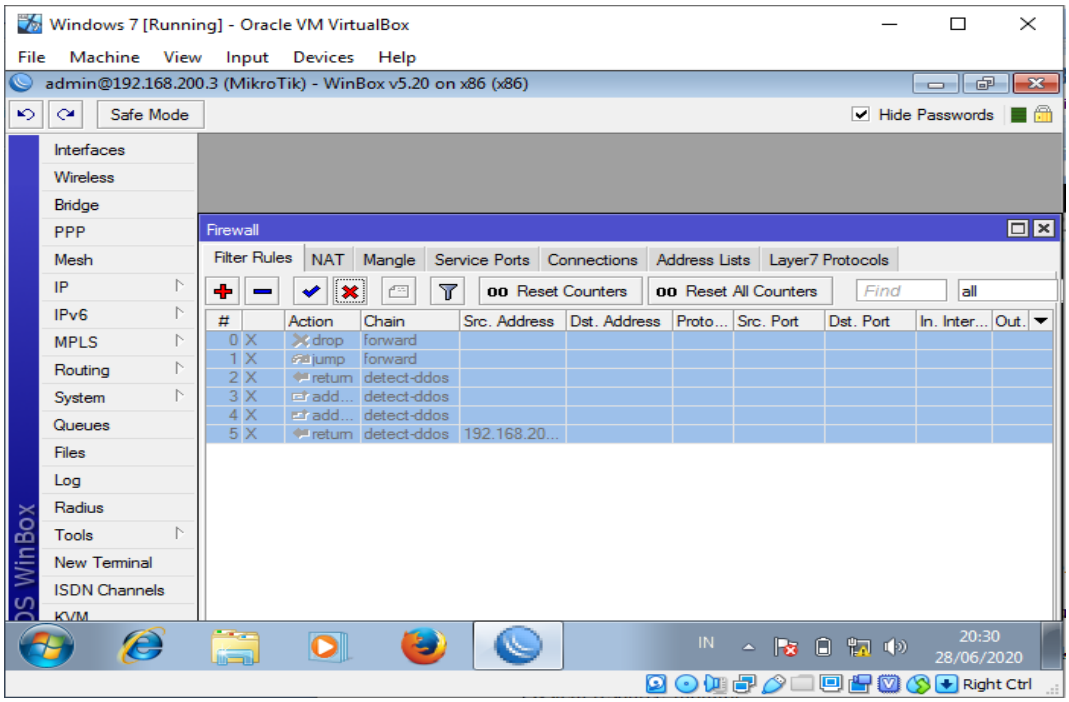
Pada gambar 4.44 ip firewall filter di setup DHCP-server dan ip yang dibuat obtain, lalu mengetikkan ether2 sampai on. Kemudian untuk melihat monitoring scara realtime saat tidak ada serangan sama sekali dengan perintah /system resource monitor.

Gambar 4.45 Tampilan sistem monitoring secara real time tidak ada serangan

Kemudian melakukan tahapan penyerangan ddos torshammer yang menargetkan ip domain yaitu 192.168.200.1 dengan menggunakan ubuntu desktop 12.04.

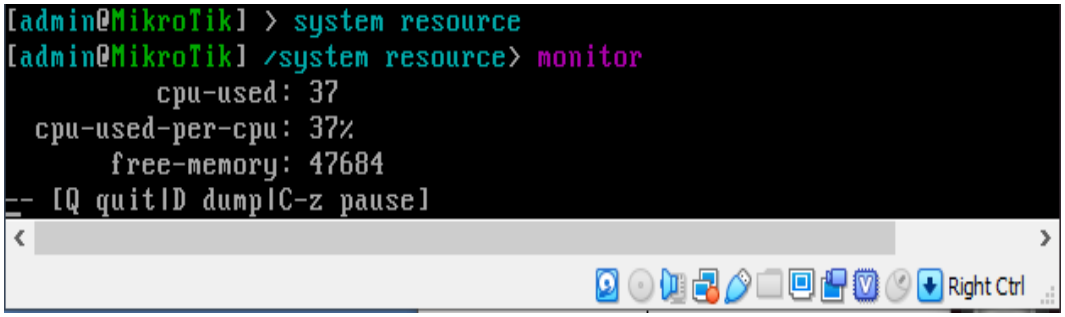


Gambar 4.46 Melakukan Serangan DDOS Torshammer



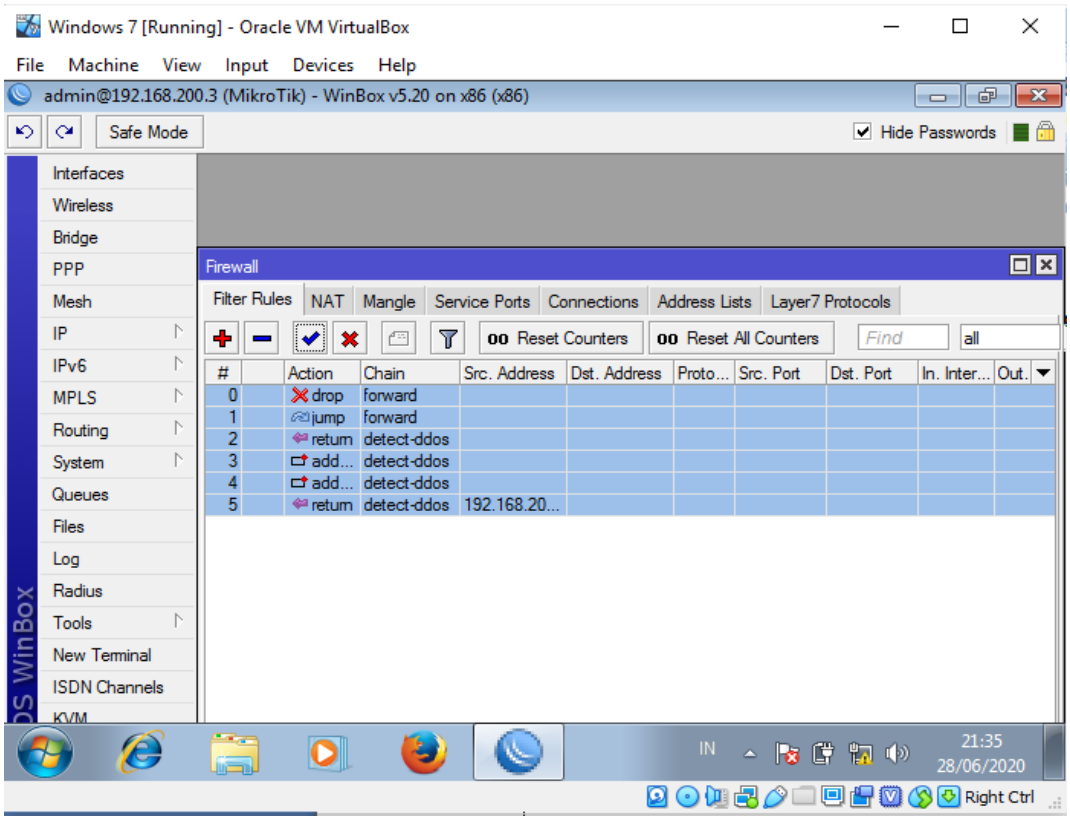
Gambar 4.47 Tampilan Rules Filter disable mikrotik os di winbox

Pada gambar 4.47 mikrotik OS login menggunakan winbox di client windows 7 pada virtualbox, dengan kondisi firewall saat disable.

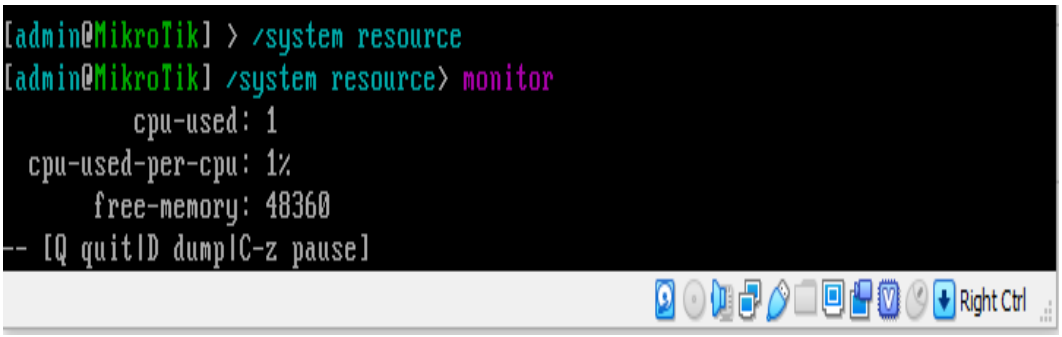


Gambar 4.48 Tampilan Hasil Monitoring Secara Realtime sebelum ada firewall

Pada gambar 4.48 hasil monitoring secara realtime dengan kondisi berpengaruh naik turun nya kinerja serangan DDOS sebelum adanya firewall.



Gambar 4.49 Tampilan Rules Filter enable mikrotik OS di Winbox



Gambar 4.50 Hasil adanya penurunan paket serangan DDOS melemah dan kondisi menjadi normal

Pada gambar 4.50 yang menampilkan bahwa pada system resource monitor mikrotik OS adanya paket serangan DDOS melemah saat firewall diaktifkan pada gambar 4.49.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pada bab-bab pembahasan sebelumnya dari proses konfigurasi dan analisis, dapat diambil beberapa kesimpulan yaitu:

1. Sistem *snort Intrusion Detection System* (IDS) dapat memberikan peringatan keamanan, sehingga dapat meningkatkan keamanan jaringan. Dapat atau tidaknya sebuah serangan terdeteksi oleh *snort* IDS tergantung dari ada tidaknya *rule* dengan jenis *signature* pada sebuah pola serangan.
2. Sistem *snort Intrusion Detection System* (IDS) bekerja dengan menggunakan *snort engine* yang memonitor paket data dan mencocokkannya pada *rules* yang telah ada. Bila paket data teridentifikasi dengan serangan, *rules* akan meneruskan serangan ke *Iptables* untuk dipisahkan dan di *block.*
3. Pada sistem keamanan snort dan *router firewall* dalam sistem yang telah diuji, *router firewall* akan melakukan pemblokiran sebuah paket-paket serangan yang telah teridentifikasi oleh snort yang berada pada tempat penyimpanan hasil identifikasi serangan di dalam *log snort* yang berisikan sebuah data-data serangan yang tersimpan, yang dilakukan oleh *attacker*.

4. Di mikrotik os dengan *rule* firewall filter yang telah dibuat ketika terdapat paket new DDOS yang tidak wajar akan dilakukan *grouping* menggunakan *address list* dengan nama *ddosed* dan *ddoser*, setelah alamat IP penyerang dan alamat IP tujuan berhasil ditangkap menggunakan *address-list* maka alamat IP tersebut akan di *drop oleh firewall filter* yang telah dibuat.

5.2 Saran

Pada penelitian ini penulis menemukan saran-saran yang perlu untuk pengembangan selanjutnya adalah:

1. Didalam sebuah website harus menambahkan *outsourcing* tambahan serta sistem yang up to date.
2. Didalam penelitian ini dapat dikembangkan dengan menggunakan algoritma lain untuk mencegah serangan DDOS.

DAFTAR PUSTAKA

ANALISIS_DAN_DESAIN_SISTEM_INFORMASI_BER. *Implementation Science*, *39*(1), 1–24. https://doi.org/10.4324/9781315853178

Cindy Nataliana. (2019). *ACCESS CONTROL SECURITY* (hal. 3). https://sis.binus.ac.id/2019/02/18/access-control-security/

Digital, K. F., Studi, P., Teknik, M., Pascasarjana, P., Teknologi, F., & Indonesia, U. I. (2018). *Metode Live Forensik Analisis Serangan Dos*.

DimensiData. (2017). *Fungsi Server, Jenis Server dan Cara Kerja Server*. https://blog.dimensidata.com/fungsi-server-jenis-server-dan-cara-kerja-server/

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." Jurnal Aksara Komputer Terapan 1.2 (2012).

Erika, Winda. "ANALISIS PERBANDINGAN METODE TAM (Technology Acceptance Model) DAN UTAUT (Unified of Acceptance and Use of Technology) TERHADAP PERSEPSI PENGGUNA SISTEM INFORMASI DIGITAL LIBRARY (Studi Kasus: Universitas Pembangunan Panca Budi Medan)." Jurnal Mahajana Informasi 4.1 (2019): 78-83.

Fuad Jauhari. (2008). KEAMANAN JARINGAN KOMPUTER PADA SISTEM PEMERINTAHAN ELEKTRONIK. *Artificial, ICT Research Center UNAS*, *2*, 78–84.

Habib Ahmad Purba. (2010). *Jenis-Jenis Server dan Fungsinya*. https://habibahmadpurba.wordpress.com/2013/07/10/jenis-jenis-server-dan- fungsinya/

Hafni, Layla, and Rismawati Rismawati. "ANALISIS FAKTOR-FAKTOR INTERNAL YANG MEMPENGARUHI NILAI PERUSAHAAN PADA PERUSAHAAN MANUFAKTUR YANG TERDAFTAR DI BEI 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

Hamdi, Nurul. "Model Penyiraman Otomatis pada Tanaman Cabe Rawit Berbasis Programmable Logic Control." Jurnal Ilmiah Core IT: Community Research Information Technology 7.2 (2019).

Hamdi, Muhammad Nurul, Evi Nurjanah, and Latifah Safitri Handayani. "COMMUNITY DEVELOPMENT BASED ONIBNU KHALDUN THOUGHT, SEBUAH INTERPRETASI PROGRAM PEMBERDAYAAN UMKM DI BANK ZAKAT EL-ZAWA." EL MUHASABA: Jurnal Akuntansi (e-journal) 5.2 (2014): 158-180.

Hasibuan, Alfiansyah. "Analisis Penggunaan Metode Algoritma Kohonen pada Jaringan Syaraf Tiruan Learning Vector Quantization (LVQ) pada Pengenalan Pola." (2019).

Hendrawan, J., & Perwitasari, I. D. (2019). Aplikasi Pengenalan Pahlawan Nasional dan Pahlawan Revolusi Berbasis Android. JurTI (Jurnal Teknologi Informasi), 3(1), 34-40.

Hermawan, R. (2013). Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos). *Analisis Konsep Dan Cara Kerja Serangan Komputer Distributed Denial of Service (Ddos)*, *5*(1), 1–14.

Indrat Susilo dan Gesang Kristiyanto Nugraha. (2012). Pembangunan Web Server Mengunakan Debian Server Untuk Media Pembelajaran Di Sekolah Menengah Kejuruan (Smk) Negeri 1 Sragen. *Indonesian Jurnal on Networking and Security (IJNS)*, *2*(1), 22–27.

Mahardani, A. A., & Asmunin. (2017). Implementasi Openvpn Menggunakan Ldap Sebagai Manajemen User. *Jurnal Manajemen Informatika*, *7*(1), 29–35. Muhammad Suyuti Ma'sum. (2017). No Title. *jurnal sistem dan teknologi informasi*, *5*, 56–60.

Muttaqin, Muhammad. "ANALISA PEMANFAATAN SISTEM INFORMASI E-OFFICE PADA UNIVERSITAS PEMBANGUNAN PANCA BUDI MEDAN DENGAN MENGGUNAKAN METODE UTAUT." Jurnal Teknik dan Informatika 5.1 (2018): 40-43.

Nurrofiq, M. (2012). *Pengertian Router Firewall dalam Jaringan*. https://www.diwarta.com/2012/06/13/pengertian-router-firewall-dalam-jaringan.html

Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 8-18.

Pratama, I. P. A. E., & Dharmesta, P. A. (2018). Implementasi Teknik Deep Packet Inspection Dengan Menggunakan Wireshark Pada Sistem Operasi Ubuntu. *Jurnal RESISTOR (Rekayasa Sistem Komputer)*, *1*(2), 79–85. https://doi.org/10.31598/jurnalresistor.v1i2.274

Priyono, D. T., Purnama, B. E., & Sukadi. (2013). Pembangunan Server Proxy Squid Menggunakan Ubuntu Server 11.10 Pada Sekolah Tinggi Keguruan Ilmu Pendidikan PGRI Pacitan. *Indonesian Journal on Networking and Security*, 1–11.

Ramadhan Triyanto Prabowo. (2015). *Network Development Life Cycle*. *2*.

Ramadhani, S., Suherman, S., Melvasari, M., & Herdianto, H. (2018). Perancangan Teks Berjalan Online Sebagai Media Informasi Nelayan. Jurnal Ilmiah Core IT: Community Research Information Technology, 6(2).

Rizal, Chairul. "SISTEM PENDUKUNG KEPUTUSAN PENENTUAN GURU DAN PEGAWAI TERBAIK MENGGUNAKAN METODE SAW (SIMPLE ADDITIVE WEIGHTING) STUDI KASUS SMAS ISLAM ALULUM TERPADU MEDAN." Jurnal Teknik dan Informatika 6.2 (2019): 14-17.

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

S, D. G., Faiqurahman, M., & Sari, Z. (2016). *PENERAPAN HYBRID HONEYPOT DAN PHAD UNTUK*. 116–125.

Saputra, Muhammad Juanda, and Nurul Hamdi. "RANCANG BANGUN APLIKASI SEJARAH KEBUDAYAAN ACEH BERBASIS ANDROID STUDI KASUS DINAS KEBUDAYAAN DAN PARIWISATA ACEH." JOURNAL OF INFORMATICS AND COMPUTER SCIENCE 5.2 (2019): 147-157.

SISTEM OPERASI ubuntu. (2017). http://adryanmuh18.blogspot.com/2017/05/sistem-operasi-jaringan-ubuntu.html

Sitanggang, R. (2019). SISTEM INFORMASI LAPORAN PENJUALAN KOMPUTER BERBASIS LAN, JURNAL MAHAJANA INFORMASI, VOL. 4 NO.1 TAHUN 2019, e-ISSN: 2527-8290, 62-77. *Jurnal Mahanana Informasi*, *4*(1), 62–77.

Sudradjat, B. (2017). *ISSN : 2598-8700 (Printed) ISSN : 2598-8719 (Online) PADA JARINGAN KOMPUTER DENGAN MENGUNAKAN ISSN : 2598-8719 (Online) Volume 1 Nomor 1 November 2017*. *1*(November), 10–24. Sutarti, Pancaro, Adi, P., & Saputra, Fembi, I. (2018). Implementasi IDS (Intrusion Detection System) Pada Sistem Keamanan Jaringan SMAN 1 Cikeusal. *Jurnal PROSISKO*, *5*(1). http://e-jurnal.lppmunsera.org/index.php/PROSISKO/article/download/584/592

Syahputra, Rizki, and Hafni Hafni. "ANALISIS KINERJA JARINGAN SWITCHING CLOS TANPA BUFFER." JOURNAL OF SCIENCE AND SOCIAL RESEARCH 1.2 (2018): 109-115.

Wikipedia. (n.d.). *Serangan Dos*. www

Zen, Muhammad. "PERBANDINGAN METODE DIMENSI FRAKTAL DAN JARINGAN SYARAF TIRUAN BACKPROPAGATION DALAM SISTEM IDENTIFIKASI SIDIK JARI PADA CITRA DIGITAL." JITEKH 7.2 (2019): 42-50.