HALAMAN PENGESAHAN

HALAMAN PERSEMBAHAN

Untuk Ibu, Bapak,
dan Adik-adikku tercinta.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji syukur penulis panjatkan ke hadirat Allah SWT karena hanya dengan rahmat dan hidayah-Nya, Tugas Akhir ini dapat terselesaikan tanpa halangan berarti. Keberhasilan dalam menyusun laporan Tugas Akhir ini tidak lepas dari bantuan berbagai pihak yang mana dengan tulus dan ikhlas memberikan masukan guna sempurnanya Tugas Akhir ini. Oleh karena itu dalam kesempatan ini, dengan kerendahan hati penulis mengucapkan terima kasih kepada:

1. Bapak Surya Michrandi Nasution, S.T., M.T Selaku Dosen Pembimbing pertama saya, dan sebagai KK Seculab
2. Bapak Fairuz Azmi, S.T., M.T Selaku Dosen Pembimbing kedua saya
3. Bapak Ir. Burhanuddin Dirgantoro ,M.T Selaku Dosen Wali saya
4. Temen-temen kelas SK-37-04 yang selalu membuat saya tertawa dengan humornya
5. Dan Teman-teman yang masih banyak yang tidak mungkin saya sebutkan

Penulis menyadari bahwa penyusunan Tugas Akhir ini jauh dari sempurna.Akhir kata penulis mohon maaf yang sebesar-besarnya apabila ada kekeliruan di dalam penulisan Tugas Akhir ini.

Wassalamu'alaikum Wr. Wb.

Bandung, 28 Juni 2017

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

Abstrak

Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah hacking dan cracking yang bersifat free dan ada pula yang dikomersilkan. Kemudian dari sisi software pendukung pun sudah banyak tool-tool yang bersifat free yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan attacker.

Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan.

Pada permasalahan tersebut, pada penelitian ini akan dibuat sebuah aplikasi yang dapat membantu network administrator dalam memonitoring server, aplikasi ini bertujuan untuk mempermudah network administrator dalam mengamankan server dari berbagai macam jenis serangan (ddos, scaning , brute force)

Kata kunci : *TelegramBot, attacker , server, ddos , scanning , brute force*

Abstract

In today's rapidly growing technological developments, the need for network security certainly increases with the development of knowledge about hacking and cracking problems that are free and some are commercialized. Then from the side of the software support is already a lot of tool tools that are free of which ability can be said to be used as a means of attack by attackers.

On the other hand there is a serious problem that is the security factor, but on the one hand humans are very dependent with the information system. This is what causes the statistics of network security incidents continue to increase sharply from year to year. This is due to the people's awareness which is very less towards Network security system.

In this research, we will create an application that can help network administrator in monitoring server, this application is aimed to facilitate network administrator in securing server from various kinds of attack (ddos, scaning, brute force)

Keywords : *wireless sensor network, Internet Protokol, WiFi, interoperability*.

BAB I

LATAR BELAKANG

1.1 Latar Belakang Masalah

Dalam perkembangan teknologi yang semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat *free* dan ada pula yang dikomersilkan. Kemudian dari sisi *software* pendukung pun sudah banyak *tools* yang bersifat *free* yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan *attacker*.

Pada sisi lain timbul masalah serius yaitu faktor keamanannya, namun disatu sisi manusia sudah sangat tergantung dengan sistem informasi. Hal itu yang menyebabkan statistik insiden keamanan jaringan terus meningkat tajam dari tahun ke tahun. Ini disebabkan karena kepedulian masyarakat yang sangat kurang terhadap sistem keamanan jaringan

Keamanan jaringan lokal ini bergantung sepenuhnya terhadap bagaimana seorang *network administrator* merespon dengan cepat sebuah serangan yang terjadi. Tapi *network administrator* hanyalah seorang manusia yang terbatas akan waktu. Seorang *network administrator* tidak dapat mengawasi seluruh jaringan secara terusmenerus. Maka dari itu dibutuhkan sebuah sistem yang dapat membantu *network administrator* untuk digunakan sebagai mengetasi segala macam serangan. Pada permasalahan tersebut, pada penelitian ini akan dibuat sebuah aplikasi yang dapat membantu *network administrator* dalam *memonitoring server*, aplikasi ini bertujuan untuk mempermudah *network administrator* dalam mengamankan *server* dari berbagai macam jenis serangan *(ddos, scaning , brute force)*.

Selain itu aplikasi ini terhubung dengan fitur bot yang dimiliki oleh aplikasi *chat* telegram, yang berfungsi sebagai *command and control* pada server. Setiap serangan yang terdeteksi akan dikirim melalui telegram, sehingga *network administrator* dapat mengetahui serangan apa saja yang terjadi pada *server* ditambah dengan fitur bot dari telegram yang berfungsi sebagai *command and control* yang digunakan untuk memerintah *server* untuk melakukan pencegahan / *bloking*.

1.2 Rumusan Masalah

Dalam perkembangan teknologi sekarang yang sudah semakin pesat, kebutuhan akan keamanan jaringan tentunya meningkat seiring dengan berkembangnya ilmu pengetahuan tentang masalah *hacking* dan *cracking* yang bersifat free dan ada pula yang dikomersilkan. Kemudian dari sisi software pendukung pun sudah banyak tool-tool yang bersifat free yang kemampuannya sudah bisa dikatakan mumpuni untuk digunakan sebagai alat penyerangan oleh kalangan attacker. Serangan-serangan tersebut dapat melumpuhkan server. Sehingga dapat menimbulkan kerugian.

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Membutuhkan kapasitas memori yang cukup besar.
2. Berjalan sistem operasi linux .
3. Hanya bisa melakukan monitoring pada satu *interface network* saja..
4. Hanya mendeteksi serangan (DDoS, Scanning, Brute Force)

1.4 Hipotesis

Dengan menggunakan rule deteksi yang didapatkan dengan pengolahan datasheet akan ditemukan fitur serangan yang mempunyai ciri-ciri masing-masing dalam jenis serangan, hal ini akan mempermudah dalam melakukan deteksi serangan tersebut, dikarenakan semua jenis serangan akan dibedakan dari masing masing fitur serangan yang telah ditentukan. Dalam mendeteksi serangan diharapkan sekurang-kurangnya 70%

1.5 Tujuan Penelitian

Tujuan dari penelitian tugas akhir ini adalah membuat sebuah aplikasi yang digunakan untuk membantu *sysadmin* dalam memonitoring serangan-serangan yang terjadi pada *server*, baik dalam proses pencegahan dan pendektesian terhadap serangan yang mempu membahayakan *server*.

1.6 Metode Penyelesain Masalah

Metode penelitian yang digunakan:

1. STUDI LITERATUR.
   Melakukan pencarian refrensi mengenai telegram bot dan pengolahan data trafik jaringan berdasarkan serangan yang diperlukan.

2. PENGUMPULAN DATA.
   Pada tahap ini, dilakukan pengumpulan data training yang akan diolah menggunakan algoritma Decision Tree. Data training dikumpulkan menggunakan scapy. Data Training pada serangan DDoS, Brute Force dan Scanning masing-masing berjumlah 5 juta data.

3. PERANCANGAN KEBUTUHAN SISTEM.
   Melakukan perancangan sistem deteksi untuk mendeteksi serangan DDoS, Brute Force dan Scanning serta dapat di integrasikan terhadap library scapy

4. PENGUJIAN SISTEM.
   Pada tahap ini sistem yang telah dibangun akan diuji berdasarkan hasil analisa dari algoritma decision tree yang menghasilkan fitur dan rules serangan..Hasil dari pengujian tersebut, diantaranya adalah kemampuan sistem untuk menghasilkan tree berdasarkan jumlah data training yang ditentukan dan kemampuan sistem untuk mendeteksi serangan berdasarkan fitur dan rules serangan yang di inputkan kedalam sistem deteksi.

5. ANALISA HASIL PENGUJIAN.
   Pada tahap analisis hasil pengujian, dilakukan perbandingan trafik serangan terhadap jumlah keseluruhan trafik. Hasil dari analisis tersebut, diantaranya adalah akurasi untuk mendeteksi serangan.

6. PENYUSUNAN LAPORAN TUGAS AKHIR.
   Pada tahap ini semua data dan hasil dari penelitian akan dibuat menjadi sebuah laporan dengan sistematika penulisan yang sesuai dengan ketentuan institusi.

1.7 Sistematika Penulisan

BAB I : PENDAHULUAN

Pada bab ini dijelaskan latar belakang, rumusan masalah, batasan, tujuan, manfaat, keaslian penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA DAN LANDASAN TEORI

Pada bab ini dijelaskan teori-teori dan penelitian terdahulu yang digunakan sebagai acuan dan dasar dalam penelitian.

BAB III : METODOLOGI PENELITIAN

Pada bab ini dijelaskan metode yang digunakan dalam penelitian meliputi langkah kerja, pertanyaan penilitian, alat dan bahan, serta tahapan dan alur penelitian.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini dijelaskan hasil penelitian dan pembahasannya.

BAB V : KESIMPULAN DAN SARAN

Pada bab ini ditulis kesimpulan akhir dari penelitian dan saran untuk pengembangan penelitian selanjutnya.

BAB II

TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Telegram Bot

Telegram adalah aplikasi pesan chatting yang memungkinkan pengguna untuk mengirimkan pesan chatting rahasia yang dienkripsi end-to-end sebagai keamanan tambahan. Selain itu telegram dilengkapi dengan fitur bot yang bersifat open source yang dimana fitur ini sangat cocok digunakan dalam penelitian ini. pada penelitian ini penulis menggunakan aplikasi telegram dikarenakan fitur bot telegram bisa digunakan sebagai *Command and Control (CNC)* pada *server* , baik *memonitoring server* , monitoring serangan. Namun pada penelitian ini bot difungsikan sebagai Command and Control pada server yaitu jika terjadi serangan apakah alamat ipaddres yang terdeteksi akan di blok atau tidak. Sehingga sysadmin tidak perlu melakukan remote server untuk itu[2].

2.2 *Intrusion Detection System (IDS)*

Menurut Chris Brenton (2003:289), Intrusion Detection System (IDS) adalah sistem pendeteksian penyusupan yang dapat melakukan scanning log-log access dan menganalisis karakteristik-karakteristik dari file-file untuk mengetahui apakah file tersebut telah diserang. Intrusion Detection System mampu mendeteksi aktivitas yang mencurigakan dalam sebuah sistem atau jaringan.[1]

2.2.1 *Network Intrusion Detection System (*NIDS*)*

Network Intrusion Detection System adalah sistem pendeteksian penyusupan *network*. *network Intrusion Detection System* memiliki fungsi untuk menganalisis paket di sebuah *network* dan mencoba untuk menentukan apakah seorang cracker sedang mencoba untuk masuk ke dalam sebuah sistem atau menyebabkan sebuah serangan Denial of Service (DOS)[2].

2.2.2 *Host Intrusion Detection System (*HIDS*)*

Host Intrusion Detection System adalah sistem pendeteksian penyusupan host. Sama seperti *NIDS*, sebuah *HIDS* menganalisis lalu lintas *network* yang dikirimkan menuju dan dari sebuah mesin tunggal. Sebagian besar dari *NIDS* komersial saat ini biasanya memiliki suatu unsur *HIDS*, dan sistem-sistem ini disebut hybrid IDS[2].

2.2.3 *System Integrity Verifier (SIV)*

System Integrity Verifier adalah alat untuk verifikasi integritas sistem. Melacak file-file sistem yang kritikal dan memberitahukan kepada administrator pada saat file-file tersebut diubah (biasanya oleh seorang cracker yang mencoba untuk mengganti file yang valid dengan sebuah Trojan Horse). Contoh dari SIV adalah Tripwire[3].

2.2.4 *Log File Monitor (LFM)*

Log File Monitor adalah alat yang digunakan untuk membaca log-log yang dihasilkan oleh servis- servis *network* yang mencari pola-pola serangan. Contoh dari LFM adalah Swatch[3].

2.3 *Distributed Denial of Service (DDoS)*

Rui Zhong et al.[4] *Distributed Denial of Service (DDoS)* adalah jenis serangan yang dilakukan secara masif dengan tujuan mengganggu hak akses pengguna jaringan. DDoS merupakan serangan flooding trafik yang dilakukan dengan sengaja untuk mengganggu QoS dari sistem jaringan yang bertujuan untuk membuat sumber daya server habis. Serangan DDoS pada dasarnya sama dengan serangan DoS namun serangan dilakukan dengan banyak sumber secara serentak. Untuk melancarkan serangan DDoS, penyerang biasanya mengumpulkan pasukan dengan cara mengambil alih komputer-komputer yang kemudian dijadikan zombie yang merupakan komputer yang siap diperintah dan dikendalikan oleh botnet[2].

2.4 *Brute Force Attack*

Brute Force attack adalah serangan pada protokol jaringan yang bertujuan untuk mendapat hak akses penuh dengan cara melakukan kegiatan penebakan username dan password login dari sebuah service dengan menggunakan kombinasi username dan password yang berbeda[4]

2.5 *Scanning*

Scanning Attack adalah serangan yang bertujuan pada jaringan yang bertujuan untuk menemukan port ataupun service yang terdapat pada sebuah host yang sedang tersambung kedalam jaringan[5].Berikut akan dijelaskan macam-macam serangan scanning:

2.5.1 *Host Discovery*

Serangan *Host Discovery* adalah jenis serangan scaning yang digunakan untuk mengetahui junmlah host yang sedang aktip pada suatu jaringan[5]. Jenis serangan ini mengirimkan packet icmp kesetiap alamat subnet pada sebauh jaringan.

2.5.2 *Port Detections*

Jenis serangan scanning ini bertujuan untuk mengetahui port-port yang sedang terbuka pada sebuah host yang telah ditentukan. Untuk menemukan port yang terbuka serangan ini melakukan pengiriman paket tcp terhadap host yang sedanga aktip dengan menargetkan port 1-65536.

2.5.3 *Service Scanning*

Jenis serangan scanning ini adalah serangan yang akan mengetahui macam macam service yang berjalan pada sebuah host yang menjalankan port tertentu.Serangan ini melakukan scanning pada masing-masing port yang sedang berjalan dan akan melakukan penyamaan signature pada software yang menjalankan port tersebut[5].

2.5.4 *Host Detection*

Serangan scanning ini bertujuan untuk mengetahui jenis sistem operasi yang dijalankan. Serangan ini menargetkan port 443 (netbios) yang mempunyai signature (ciri-ciri) tiap masing-masing host[6].

2.5.5 *Scapy*

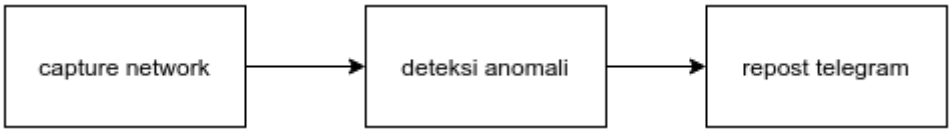
Scapy adalah suatu library yang dibangun menggunakan bahasa pemrograman python dan sangat powerfull untuk memanipulasi paket yang ada pada jaringan. Scapy mampu membuat dan memecah paket-paket dari berbagai jenis protocol yang ada, mentransimikannya, menangkapnya, menerima permintaan dan menjawabnya, dan banyak lagi. Scapy dapat digunakan untuk menangani macam-macam kegiatan yang berhubungan dengan *network*ing, seperti kegiatan "scanning","tracerouting", "attack" atau "*network* discovery". Scapy juga dapat mengajarkan kita tentang semua proses-proses dari suatu protocol.

BAB III

METODOLOGI PENELITIAN

3.1 Gambaran Umum

Pada perancangan sistem menjelaskan mengenai alur dari proses yang dikerjakan pada tugas akhir ini. Penjelasan yang ada meliputi alur deteksi *anomali* dan hal-hal yang terkait untuk sistem deteksi *anomali*. Pada penelitian tugas akhir mengikuti alur sistem seperti gambar berikut:



Gambar 3.1 Gambaran Umum Sistem

3.1.1 *(Capture Network)*

Pada proses ini akan dilaukan monitoring *traffik* menggunakan *scappy* , setiap semua *traffik* yang berjalan pada *network* akan disamanakan dengan *rule* deteksi yang sudah disediakan selama proses ini tidak akan dilakukan perintah apapun pada sisi *server*.

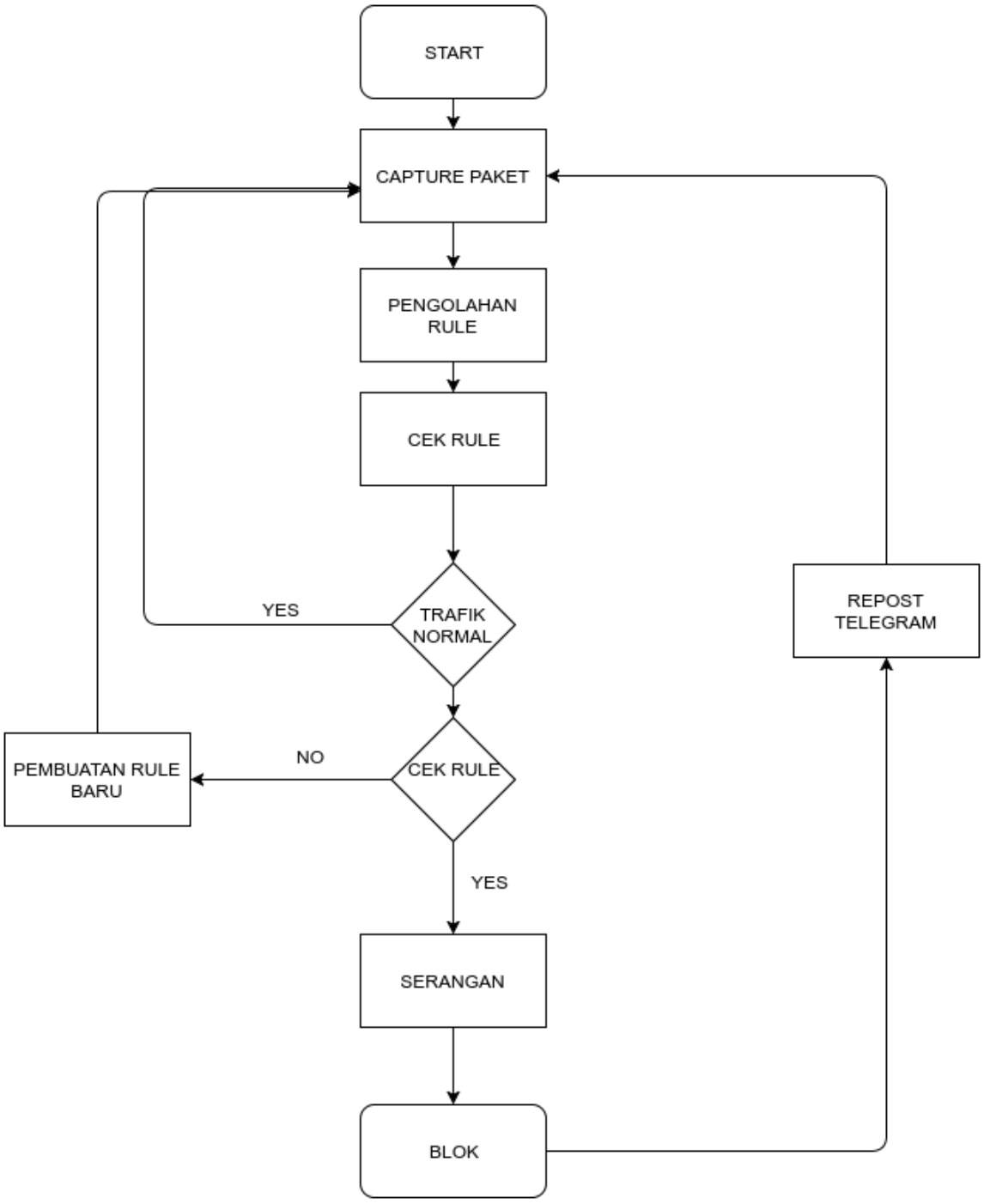
3.1.2 Deteksi *Anomali*

Pada proses ini dilakukan pemindaian pada *traffik* dan *rule* deteksi yang digunakan, ketika *traffik* tersebut sama dengan *rule* serangan , maka akan terdeteksi sebagai anomali / serangan. Pada proses ini akan mengu perintah untuk melakukan bloking dari telegram.

3.1.3 Repost Telegram

Proses ini akan mengirim repost berupa pesan ,ketika terjadi anomali/serangan pada *network* dan akan menunggu printah dari user untuk melakukan bloking dan sebagainya.

3.2 Gambaran Khusus



Gambar 3.2 Gambaran Khusus Sistem

3.2.1 *Capture Packet*

Pada proses ini akan dilaukan monitoring *traffik* menggunakan *scappy* , setiap semua *traffik* yang berjalan pada *network* akan disamanakan dengan *rule* deteksi yang sudah disediakan selama proses ini tidak akan dilakukan perintah apapun pada sisi *server*.

3.2.2 Pengolahan *Rule*

Proses ini akan melakukan pengolahan *rule* yang digunakan untuk mendetesi serangan , setiap *rule* yang terbentuk akan disimpan dalam sebuah file yang akan digunakan untuk deteksi anomali

3.2.3 Pemindain *Rule*

Pada proses ini dilakukan pemindaian pada *traffik* dan *rule* deteksi yang digunakan, ketika *traffik* tersebut sama dengan *rule* serangan , maka akan terdeteksi sebagai anomali / serangan. Pada proses ini akan mengu perintah untuk melakukan bloking dari telegram.

3.2.4 *Blocking*

Proses ini akan melakukan perintah dari user melalui telegram , pada proses ini blocking menggunakan tools iptables yang berfungsi sebagai tools untuk melakukan blok paket dan koneksi yang terhadi.

3.2.5 Repost Telegram

Proses ini akan mengirim repost berupa pesan ,ketika terjadi anomali/serangan pada *network* dan akan menunggu printah dari dari user untuk melakukan bloking dan sebagainya.

3.2.6 Pembuatan *Rule* Baru

Pada proses pembuatan *rule* baru ini akan dilakukan ketika ada anommali dalam *network* namum *traffik* tersebut tidak terdeteksi sebagai serangan, sehingga dibutuhkan *rule* baru untuk mendeteksi jenis *traffik* tersebut.

3.3 *Capture Packet*

Dalam Penelitian tugas akhir menggunakan fitur packet yang telah disesuaikan dengan fitur pengoalahan *rule* sebelumnya, yaitu dengan menggunakan dataset hasil pengolahan dari capture scapy.

3.4 Pengolahan *Traffik*

Pada pengoalahan trafik dilakukan proses pencocokan dengan hasil pengolahan dataset serangan yang telah didapatkan.

Tabel 3.1 Jumlah dataset

NO	*traffik*	JUMLAH DATASET
1	SCANNING	5.000.000
2	BRUTE FORCE	5.000.000
3	DDoS	5.000.000
4	NORMAL	5.000.000

3.5 Dataset

Pada penelitian tugas akhir ini diguanakan dataset scapy. Berikut adalah fitur dataset scapy antara lain:

A. *Transmission Control Protocol (TCP)*
B. *Internet Control Message Protocol (ICMP)*
C. *Internet Protocol Address (IP)*
D. *User Datagram Protocol (UDP)*

berikut adalah penjelasan dari masing masing dataset yang digunakan untuk pembuatan *rule* deteksi serangan .

3.5.1 *Transmission Control Protocol (TCP)*

Transmission Control Protocol (TCP) adalah suatu protokol yang berada di lapisan transport (baik itu dalam tujuh lapis model referensi OSI atau model DARPA) yang berorientasi sambungan (connection-oriented) dan dapat diandalkan (reliable). TCP dispesifikasikan dalam RFC 793.Pada scapy terdapat 11 fitur sebagai berikut :

Tabel 3.2 Fitur ICMP

NO	FITUR	TIPE
1	SPORT	ShortEnumField
2	DPORT	ShortEnumField
3	SEQ	IntField
4	ACK	IntField
5	DATAOFS	BitField
6	RESERVED	BitField
7	FLAGS	FlagsField
8	WINDOW	ShortField
9	CHKSUM	XShortField
10	ARGPTR	ShortField
11	OPTIONS	TCPOptionsField

3.5.2 *Internet Control Message Protocol (ICMP)*

Internet Control Message Protocol (ICMP) adalah salah satu protokol inti dari keluarga protokol internet. ICMP utamanya digunakan oleh sistem operasi komputer jaringan untuk mengirim pesan kesalahan yang menyatakan, sebagai contoh, bahwa komputer tujuan tidak bisa dijangkau. ICMP berbeda tujuan dengan TCP dan UDP dalam hal ICMP tidak digunak- an secara langsung oleh aplikasi jaringan milik pengguna. salah satu pengecualian adalah aplikasi ping yang mengirim pesan ICMP Echo Request (dan menerima Echo Reply) untuk menentukan apakah komputer tujuan dapat dijangkau dan berapa lama paket yang dikirimkan dibalas oleh komputer tujuan. Berikut adalah fitur icmp yang terdapat pada scapy :

Tabel 3.3 Fitur ICMP

NO	FITUR	TIPE
1	TYPE	ByteEnumField
2	CODE	MultiEnumField
3	CHKSUM	XShortField
4	ID	ConditionalField
5	SEQ	ConditionalField
6	TSORI	ConditionalField
7	TSRX	ConditionalField
8	TSTX	ConditionalField
9	GW	ConditionalField
10	PTR	ConditionalField
11	RESERVED	ConditionalField
12	ADDRMASK	ConditionalField
13	UNUSED	ConditionalField

3.5.3 *Internet Protocol Address (IP)*

Internet Protocol Address (IP) adalah protokol lapisan jaringan (network layer dalam OSI Reference Model) atau protokol lapisan internetwork (internetwork layer dalam DARPA Reference Model) yang digunakan oleh protokol TCP/IP untuk melakukan pengalamatan dan routing paket data antar host-host di jaringan komputer berbasis TCP/IP. Versi IP yang banyak digunakan adalah IP versi 4 (IPv4) yang didefinisikan pada RFC 791 dan dipublikasikan pada tahun 1981, tetapi akan digantikan oleh IP versi 6 pada beberapa waktu yang akan datang.Berikut adalah fitur yang terdapat pada IP :

Tabel 3.4 Fitur IP

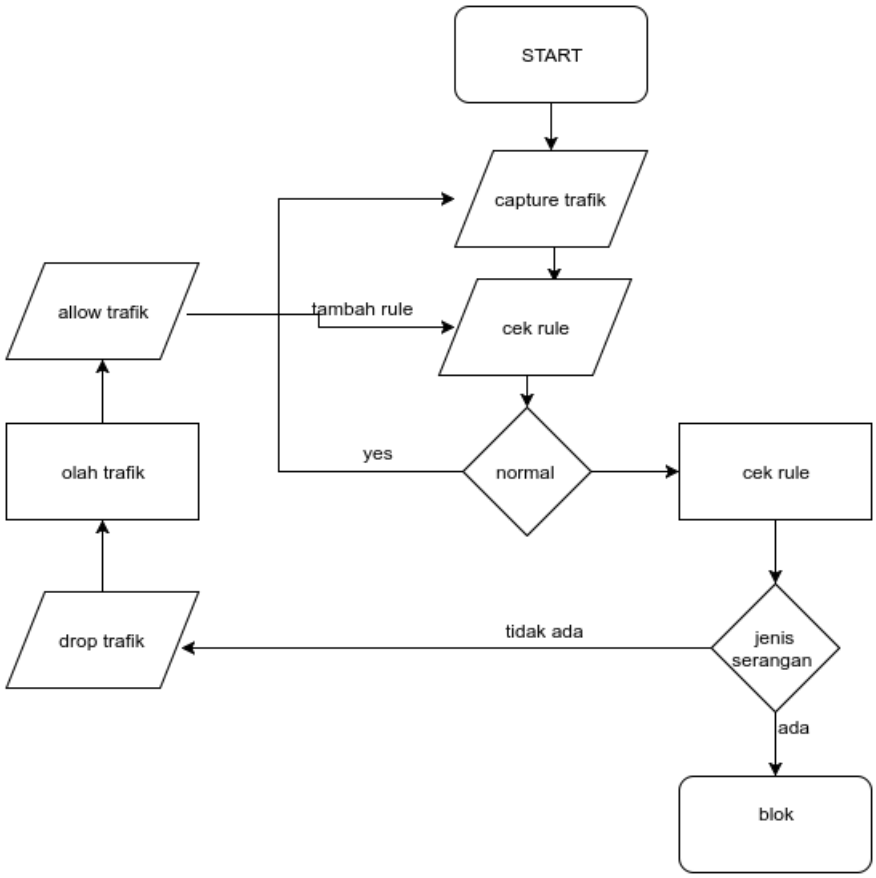
NO	FITUR	TIPE
1	VERSION	BitField
2	IHL	BitField
3	TOS	XByteField
4	LEN	ShortField
5	ID	ShortField
6	FLAGS	FlagsField
7	FRAGS	BitField
8	TTL	ByteField
9	CHKSUM	XShortField
10	SRC	Emph
11	DST	Emph
12	OPTIONS	PacketListField

3.5.4 *User Datagram Protocol (UDP)*

User Datagram Protocol merupakan bagian dari internet protocol. Dengan UDP, aplikasi komputer dapat mengirimkan pesan kepada komputer lain dalam jaringan lain tanpa melakukan komunikasi awal.[7] UDP melakukan komunikasi secara sederhana dengan mekanisme yang sa- ngat minimal. Ada proses checksum untuk menjaga integritas data. UDP digunakan untuk komunikasi yang sederhana seperti *query DNS (Domain Name System), NTP (Network Time Protocol), DHCP (Dinamic Host Configuration Protocol), dan RIP (Routing Information Protocol).*

3.6 *Autonomous System*

Cara kerja *Autonomus System* ini adalah ketika *traffik* terindikasi bukan *traffik* normal, maka akan dilakukan pemindaian pada jenis serangan pada *rule* yang telah disediakan, namun tidak semua *rule* tersebut akan dianggap serangan. Pada kenyataannya *traffik* yang tidak terindikasi serangan ini merupakan serangan jenis lain yang dimana didalam *rule* tersebut *traffik* atau ciri ciri serangan ini belum ada. Oleh kerena itu pada penelitian tugas akhir ini dibuat Autonomus System yang dimana *traffik* serangan jenis baru secara langsung akan diolah menjadi *rule* baru. Sehingga secara terus menerus akan mampu mengenali serangan tipe baru. Berikut adalah *flowchart* Autonomus System :



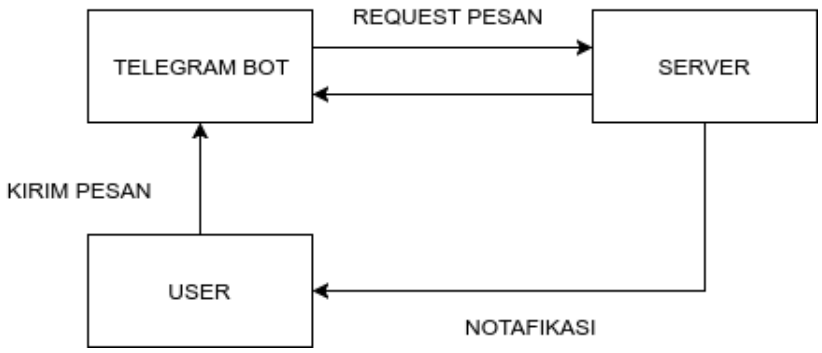
Gambar 3.3 Autonomous System

3.7 *Telegram Command and Control (CNC)*

Telegram bot berfungsi sebagai *Command and Control (CNC)* pada bagian ini aplikasi telegram berfungsi sebagai kimunikasi antara *server* dan client. Ketika *server* mendapat serangan , *server* akan melakukan authentikasi melalui telegram ,sehingga sysadmin bisa melakukan tindakan defensive terhadap serangan tersebut berikut adalah gambar *repost telegram*:

Gambar 3.4 Telegram Repost

Berikut adalah *flowchart* TelegramBot



Gambar 3.5 Telegram

Pada flowchrat diatas dapat deketahui *user* mengirim pesan ketelegram , kemuadi setiap pesan akan dianggap sebuah perintah ketika pesan yang dikirimkan dikenali olah *server* , setiap *server* menerima serangan , pesan akan dikirim melalu telegram chat oleh bot ke user.

3.8 *Attacking Tools*

Pada penelitian tugas akhir ini digunakan *tools* untuk melakukan *attacking* sebagai berikut :

3.8.1 NMAP

NMAP (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port *scanning*. Aplikasi ini digunakan untuk meng-audit jaringan yang ada. Dengan menggunakan *tools* ini, kita dapat melihat *host* yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan *feature-featur scanning* lainnya.

3.8.2 NESSUS

Nessus adalah scanner keamanan jaringan yang harus digunakan oleh administrator system . Nessus adalah software yang gratis dan bebas di download. Nessus merupakan sebuah software , yangdapat digunakan untuk meng-audit kemanan sebuah sistem, seperti vulnerability, misconfiguration,security patch yang belum diaplikasikan, default password, dan denial of service.

Nessus berfungsi untukmonitoring lalu-lintas jaringan.Dikarenakan fungsi dari Nessus dapat digunakan untuk mendeteksi adanya kelemahan ataupun cacatdari suatu sistem maka Nessus menjadi salah satu tool andalan ketika melakukan audit keamanan suatusistem.

3.8.3 METASPLOIT AUXILIARY

Metasploit Auxiliary adalah sebuah tools yang diguanakan untuk melakukan penetrasi keamanan jaringan dengan memamfaatkan celah keaman yang ada , *tools* ini suda dilengkapi dengan *auxiliary* yang berfungsi sebagai tools tambahan untuk melakuan pemindaian pada jaringan yang bertujuan untuk menemukan celah pada jaringan sebelum diexploitasi.

3.8.4 TCP Scanning

Tools ini digunakan untuk melakukan pemindain pada sebuah jaringan yang bertujuan untuk mengetahui *host* yang aktif dan tools ini juga bisa digunakan untuk melakukan pemindain *port* pada *host* yang aktip.

3.8.5 HYDRA dan Medusa

Hydra dan Medusa adalah sebuah tools yang didesain untuk melakukan *brute force* pada sebuah *service* yang membutuhkan *authentication* berupa inputan login untuk dapat melaukan akses.

3.8.6 Zero Brute

Zero brute adalah sebauah tools yang digunakan untuk melakukan serangan *brute force* yang bertujuan untuk mendapatkan hak akses secara penuh pada sebuah titik layanan.

3.8.7 Metasploit SynFlood

Metasploit Auxiliary adalah sebuah tools yang diguanakan untuk melakukan penetrasi keamanan jaringan dengan memamfaatkan celah keaman yang ada , *tools* ini suda dilengkapi dengan *auxiliary* yang berfungsi sebagai tools tambahan untuk melakuan pemindaian pada jaringan yang bertujuan untuk menemukan celah pada jaringan sebelum diexploitasi.

3.8.8 Slowloris

Slowloris adalah sebuah tools DDoS yang berfungsi sebagai alat untuk membanjiri lalu lintas jaringan sehingga bisa membuat layanan tidak bisa berfungsi dengan normal

3.8.9 HULK

Tools ini didesain untuk membanjiri layanan HTTP dan HTTPS yang berfungsu sebagai titik layanan pada sebuah *web server* , tool ini sering digunakan sebagai DDoS Bot

3.8.10 PyLoris

Tools ini hasil pengembangan dari *slowloris* , tools ini bersifat open-source sehingga kita bisa mengatur layanan yang akan diserangan , biasanya tools ini diguanakan untuk menyerang layanan UDP .

3.9 Alat dan Bahan

Alat dan bahan yang digunakan pada penelitian ini terbagi atas perangkat keras dan perangkat lunak yang akan dijelaskan seperti berikut.

3.9.1 Perangkat Keras

Adapaun perangakat keras yang kami gunakan pada peneletian kali ini adalah sebagai berikut

a. 1 buah server vps
b. 2 unit PC.
c. 1 buah switch koneksi local (LAN)
d. kabel LAN RJ45,
e. 1 buah handphone,

3.9.2 Perangkat Lunak

Adapaun perangakat keras yang kami gunakan pada peneletian kali ini adalah sebagai berikut :

a. python compiler.
b. module scapy.
c. wireshark.
d. mongodb.
e. telegram.
f. Linux Server.
g. driffnet.
h. etherape.
i. nmap
j. metasploit
k. nessus
l. tcp scanning .

BAB IV

HASIL DAN PEMBAHASAN

Pada penelitian tugas akhir ini, pengujian sistem deteksi *anomali traffik* dilakukan dengan mengukur detection rate, accuracy. Data yang digunakan dalam pengujian berjumlah 5 juta dataset normal ,5 juta dataset serangan DDos ,5 juta dataset serangan Brute Force ,5 juta dataset serangan Scanning. Pengujian pada peneltian ini akan menghitung akurasi deteksi setiap serangan , kecepatan waktu komukiasin antara server dan telegram, dan kapasitas memory yang digunakan oleh server dalam menjalankan aplikasi ini.

4.1 Kebutuhan Pengujian

Data yang digunakan pada pengujian merupakan sebagian data dari dataset hasil scapy preprocessing yang telah telah dijadikan sebuah *rule* dengan data sebanyak masing masing 5 juta dataset . Data yang digunakan untuk proses training decision tree menggunakan data dari hasil *capturing traffik* menggunakan scapy dengan komposisi data yaitu data normal dan data serangan yang telah dijadikan *rule* sebagai deteksi serangan. Pengujian ini menggunakan *tools-tools* yang sudah bersifat umum dalam melakukan serangan dianataranta adalah sebagai berikut

4.1.1 *Scanning Tools*

A. NMAP
B. NESSUS
C. Metasploit auxilary
D. TCP scanning tools,

4.1.2 *Brute Force Tools*

A. Hydra
B. Medusa.
C. Metasploit Auxiliary
D. Zero brute
E. Nmap Script Enggine

4.1.3 *DDoS Tools*

A. Metasploit SynFlood
B. Slowloris.
C. TCP flood
D. HULK (HTTP Unbearable Load King)
E. PyLoris

4.2 Pengujian Akurasi Masing-Masing Tools

Pada pengujian ini akan diuji akurasi deteksi serangan dari masing masing *tools* serangan yang digunakan dengan 10 kali percobaan terhadap 3 *rule* serangan , berikut adalah tabel pengujian serangan

4.2.1 NMAP

Hasil akurasi deteksi NMAP dari 10 kali percobaan

Tabel 4.1 Akurasi Deteksi Nmap

Nomer	Scanning	Brute Force	DDoS
1	93.00%	5.00%	0.00%
2	94.00%	6.00%	0.00%
3	94.00%	6.00%	0.00%
4	93.00%	5.00%	0.00%
5	94.00%	6.00%	0.00%
6	94.00%	6.00%	0.00%
7	92.00%	8.00%	0.00%
8	94.00%	6.00%	0.00%
9	94.00%	6.00%	0.00%
10	94.00%	6.00%	0.00%
rata-rata	93.60%	6.33%	0.00%

4.2.2 NESSUS

Hasil akurasi deteksi NESSUS dari 10 kali percobaan

Tabel 4.2 Akurasi Deteksi Nessus

Nomer	Scanning	Brute Force	DDoS
1	91.00%	6.00%	0.00%
2	92.00%	6.00%	0.00%
3	90.00%	8.00%	0.00%
4	88.00%	8.00%	0.00%
5	90.00%	6.00%	0.00%
6	94.00%	6.00%	0.00%
7	94.00%	6.00%	0.00%
8	95.00%	5.00%	0.00%
9	95.00%	5.00%	0.00%
10	96.00%	4.00%	0.00%
rata-rata	92.50%	6.00%	0.00%

4.2.3 Metasploit Auxiliary

Hasil akurasi deteksi *Metasploit Auxiliary* dari 10 kali percobaan

Tabel 4.3 Akurasi Deteksi Metasploit Auxiliary

Nomer	Scanning	Brute Force	DDoS
1	90.00%	8.00%	0.00%
2	91.00%	6.00%	0.00%
3	92.00%	6.00%	0.00%
4	90.00%	8.00%	0.00%
5	91.00%	6.00%	0.00%
6	94.00%	6.00%	0.00%
7	92.00%	8.00%	0.00%
8	94.00%	6.00%	0.00%
9	94.00%	6.00%	0.00%
10	98.00%	2.00%	0.00%
rata-rata	92.60%	6.20%	0.00%

4.2.4 TCP Scanning Tools

Hasil Akurasi Deteksi *TCP Scanning Tools* dari 10 kali percobaan

Tabel 4.4 Akurasi Deteksi TCP Scanning Tools

Nomer	Scanning	Brute Force	DDoS
1	98.00%	2.00%	0.00%
2	94.00%	6.00%	0.00%
3	92.00%	8.00%	0.00%
4	94.00%	6.00%	0.00%
5	94.00%	6.00%	0.00%
6	98.00%	2.00%	0.00%
7	94.00%	6.00%	0.00%
8	94.00%	6.00%	0.00%
9	95.00%	5.00%	0.00%
10	95.00%	5.00%	0.00%
rata-rata	94.80%	5.20%	0.00%

4.2.5 Hydra

Hasil akurasi deteksi hyrda dari 10 kali percobaan

Tabel 4.5 Akurasi Deteksi Hydra

Nomer	Scanning	Brute Force	DDoS
1	7.00%	87.00%	0.00%
2	6.00%	86.00%	0.00%
3	7.00%	87.00%	0.00%
4	7.00%	87.00%	0.00%
5	6.00%	86.00%	0.00%
6	6.00%	88.00%	0.00%
7	6.00%	87.00%	0.00%
8	7.00%	88.00%	0.00%
9	7.00%	87.00%	0.00%
10	6.00%	88.00%	0.00%
rata-rata	6.50%	87.10%	0.00%

4.2.6 Medusa

Hasil akurasi deteksi Medusa dari 10 kali percobaan

Tabel 4.6 Akurasi deteksi medusa

Nomer	Scanning	Brute Force	DDoS
1	6.00%	94.00%	0.00%
2	7.00%	93.00%	0.00%
3	6.00%	94.00%	0.00%
4	6.89%	93.11%	0.00%
5	7.00%	93.00%	0.00%
6	6.00%	94.00%	0.00%
7	6.00%	94.00%	0.00%
8	7.00%	93.00%	0.00%
9	6.00%	94.00%	0.00%
10	6.89%	93.11%	0.00%
rata-rata	6.48%	93.52%	0.00%

4.2.7 Metasploit Auxiliary

Hasil akurasi Metasploit Auxiliary dari 10 kali percobaan

Tabel 4.7 Akurasi Deteksi Metasploit Auxiliary

Nomer	Scanning	Brute Force	DDoS
1	6.00%	86.00%	0.00%
2	7.00%	87.00%	0.00%
3	7.00%	87.00%	0.00%
4	6.00%	86.00%	0.00%
5	6.00%	88.00%	0.00%
6	6.00%	87.00%	0.00%
7	7.00%	88.00%	0.00%
8	7.00%	87.00%	0.00%
9	7.00%	87.00%	0.00%
10	6.00%	86.00%	0.00%
rata-rata	6.50%	86.90%	0.00%

4.2.8 Zero Brute

Hasil akurasi deteksi Zero Brute dari 10 kali percobaan

Tabel 4.8 Akurasi deteksi Zero brute

Nomer	Scanning	Brute Force	DDoS
1	6.00%	87.00%	0.00%
2	7.00%	88.00%	0.00%
3	7.00%	87.00%	0.00%
4	7.00%	87.00%	0.00%
5	6.00%	86.00%	0.00%
6	6.00%	88.00%	0.00%
7	6.00%	87.00%	0.00%
8	7.00%	88.00%	0.00%
9	7.00%	87.00%	0.00%
10	7.00%	87.00%	0.00%
rata-rata	6.60%	87.20%	0.00%

4.2.9 Nmap Script Enggine

Hasil akurasi deteksi Nmap Script Enggine dari 10 kali percobaan

Tabel 4.9 Akurasi Nmap SCript Enggine

Nomer	Scanning	Brute Force	DDoS
1	7.00%	87.00%	0.00%
2	6.00%	86.00%	0.00%
3	6.00%	88.00%	0.00%
4	6.00%	87.00%	0.00%
5	7.00%	88.00%	0.00%
6	7.00%	93.00%	0.00%
7	6.00%	94.00%	0.00%
8	6.89%	93.11%	0.00%
9	7.00%	93.00%	0.00%
10	6.00%	94.00%	0.00%
rata-rata	6.49%	90.31%	0.00%

4.2.10 Metasploit SynFlood

Hasil akurasi deteksi Metasploit Synflood Enggine dari 10 kali percobaan

Tabel 4.10 Akurasi Metasploit SynFlood

Nomer	Scanning	Brute Force	DDoS
1	3.00%	0.00%	96.00%
2	2.00%	0.00%	98.00%
3	2.00%	0.00%	98.00%
4	2.00%	0.00%	98.00%
5	2.00%	0.00%	98.00%
6	2.00%	0.00%	98.00%
7	2.00%	0.00%	98.00%
8	3.00%	0.00%	97.00%
9	2.00%	0.00%	98.00%
10	2.00%	0.00%	98.00%
rata-rata	2.50%	0.00%	97.00%

4.2.11 Slowloris

Hasil akurasi deteksi slowloris dari 10 kali percobaan

Tabel 4.11 Akurasi Deteksi Slowloris

Nomer	Scanning	Brute Force	DDoS
1	3.00%	0.00%	96.00%
2	2.00%	0.00%	98.00%
3	2.00%	0.00%	98.00%
4	2.00%	0.00%	98.00%
5	2.00%	0.00%	98.00%
6	2.00%	0.00%	98.00%
7	2.00%	0.00%	98.00%
8	3.00%	0.00%	97.00%
9	2.00%	0.00%	98.00%
10	2.00%	0.00%	98.00%
rata-rata	2.50%	0.00%	97.00%

4.2.12 TCP Flood

Hasil akurasi deteksi TCP flood dari 10 kali percobaan

Tabel 4.12 Pengujian Akurasi TCP Flood

Nomer	Scanning	Brute Force	DDoS
1	2.00%	0.00%	98.00%
2	2.00%	0.00%	98.00%
3	2.00%	0.00%	98.00%
4	2.00%	0.00%	98.00%
5	3.00%	0.00%	97.00%
6	2.00%	0.00%	98.00%
7	2.00%	0.00%	98.00%
8	3.00%	0.00%	97.00%
9	2.00%	0.00%	96.00%
10	2.00%	0.00%	98.00%
rata-rata	2.00%	0.00%	98.00%

4.2.13 HULK

Hasil akurasi deteksi Hulk dari 10 kali percobaan

Tabel 4.13 Akurasi HULK

Nomer	Scanning	Brute Force	DDoS
1	3.00%	0.00%	96.00%
2	2.00%	0.00%	98.00%
3	2.00%	0.00%	98.00%
4	2.00%	0.00%	98.00%
5	2.00%	0.00%	98.00%
6	2.00%	0.00%	98.00%
7	2.00%	0.00%	98.00%
8	3.00%	0.00%	97.00%
9	2.00%	0.00%	98.00%
10	2.00%	0.00%	98.00%
rata-rata	2.50%	0.00%	97.00%

4.2.14 PyLoris

Hasil akurasi deteksi Pyloris dari 10 kali percobaan

Tabel 4.14 Akurasi Deteksi Pyloris

Nomer	Scanning	Brute Force	DDoS
1	2.00%	0.00%	98.00%
2	2.00%	0.00%	98.00%
3	2.00%	0.00%	98.00%
4	2.00%	0.00%	98.00%
5	3.00%	0.00%	97.00%
6	2.00%	0.00%	98.00%
7	2.00%	0.00%	98.00%
8	3.00%	0.00%	97.00%
9	2.00%	0.00%	96.00%
10	2.00%	0.00%	98.00%
rata-rata	2.00%	0.00%	98.00%

4.3 Pengujian Akurasi

Pada pengujian ini untuk mengukur akurasi serangan, pada pengujian ini dilakukan serangan menggunakan *tools-tools* yang sudah disediakan , setiap serangan pada pengujian ini dilakukan secara acak ,*tools* yang diguanakn adalah *tools* yang sudah umum diguankan dalam melakukan serangan . Pengujian ini dilakukan dengan beberapa skenario pengujian sebagai berikut :

4.3.1 Skenario Pertama

Pada skenario pertama akan diuji masing masing akurasi deteksi serangan tanpa memasukan *rule* traffik normal,pengujian ini dilakukan sealama 50 kali pengujian serangan dimana masing-masing serangan dilakukan secara satu persatu atau terpisah disamping itu dalam skenario ini dilakukan serangan secara acak dari masing masing *tools* dan pada penelitian tugas akhir ini dilakukan monitoring deteksi serangan, berikut kami sajikan tabel dan bagan hasil pengujian dari masing masing deteksi serangan :

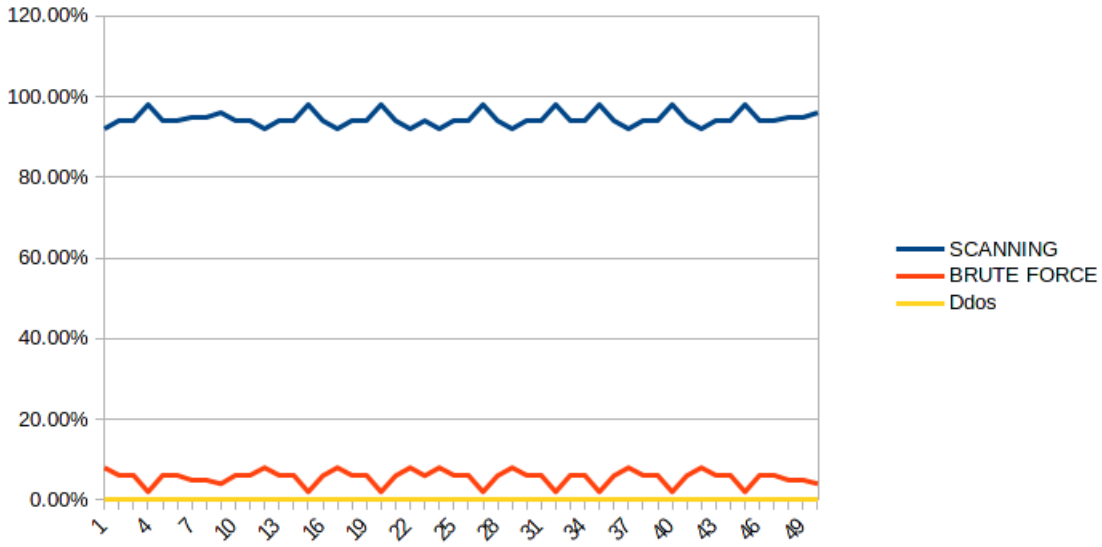
A. Akurasi Deteksi *Scanning*

Berikut adalah tabel hasil pengujian akurasi deteksi serangan *Scanning* tanpa paket normal yang penulis dapatkan

Tabel 4.15 Akurasi Deteksi *Scanning*

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
1	92.00%	8.00%	0.00%	NMAP
2	94.00%	6.00%	0.00%	NMAP
3	94.00%	6.00%	0.00%	METASPLOIT
4	98.00%	2.00%	0.00%	TCP SCANNING
5	94.00%	6.00%	0.00%	NESSUS
6	94.00%	6.00%	0.00%	NESSUS
7	95.00%	5.00%	0.00%	NMAP
8	95.00%	5.00%	0.00%	METASPLOIT
9	96.00%	4.00%	0.00%	METASPLOIT
10	94.00%	6.00%	0.00%	TCP SCANNING
11	94.00%	6.00%	0.00%	NESSUS
12	92.00%	8.00%	0.00%	TCP SCANNING
13	94.00%	6.00%	0.00%	METASPLOIT
14	94.00%	6.00%	0.00%	METASPLOIT
15	98.00%	2.00%	0.00%	TCP SCANNING
16	94.00%	6.00%	0.00%	NESSUS
17	92.00%	8.00%	0.00%	NESSUS
18	94.00%	6.00%	0.00%	NMAP
19	94.00%	6.00%	0.00%	METASPLOIT
20	98.00%	2.00%	0.00%	METASPLOIT
21	94.00%	6.00%	0.00%	TCP SCANNING
22	92.00%	8.00%	0.00%	NESSUS
23	94.00%	6.00%	0.00%	TCP SCANNING
24	92.00%	8.00%	0.00%	METASPLOIT
25	94.00%	6.00%	0.00%	NESSUS

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
26	94.00%	6.00%	0.00%	TCP SCANNING
27	98.00%	2.00%	0.00%	METASPLOIT
28	94.00%	6.00%	0.00%	METASPLOIT
29	92.00%	8.00%	0.00%	TCP SCANNING
30	94.00%	6.00%	0.00%	NESSUS
31	94.00%	6.00%	0.00%	NESSUS
32	98.00%	2.00%	0.00%	NMAP
33	94.00%	6.00%	0.00%	METASPLOIT
34	94.00%	6.00%	0.00%	METASPLOIT
35	98.00%	2.00%	0.00%	TCP SCANNING
36	94.00%	6.00%	0.00%	NESSUS
37	92.00%	8.00%	0.00%	TCP SCANNING
38	94.00%	6.00%	0.00%	METASPLOIT
39	94.00%	6.00%	0.00%	METASPLOIT
40	98.00%	2.00%	0.00%	TCP SCANNING
41	94.00%	6.00%	0.00%	NESSUS
42	92.00%	8.00%	0.00%	NESSUS
43	94.00%	6.00%	0.00%	NMAP
44	94.00%	6.00%	0.00%	METASPLOIT
45	98.00%	2.00%	0.00%	METASPLOIT
46	94.00%	6.00%	0.00%	TCP SCANNING
47	94.00%	6.00%	0.00%	NESSUS
48	95.00%	5.00%	0.00%	TCP SCANNING
49	95.00%	5.00%	0.00%	METASPLOIT
50	96.00%	4.00%	0.00%	NMAP
RATA-RATA	94.48%	5.52%	0.00%	



Gambar 4.1 Grafik Deteksi Scanning

Pada pengujian akurasi deteksi *scanning* yang belum dimasukan deteksi paket normal didapatkan hasil rata rata deteksi *scanning* 94.48%, *brute force* 5.52% dan *DDoS* 0%

Berdasarkan hasil pengujian pada deteksi akurasi *scanning* terdapat *traffik anomali* serangan *brute force* sebesar 5.52% . Setelah menganalisa traffik *scanning* dengan *wireshark* didapatkan proses *syn / syncronise* pada service *ssh dan ftp* . Hal ini didasarkan ketika proses *scanning* terjadi maka setiap *service* yang aktip akan menerima proses sinkronisasi pada TCP , untuk mengetahui apakah sebuah service aktip atau tidak.

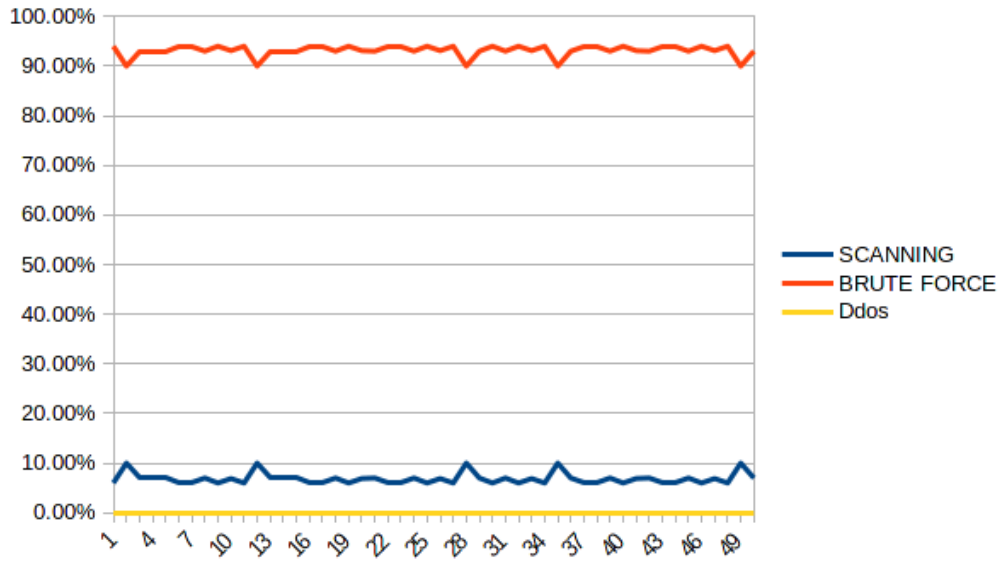
B. Akurasi Serangan *Brute Force*

Berikut akurasi serangan *Brute Force* tanpa paket normal

Tabel 4.16 Akurasi Serangan *Brute Force*

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
1	6.00%	94.00%	0.00%	MEDUSA
2	10.00%	90.00%	0.00%	HYDRA
3	7.00%	93.00%	0.00%	MEDUSA
4	7.00%	93.00%	0.00%	MEDUSA
5	7.00%	93.00%	0.00%	ZERO BRUTE
6	6.00%	94.00%	0.00%	METASPLOIT
7	6.00%	94.00%	0.00%	NMAP (NSE)
8	7.00%	93.00%	0.00%	NMAP (NSE)
9	6.00%	94.00%	0.00%	HYDRA
10	6.89%	93.11%	0.00%	MEDUSA
11	6.00%	94.00%	0.00%	HYDRA
12	10.00%	90.00%	0.00%	MEDUSA
13	7.00%	93.00%	0.00%	HYDRA
14	7.00%	93.00%	0.00%	MEDUSA
15	7.00%	93.00%	0.00%	METASPLOIT
16	6.00%	94.00%	0.00%	NMAP (NSE)
17	6.00%	94.00%	0.00%	NMAP (NSE)
18	7.00%	93.00%	0.00%	HYDRA
19	6.00%	94.00%	0.00%	MEDUSA
20	6.89%	93.11%	0.00%	NMAP (NSE)
21	7.00%	93.00%	0.00%	HYDRA
22	6.00%	94.00%	0.00%	MEDUSA
23	6.00%	94.00%	0.00%	METASPLOIT
24	7.00%	93.00%	0.00%	MEDUSA
25	6.00%	94.00%	0.00%	METASPLOIT

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
26	6.89%	93.11%	0.00%	METASPLOIT
27	6.00%	94.00%	0.00%	NMAP (NSE)
28	10.00%	90.00%	0.00%	NMAP (NSE)
29	7.00%	93.00%	0.00%	HYDRA
30	6.00%	94.00%	0.00%	MEDUSA
31	7.00%	93.00%	0.00%	HYDRA
32	6.00%	94.00%	0.00%	MEDUSA
33	6.89%	93.11%	0.00%	HYDRA
34	6.00%	94.00%	0.00%	MEDUSA
35	10.00%	90.00%	0.00%	METASPLOIT
36	7.00%	93.00%	0.00%	NMAP (NSE)
37	6.00%	94.00%	0.00%	NMAP (NSE)
38	6.00%	94.00%	0.00%	HYDRA
39	7.00%	93.00%	0.00%	HYDRA
40	6.00%	94.00%	0.00%	MEDUSA
41	6.89%	93.11%	0.00%	METASPLOIT
42	7.00%	93.00%	0.00%	NMAP (NSE)
43	6.00%	94.00%	0.00%	NMAP (NSE)
44	6.00%	94.00%	0.00%	HYDRA
45	7.00%	93.00%	0.00%	MEDUSA
46	6.00%	94.00%	0.00%	NMAP (NSE)
47	6.89%	93.11%	0.00%	HYDRA
48	6.00%	94.00%	0.00%	MEDUSA
49	10.00%	90.00%	0.00%	METASPLOIT
50	7.00%	93.00%	0.00%	MEDUSA
RATA-RATA	7.00%	93.00%	0.00%	



Gambar 4.2 Grafik Deteksi *Brute Force* Tanpa Paket Normal

Pada pengujian akurasi deteksi *scanning* yang belum dimasukan deteksi paket normal didapatkan hasil rata rata deteksi *scanning* 6.85%, *brute force* 93.15% dan *DDoS* 0%

Sama halnya dengan hasil pengujian deteksi akurasi *scanning* akan ditemukan *anomali traffik* serangan *brute force* sebesar 6.85%. Hal ini dikarenakan ketikana akan melakukan *brute force* pada service yang akan di serangan , dalam kasus ini dilakukan serangan pada *service ssh*, setiap 5 detik (setingan default hydra yang digunakan untuk brute force) akan melakukan syncronisasi yang membawa payload *traffik scanning* hal ini yang menyebabkan terjadinya serangan *scanning* pada serangan *brute force*

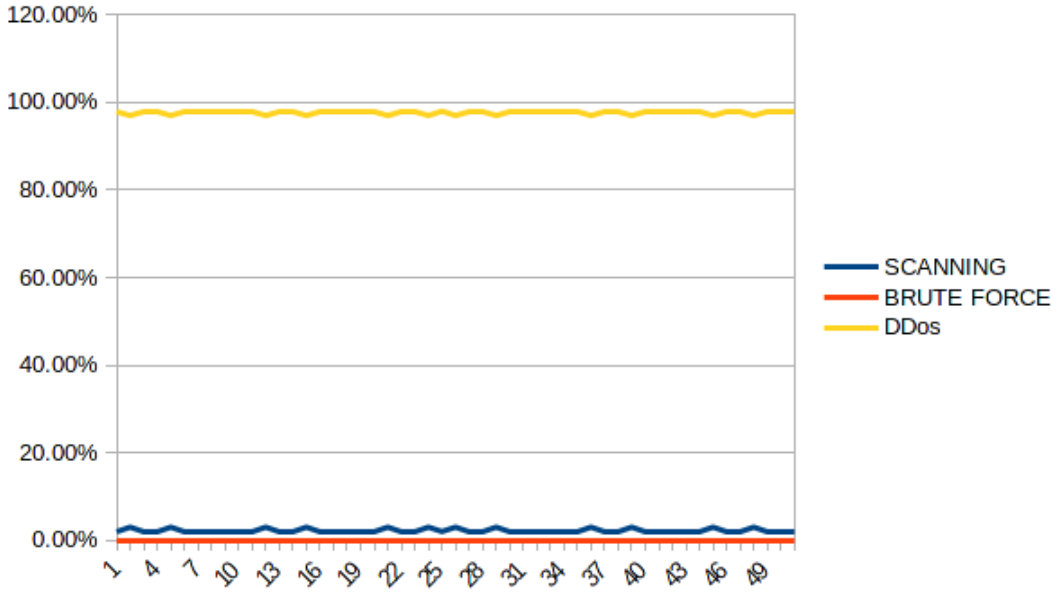
C. Akurasi Deteksi DDoS

Berikut akurasi serangan *DDoS* tanpa paket normal

Tabel 4.17 Akurasi Serangan DDoS

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
1	2.00%	0.00%	98.00%	METASPLOIT
2	3.00%	0.00%	97.00%	METASPLOIT
3	2.00%	0.00%	98.00%	SLOWLORIS
4	2.00%	0.00%	98.00%	PYLoris
5	3.00%	0.00%	97.00%	HULK
6	2.00%	0.00%	98.00%	HULK
7	2.00%	0.00%	98.00%	TCP FLOOD
8	2.00%	0.00%	98.00%	METASPLOIT
9	2.00%	0.00%	98.00%	METASPLOIT
10	2.00%	0.00%	98.00%	SLOWLORIS
11	2.00%	0.00%	98.00%	PYLoris
12	3.00%	0.00%	97.00%	HULK
13	2.00%	0.00%	98.00%	HULK
14	2.00%	0.00%	98.00%	SLOWLORIS
15	3.00%	0.00%	97.00%	PYLoris
16	2.00%	0.00%	98.00%	HULK
17	2.00%	0.00%	98.00%	HULK
18	2.00%	0.00%	98.00%	TCP FLOOD
19	2.00%	0.00%	98.00%	TCP FLOOD
20	2.00%	0.00%	98.00%	PYLoris
21	3.00%	0.00%	97.00%	HULK
22	2.00%	0.00%	98.00%	HULK
23	2.00%	0.00%	98.00%	TCP FLOOD
24	3.00%	0.00%	97.00%	METASPLOIT
25	2.00%	0.00%	98.00%	METASPLOIT

NOMER	SCANNING	BRUTE FORCE	DDoS	KETERANGAN
26	3.00%	0.00%	97.00%	SLOWLORIS
27	2.00%	0.00%	98.00%	PYLoris
28	2.00%	0.00%	98.00%	HULK
29	3.00%	0.00%	97.00%	HULK
30	2.00%	0.00%	98.00%	SLOWLORIS
31	2.00%	0.00%	98.00%	PYLoris
32	2.00%	0.00%	98.00%	HULK
33	2.00%	0.00%	98.00%	HULK
34	2.00%	0.00%	98.00%	HULK
35	2.00%	0.00%	98.00%	TCP FLOOD
36	3.00%	0.00%	97.00%	METASPLOIT
37	2.00%	0.00%	98.00%	METASPLOIT
38	2.00%	0.00%	98.00%	SLOWLORIS
39	3.00%	0.00%	97.00%	PYLoris
40	2.00%	0.00%	98.00%	METASPLOIT
41	2.00%	0.00%	98.00%	METASPLOIT
42	2.00%	0.00%	98.00%	SLOWLORIS
43	2.00%	0.00%	98.00%	SLOWLORIS
44	2.00%	0.00%	98.00%	PYLoris
45	3.00%	0.00%	97.00%	HULK
46	2.00%	0.00%	98.00%	HULK
47	2.00%	0.00%	98.00%	SLOWLORIS
48	3.00%	0.00%	97.00%	TCP FLOOD
49	2.00%	0.00%	98.00%	METASPLOIT
50	2.00%	0.00%	98.00%	METASPLOIT
RATA-RATA	2.00%	0.00%	98.00%	



Gambar 4.3 Grafik Deteksi DDoS Tanpa Paket Normal

Pada hasil pengujian akurasi serangan deteksi DDoS didapatkan hasil rata-rata deteksi *(scanning)* 2.23% , *brute force* 0.00 % dan *DDoS* 97.73% .

Pada serangan ini pun ditemukan *traffik anomali* serangan *scanning* hal ini diakibatkan karena pada saat proses *DDoS* terjadi , service yang sedang dibanjiri *traffik DDoS* secara terus menurus akan melakukan proses *syn/ack* kepada *host* yang melakukan serangan, pada proses itu ada *traffik* yang sama dengan *traffik scanning*

4.3.2 Skenario Kedua

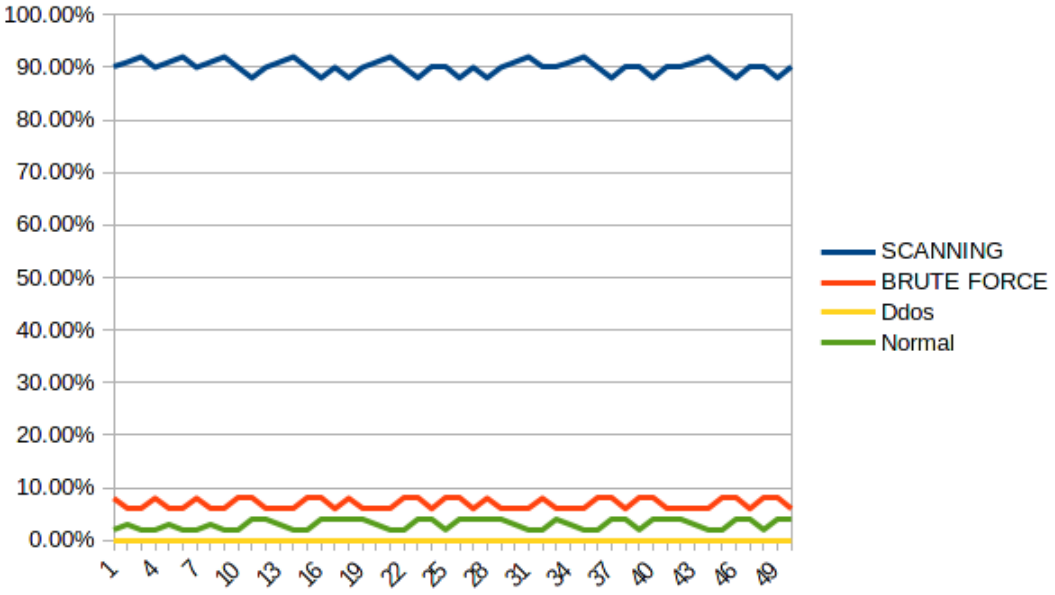
Pada scenario ini akan diuji masing masing akurasi deteksi serangan dengan memasukan *rule* traffik normal,pengujian ini dilakukan sealama 50 kali pengujian serangan dimana masing-masing serangan dilakukan secara satu persatu atau terpisah disamping itu dalam penelitian tugas akhir ini dilukan monitoring penggunaan serangan, berikut kami sajikan table dan bagan hasil pengujian dari masing masing akurasi deteksi serangan :

A. Akurasi Deteksi Scanning Dengan Memasukan Data Normal

Tabel 4.18 Akurasi Deteksi Scanning Dengan Memasukan Data Normal

NOMER	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
1	90.00%	8.00%	0.00%	2%	NMAP
2	91.00%	6.00%	0.00%	3%	NMAP
3	92.00%	6.00%	0.00%	2%	METASPLOIT
4	90.00%	8.00%	0.00%	2%	TCP SCANNING
5	91.00%	6.00%	0.00%	3%	NESSUS
6	92.00%	6.00%	0.00%	2%	NESSUS
7	90.00%	8.00%	0.00%	2%	NMAP
8	91.00%	6.00%	0.00%	3%	METASPLOIT
9	92.00%	6.00%	0.00%	2%	METASPLOIT
10	90.00%	8.00%	0.00%	2%	TCP SCANNING
11	88.00%	8.00%	0.00%	4%	NESSUS
12	90.00%	6.00%	0.00%	4%	TCP SCANNING
13	91.00%	6.00%	0.00%	3%	METASPLOIT
14	92.00%	6.00%	0.00%	2%	METASPLOIT
15	90.00%	8.00%	0.00%	2%	TCP SCANNING
16	88.00%	8.00%	0.00%	4%	NESSUS
17	90.00%	6.00%	0.00%	4%	NESSUS
18	88.00%	8.00%	0.00%	4%	NMAP
19	90.00%	6.00%	0.00%	4%	METASPLOIT

NOMER	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
20	91.00%	6.00%	0.00%	3%	METASPLOIT
21	92.00%	6.00%	0.00%	2%	TCP SCANNING
22	90.00%	8.00%	0.00%	2%	NESSUS
23	88.00%	8.00%	0.00%	4%	TCP SCANNING
24	90.00%	6.00%	0.00%	4%	METASPLOIT
25	90.00%	8.00%	0.00%	2%	NESSUS
26	88.00%	8.00%	0.00%	4%	TCP SCANNING
27	90.00%	6.00%	0.00%	4%	METASPLOIT
28	88.00%	8.00%	0.00%	4%	METASPLOIT
29	90.00%	6.00%	0.00%	4%	TCP SCANNING
30	91.00%	6.00%	0.00%	3%	NESSUS
31	92.00%	6.00%	0.00%	2%	NESSUS
32	90.00%	8.00%	0.00%	2%	NMAP
33	90.00%	6.00%	0.00%	4%	METASPLOIT
34	91.00%	6.00%	0.00%	3%	METASPLOIT
35	92.00%	6.00%	0.00%	2%	TCP SCANNING
36	90.00%	8.00%	0.00%	2%	NESSUS
37	88.00%	8.00%	0.00%	4%	TCP SCANNING
38	90.00%	6.00%	0.00%	4%	METASPLOIT
39	90.00%	8.00%	0.00%	2%	METASPLOIT
40	88.00%	8.00%	0.00%	4%	TCP SCANNING
41	90.00%	6.00%	0.00%	4%	NESSUS
42	90.00%	6.00%	0.00%	4%	NESSUS
43	91.00%	6.00%	0.00%	3%	NMAP
44	92.00%	6.00%	0.00%	2%	METASPLOIT
45	90.00%	8.00%	0.00%	2%	METASPLOIT
46	88.00%	8.00%	0.00%	4%	TCP SCANNING
47	90.00%	6.00%	0.00%	4%	NESSUS
48	90.00%	8.00%	0.00%	2%	TCP SCANNING
49	88.00%	8.00%	0.00%	4%	METASPLOIT
50	90.00%	6.00%	0.00%	4%	NMAP
RATA-RATA	90.08%	6.88%	0.00%	3.04%	



Gambar 4.4 Grafik Deteksi Scanning Dengan Paket Normal

Pada pengujian yang ini didapatkan hasil akurasi *scanning* 90.08% *brute force* 6.88% *DDoS* 0.0% dan paket normal 3.04 %.

Sama halnya dengan peengujian sebelumnya akan terdeteksi juga serangan *brute force*

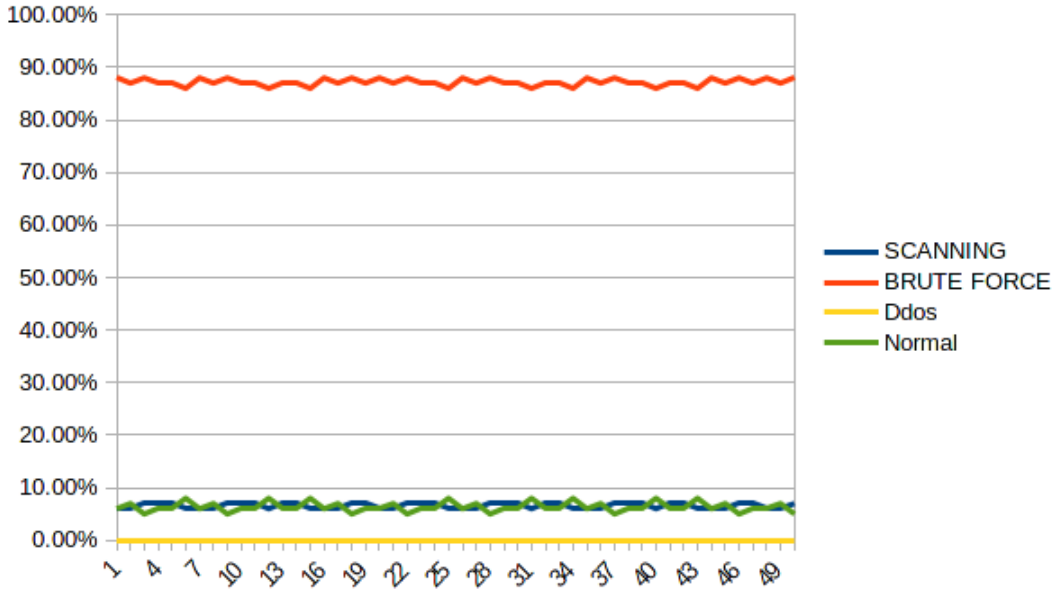
Setalah memasukan deteksi *traffik* normal akan didapatkan pada serangan *scanning* sebesar 3.04% hal itu diakibatkan kerana proses *echo-reply* paket *icmp*

B. Akurasi Deteksi Brute Force Dengan Memasukan Data Normal

Tabel 4.19 Akurasi Deteksi Brute Force Dengan Memasukan Data Normal

NOMER	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
1	6.00%	88.00%	0.00%	6%	MEDUSA
2	6.00%	87.00%	0.00%	7%	HYDRA
3	7.00%	88.00%	0.00%	5%	MEDUSA
4	7.00%	87.00%	0.00%	6%	MEDUSA
5	7.00%	87.00%	0.00%	6%	ZERO BRUTE
6	6.00%	86.00%	0.00%	8%	METASPLOIT
7	6.00%	88.00%	0.00%	6%	NMAP (NSE)
8	6.00%	87.00%	0.00%	7%	NMAP (NSE)
9	7.00%	88.00%	0.00%	5%	HYDRA
10	7.00%	87.00%	0.00%	6%	MEDUSA
11	7.00%	87.00%	0.00%	6%	HYDRA
12	6.00%	86.00%	0.00%	8%	MEDUSA
13	7.00%	87.00%	0.00%	6%	HYDRA
14	7.00%	87.00%	0.00%	6%	MEDUSA
15	6.00%	86.00%	0.00%	8%	METASPLOIT
16	6.00%	88.00%	0.00%	6%	NMAP (NSE)
17	6.00%	87.00%	0.00%	7%	NMAP (NSE)
18	7.00%	88.00%	0.00%	5%	HYDRA
19	7.00%	87.00%	0.00%	6%	MEDUSA
20	6.00%	88.00%	0.00%	6%	NMAP (NSE)
21	6.00%	87.00%	0.00%	7%	HYDRA
22	7.00%	88.00%	0.00%	5%	MEDUSA
23	7.00%	87.00%	0.00%	6%	METASPLOIT
24	7.00%	87.00%	0.00%	6%	MEDUSA
25	6.00%	86.00%	0.00%	8%	METASPLOIT

NOMER	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
26	6.00%	88.00%	0.00%	6%	METASPLOIT
27	6.00%	87.00%	0.00%	7%	NMAP (NSE)
28	7.00%	88.00%	0.00%	5%	NMAP (NSE)
29	7.00%	87.00%	0.00%	6%	HYDRA
30	7.00%	87.00%	0.00%	6%	MEDUSA
31	6.00%	86.00%	0.00%	8%	HYDRA
32	7.00%	87.00%	0.00%	6%	MEDUSA
33	7.00%	87.00%	0.00%	6%	HYDRA
34	6.00%	86.00%	0.00%	8%	MEDUSA
35	6.00%	88.00%	0.00%	6%	METASPLOIT
36	6.00%	87.00%	0.00%	7%	NMAP (NSE)
37	7.00%	88.00%	0.00%	5%	NMAP (NSE)
38	7.00%	87.00%	0.00%	6%	HYDRA
39	7.00%	87.00%	0.00%	6%	HYDRA
40	6.00%	86.00%	0.00%	8%	MEDUSA
41	7.00%	87.00%	0.00%	6%	METASPLOIT
42	7.00%	87.00%	0.00%	6%	NMAP (NSE)
43	6.00%	86.00%	0.00%	8%	NMAP (NSE)
44	6.00%	88.00%	0.00%	6%	HYDRA
45	6.00%	87.00%	0.00%	7%	MEDUSA
46	7.00%	88.00%	0.00%	5%	NMAP (NSE)
47	7.00%	87.00%	0.00%	6%	HYDRA
48	6.00%	88.00%	0.00%	6%	MEDUSA
49	6.00%	87.00%	0.00%	7%	METASPLOIT
50	7.00%	88.00%	0.00%	5%	MEDUSA
RATA-RATA	6.52%	87.15%	0.00%	6.33%	



Gambar 4.5 Grafik Deteksi Brute Force Dengan Paket Normal

Pada pengujian yang ini didapatkan hasil akurasi *scanning* 6.52% *brute force* 87.16% *DDoS* 0.0% dan paket normal 6.32 %.

Sama halnya dengan peengujian sebelumnya akan terdeteksi juga serangan *scanning*

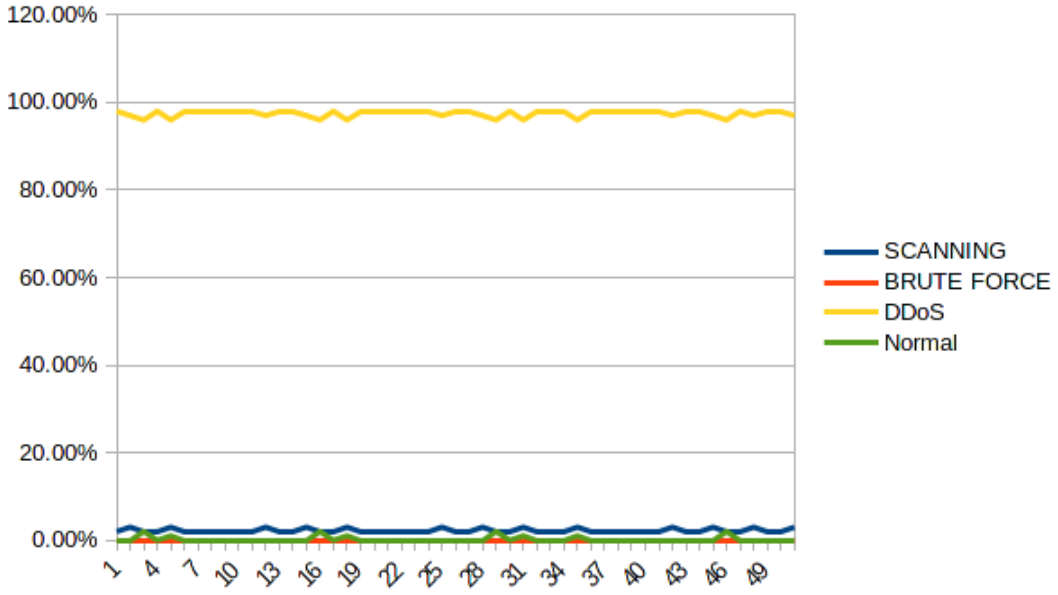
Setalah memasukan deteksi *traffik* normal akan didapatkan pada serangan *scanning* sebesar 6.32% hal itu diakibatkan kerana proses *echo-reply* paket *icmp*

C. Akurasi Deteksi DDoS Dengan Memasukan Data Normal

Tabel 4.20 Akurasi Deteksi DDoS Dengan Memasukan Data Normal

NOMER	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
1	2.00%	0.00%	98.00%	0%	METASPLOIT
2	3.00%	0.00%	97.00%	0%	METASPLOIT
3	2.00%	0.00%	96.00%	2%	SLOWLORIS
4	2.00%	0.00%	98.00%	0%	PYLoris
5	3.00%	0.00%	96.00%	1%	HULK
6	2.00%	0.00%	98.00%	0%	HULK
7	2.00%	0.00%	98.00%	0%	TCP FLOOD
8	2.00%	0.00%	98.00%	0%	METASPLOIT
9	2.00%	0.00%	98.00%	0%	METASPLOIT
10	2.00%	0.00%	98.00%	0%	SLOWLORIS
11	2.00%	0.00%	98.00%	0%	PYLoris
12	3.00%	0.00%	97.00%	0%	HULK
13	2.00%	0.00%	98.00%	0%	HULK
14	2.00%	0.00%	98.00%	0%	SLOWLORIS
15	3.00%	0.00%	97.00%	0%	PYLoris
16	2.00%	0.00%	96.00%	2%	HULK
17	2.00%	0.00%	98.00%	0%	HULK
18	3.00%	0.00%	96.00%	1%	TCP FLOOD
19	2.00%	0.00%	98.00%	0%	TCP FLOOD
20	2.00%	0.00%	98.00%	0%	PYLoris
21	2.00%	0.00%	98.00%	0%	HULK
22	2.00%	0.00%	98.00%	0%	HULK
23	2.00%	0.00%	98.00%	0%	TCP FLOOD
24	2.00%	0.00%	98.00%	0%	METASPLOIT

NO	SCANNING	BRUTE FORCE	DDoS	NORMAL	KETERANGAN
25	3.00%	0.00%	97.00%	0%	METASPLOIT
26	2.00%	0.00%	98.00%	0%	SLOWLORIS
27	2.00%	0.00%	98.00%	0%	PYLoris
28	3.00%	0.00%	97.00%	0%	HULK
29	2.00%	0.00%	96.00%	2%	HULK
30	2.00%	0.00%	98.00%	0%	SLOWLORIS
31	3.00%	0.00%	96.00%	1%	PYLoris
32	2.00%	0.00%	98.00%	0%	HULK
33	2.00%	0.00%	98.00%	0%	HULK
34	2.00%	0.00%	98.00%	0%	HULK
35	3.00%	0.00%	96.00%	1%	TCP FLOOD
36	2.00%	0.00%	98.00%	0%	METASPLOIT
37	2.00%	0.00%	98.00%	0%	METASPLOIT
38	2.00%	0.00%	98.00%	0%	SLOWLORIS
39	2.00%	0.00%	98.00%	0%	PYLoris
40	2.00%	0.00%	98.00%	0%	METASPLOIT
41	2.00%	0.00%	98.00%	0%	METASPLOIT
42	3.00%	0.00%	97.00%	0%	SLOWLORIS
43	2.00%	0.00%	98.00%	0%	SLOWLORIS
44	2.00%	0.00%	98.00%	0%	PYLoris
45	3.00%	0.00%	97.00%	0%	HULK
46	2.00%	0.00%	96.00%	2%	HULK
47	2.00%	0.00%	98.00%	0%	SLOWLORIS
48	3.00%	0.00%	97.00%	0%	TCP FLOOD
49	2.00%	0.00%	98.00%	0%	METASPLOIT
50	2.00%	0.00%	98.00%	0%	METASPLOIT
RATA-RATA	3.00%	0.00%	97.00%	0%	



Gambar 4.6 Grafik Deteksi DDoS Dengan Paket Normal

Pada pengujian yang ini didapatkan hasil akurasi *scanning* 2.25% *brute force* 0.00% *DDoS* 97.51% dan paket normal 0.24 %.

Sama halnya dengan peengujian sebelumnya akan terdeteksi juga serangan *scanning*

Setalah memasukan deteksi *traffik* normal akan didapatkan pada serangan *scanning* sebesar 0.24% hal itu diakibatkan kerana proses *echo-reply* paket *icmp*

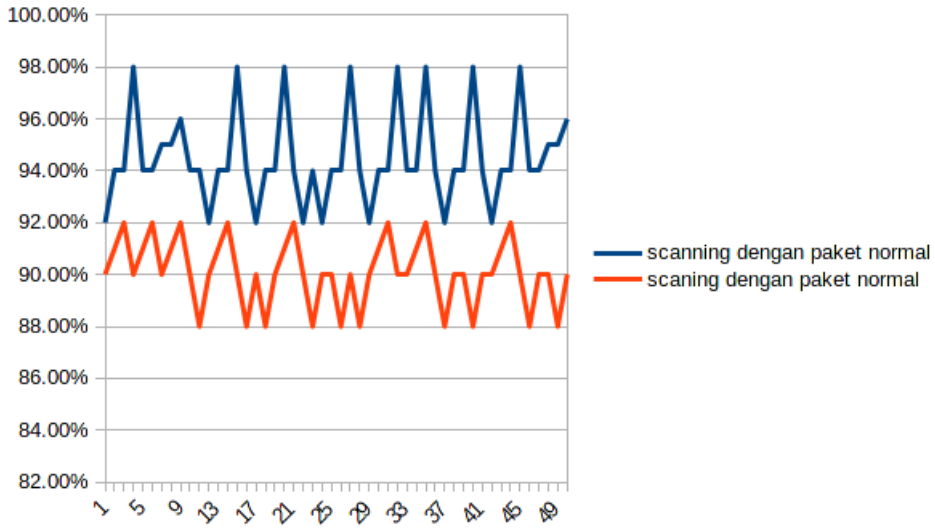
4.3.3 Skenario Ketiga

Pada pengujian di skenario ini , akan ditunjukan perbandingan akurasi deteksi antara menggunakan paket normal dan tidak menggunakan paket normal

A. Perbandingan Akurasi Deteksi Scanning

Tabel 4.21 Perbandingan Akurasi Deteksi Scanning

no	Scanning tanpa paket normal	Scanning dengan paket normal	no	Scanning tanpa paket normal	Scanning dengan paket normal
1	92.00%	90.00%	26	94.00%	88.00%
2	94.00%	91.00%	27	98.00%	90.00%
3	94.00%	92.00%	28	94.00%	88.00%
4	98.00%	90.00%	29	92.00%	90.00%
5	94.00%	91.00%	30	94.00%	91.00%
6	94.00%	92.00%	31	94.00%	92.00%
7	95.00%	90.00%	32	98.00%	90.00%
8	95.00%	91.00%	33	94.00%	90.00%
9	96.00%	92.00%	34	94.00%	91.00%
10	94.00%	90.00%	35	98.00%	92.00%
11	94.00%	88.00%	36	94.00%	90.00%
12	92.00%	90.00%	37	92.00%	88.00%
13	94.00%	91.00%	38	94.00%	90.00%
14	94.00%	92.00%	39	94.00%	90.00%
15	98.00%	90.00%	40	98.00%	88.00%
16	94.00%	88.00%	41	94.00%	90.00%
17	92.00%	90.00%	42	92.00%	90.00%
18	94.00%	88.00%	43	94.00%	91.00%
19	94.00%	90.00%	44	94.00%	92.00%
20	98.00%	91.00%	45	98.00%	90.00%
21	94.00%	92.00%	46	94.00%	88.00%
22	92.00%	90.00%	47	94.00%	90.00%
23	94.00%	88.00%	48	95.00%	90.00%
24	92.00%	90.00%	49	95.00%	88.00%
25	94.00%	90.00%	50	96.00%	90.00%
		rata - rata		94.48%	90.08%



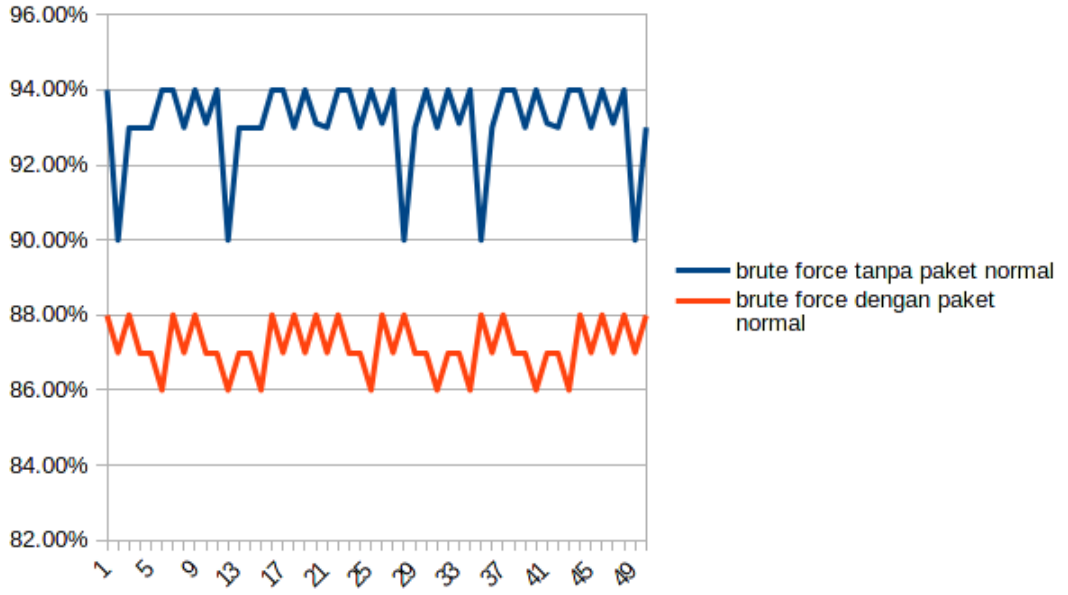
Gambar 4.7 Perbandinan Akurasi Deteksi Scanning

Pada hasil perbandingan ini didapatkan hasil *(scanning)* tanpa paket normal 94.48% dan dengan paket normal 90.08%. Seperti hasil penelitian pada skenario ke-dua hasil yang didapatkan pada hasil *scanning* tanpa paket normal lebih besar dengan *scanning* yang menggunakan paket normal . Hal ini diakibatkan karena serangan *scanning* memerlukan echo-replay terhadap target

B. Perbandingan Akurasi Deteksi Brute Force

Tabel 4.22 Perbandingan Akurasi Deteksi Brute Force

no	Brute force tanpa paket normal	Brute force dengan paket normal	no	Brute forcetanpa paket normal	Brute force dengan paket normal
1	94.00%	88.00%	26	93.11%	88.00%
2	90.00%	87.00%	27	94.00%	87.00%
3	93.00%	88.00%	28	90.00%	88.00%
4	93.00%	87.00%	29	93.00%	87.00%
5	93.00%	87.00%	30	94.00%	87.00%
6	94.00%	86.00%	31	93.00%	86.00%
7	94.00%	88.00%	32	94.00%	87.00%
8	93.00%	87.00%	33	93.11%	87.00%
9	94.00%	88.00%	34	94.00%	86.00%
10	93.11%	87.00%	35	90.00%	88.00%
11	94.00%	87.00%	36	93.00%	87.00%
12	90.00%	86.00%	37	94.00%	88.00%
13	93.00%	87.00%	38	94.00%	87.00%
14	93.00%	87.00%	39	93.00%	87.00%
15	93.00%	86.00%	40	94.00%	86.00%
16	94.00%	88.00%	41	93.11%	87.00%
17	94.00%	87.00%	42	93.00%	87.00%
18	93.00%	88.00%	43	94.00%	86.00%
19	94.00%	87.00%	44	94.00%	88.00%
20	93.11%	88.00%	45	93.00%	87.00%
21	93.00%	87.00%	46	94.00%	88.00%
22	94.00%	88.00%	47	93.11%	87.00%
23	94.00%	87.00%	48	94.00%	88.00%
24	93.00%	87.00%	49	90.00%	87.00%
25	94.00%	86.00%	50	93.00%	88.00%
		rata - rata		93.15%	87.16%



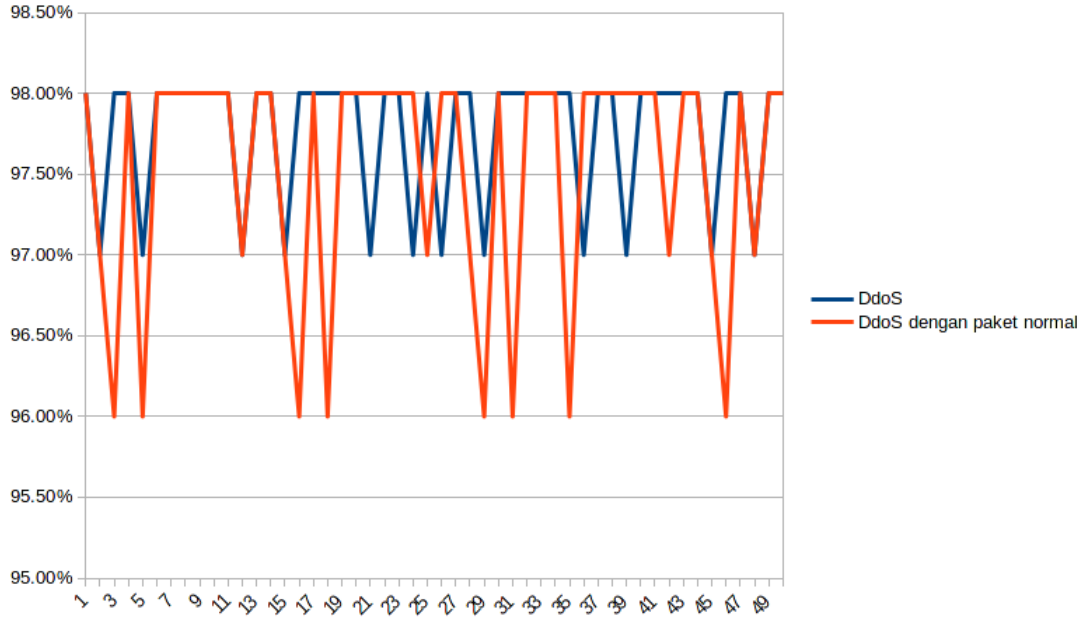
Gambar 4.8 Perbandingan Akurasi Deteksi Brute Force

Pada hasil perbandingan ini didapatkan hasil *(brute force)* tanpa paket normal 93.15% dan dengan paket normal 87.16%. Seperti hasil penelitian pada skenario kedua hasil yang didapatkan pada hasil *brute force* tanpa paket normal lebih besar dengan *brute force* yang menggunakan paket normal . Hal ini diakibatkan karena serangan *brute force* memerlukan echo-replay terhadap target hal ini juga didapatkan pada serangan *scanning*

C. Perbandingan Akurasi Deteksi DDoS

Tabel 4.23 Perbandinan Akurasi Deteksi DDoS

no	DDoS tanpa paket normal	DDoS dengan paket normal	no	DDoS tanpa paket normal	DDoS dengan paket normal
1	98.00%	98.00%	26	97.00%	98.00%
2	97.00%	97.00%	27	98.00%	98.00%
3	98.00%	96.00%	28	98.00%	97.00%
4	98.00%	98.00%	29	97.00%	96.00%
5	97.00%	96.00%	30	98.00%	98.00%
6	98.00%	98.00%	31	98.00%	96.00%
7	98.00%	98.00%	32	98.00%	98.00%
8	98.00%	98.00%	33	98.00%	98.00%
9	98.00%	98.00%	34	98.00%	98.00%
10	98.00%	98.00%	35	98.00%	96.00%
11	98.00%	98.00%	36	97.00%	98.00%
12	97.00%	97.00%	37	98.00%	98.00%
13	98.00%	98.00%	38	98.00%	98.00%
14	98.00%	98.00%	39	97.00%	98.00%
15	97.00%	97.00%	40	98.00%	98.00%
16	98.00%	96.00%	41	98.00%	98.00%
17	98.00%	98.00%	42	98.00%	97.00%
18	98.00%	96.00%	43	98.00%	98.00%
19	98.00%	98.00%	44	98.00%	98.00%
20	98.00%	98.00%	45	97.00%	97.00%
21	97.00%	98.00%	46	98.00%	96.00%
22	98.00%	98.00%	47	98.00%	98.00%
23	98.00%	98.00%	48	97.00%	97.00%
24	97.00%	98.00%	49	98.00%	98.00%
25	98.00%	97.00%	50	98.00%	98.00%
		rata - rata		97.76%	97.52%



Gambar 4.9 Perbandinan Akurasi Deteksi DDoS

Pada hasil perbandingan ini didapatkan hasil *DDoS* tanpa paket normal 97.76% dan dengan paket normal 97.52%. Seperti hasil penelitian pada skenario kedua hasil yang didapatkan pada hasil *DDoS* tanpa paket normal lebih besar dengan *DDoS* yang menggunakan paket normal . Hal ini diakibatkan karena serangan *DDoS* memerlukan echo-replay, namum pada serangan DDoS didapatkan hasil selisih yang sangat kecil yaitu 0.24% hal ini karena serangan DDoS mengirim hampir 400 paket perdetik pada tiap sekali melakukan *three-way-handshake (echo-replay)*

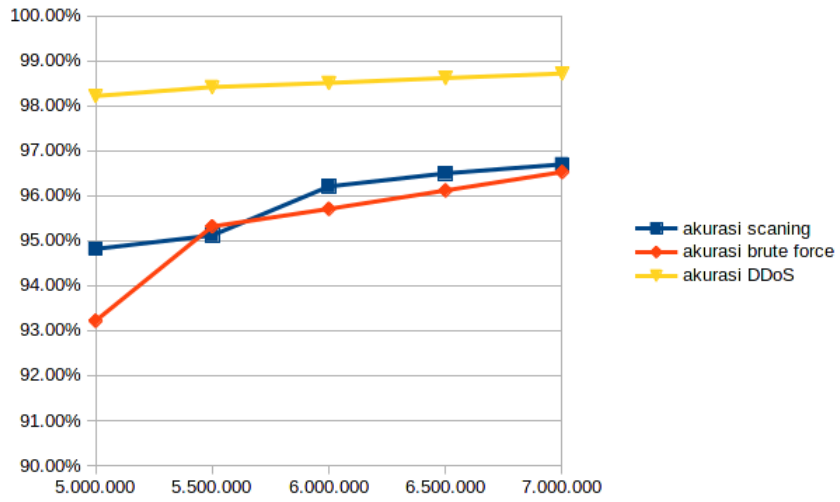
4.3.4 Skenario Keempat

Pada pengujian Skenarion ini akan diuji persentase akurasi berdasarkan banyaknya datasetm jumlah dataset yang diuji akan ditambah sebanyak 10% dari dataset awal sehingga setiap pengujian akan ditambah sebanyak 500.000 dataset , pengujian ini dilakukan pada sistem operasi Arch linux 64 bit dengan kapasitas Hardware RAM (8 GB) , CPU (2,5 GHz quad core), SSD (read 300 MB, write 350 MB). berikut adalah tabel dan bagan hasil pengujian yang didapatkan:

A. Akurasi Deteksi *(Scanning)* Terhadap Penambahan Dataset

Tabel 4.24 Akurasi Serangan Terhadap Penambahan Dataset

jumlah data set	akurasi scanning	akurasi brute force	akurasi DDoS
5.000.000	94.82%	93.22%	98.22%
5.500.000	95.12%	95.32%	98.34%
6.000.000	96.21%	95.71%	98.51%
6.500.000	96.50%	96.12%	98.62%
7.000.000	96.70%	96.56%	98.72%



Gambar 4.10 Akurasi Deteksi Serangan Dengan Penambahan Dataset

pada pengujian ini hanya mampu melukan pengolahan data pada batas maksimal 7.200.000 s/d 7.300.000 data , jika lebih dari itu aplikasi akan mengalami *force closed*

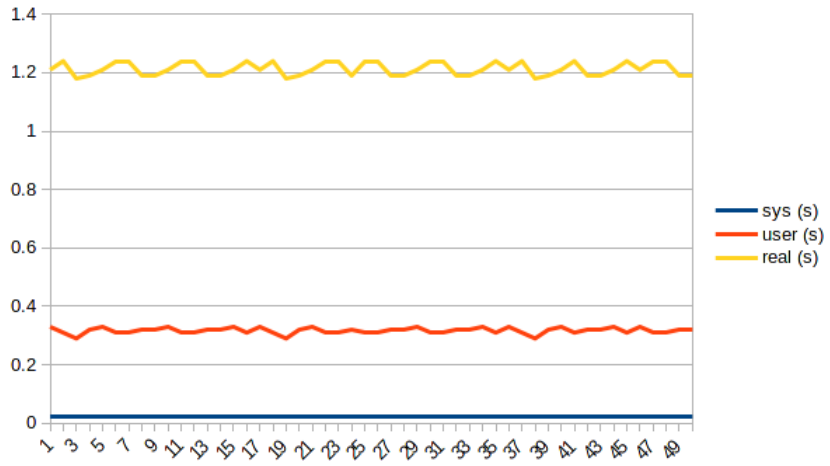
4.3.5 Skenarion Kelima

Pada pengukuran ini dilakukan untuk mengetahui waktu yang dibutuhkan untuk komunikasi antara telegram dan server. Para meter pengukuran ada 3 macan yaitu sys (waktu yang dibutukan system untuk melakukan compiler program), user (waktu yang dibutuhkan untuk interpreter menjalankan program), dan real(waktu yang dibutuhkan untuk menjalankan program sepenuhnya). Pada waktu real ini adalah waktu yang dibutuhkan unutk komuniasi antara Telegram dan Server cnc , waktu real berpengaruh pada kecepatan internet . semakin cepat koneksi internet maka semakin cepat waktu yang dibutuhkan, pada pengujian ini dilakukan pengujian pada kecepatan internet dengan kecepatan download 900/Kbps dan upload 100/Kbps. Dengan data table pengujian sebagai berikut :

Tabel 4.25waktu pengiriman telegram-server

no	sys (s)	user (s)	real (s)	no	sys (s)	user (s)	real (s)
1	0.021	0.33	1.21	26	0.023	0.31	1.24
2	0.023	0.31	1.24	27	0.023	0.32	1.19
3	0.021	0.29	1.18	28	0.023	0.32	1.19
4	0.023	0.32	1.19	29	0.021	0.33	1.21
5	0.021	0.33	1.21	30	0.023	0.31	1.24
6	0.023	0.31	1.24	31	0.023	0.31	1.24
7	0.023	0.31	1.24	32	0.023	0.32	1.19
8	0.023	0.32	1.19	33	0.023	0.32	1.19
9	0.023	0.32	1.19	34	0.021	0.33	1.21
10	0.021	0.33	1.21	35	0.023	0.31	1.24
11	0.023	0.31	1.24	36	0.021	0.33	1.21
12	0.023	0.31	1.24	37	0.023	0.31	1.24
13	0.023	0.32	1.19	38	0.021	0.29	1.18
14	0.023	0.32	1.19	39	0.023	0.32	1.19

no	sys (s)	user (s)	real (s)	no	sys (s)	user (s)	real (s)
15	0.021	0.33	1.21	40	0.021	0.33	1.21
16	0.023	0.31	1.24	41	0.023	0.31	1.24
17	0.021	0.33	1.21	42	0.023	0.32	1.19
18	0.023	0.31	1.24	43	0.023	0.32	1.19
19	0.021	0.29	1.18	44	0.021	0.33	1.21
20	0.023	0.32	1.19	45	0.023	0.31	1.24
21	0.021	0.33	1.21	46	0.021	0.33	1.21
22	0.023	0.31	1.24	47	0.023	0.31	1.24
23	0.023	0.31	1.24	48	0.023	0.31	1.24
24	0.023	0.32	1.19	49	0.023	0.32	1.19
25	0.023	0.31	1.24	50	0.023	0.32	1.19
		rata-rata			0.0224	0.3168	1.2132



Gambar 4.11waktu pengiriman telegram-server

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil analisis dan pengujian fungsional aplikasi ini, didapat kesimpulan sebagai berikut:

1. Semakin banyak data yang diolah sebagai rule deteksi semakin bagus akurasi yang didapatkan.
2. Hasil akurasi yang tidak menggunakan data normal lebih besar dari pada menggunakan data normal.
3. Akurasi deteksi scanning , brute force dan DDoS diatas 75%.
4. Waktu rata-rata komunikasi server dan telegram dibawah 2 detik.

5.2 Saran

1. Gunakan *server* yang mempunyai kapasitas memory yang besar .
2. Diharapkan dapat melakukan pengolahan data secara realtime sehinnga dijadikan *software* dengan sistem *autonomous system* yang dapat melakukan update rule secara berkala.
3. Dengan dasar sofware ini yang dibuat dengan rule terpisah dengan program inti , dihrapkan pengambang dapat mendeteksi jenis serangan lainya.

DAFTAR PUSTAKA

[1] S. B. Wibowo and Widyawan, “Wireless Sensor Network and Internet Protocol Integration with COTS,” in *2013 AUN/SEED-Net Regional Conference in Electrical and Electronics Engineering*. Department of EE, Chulalongkorn University, 2013, pp. 120–123.

[2] M.-E. Raluca, M.-E. Razvan, and A. Terzis, “Gateway design for data gathering sensor networks,” in *Sensor, Mesh and Ad Hoc Communications and Networks, 2008. SECON’08. 5th Annual IEEE Communications Society Conference on*. IEEE, 2008, pp. 296–304.

[3] B. da Silva Campos, J. J. P. C. Rodrigues, L. D. P. Mendes, E. F. Nakamura, and C. M. S. Figueiredo, “Design and construction of wireless sensor network gateway with IPv4/IPv6 support,” in *Communications (ICC), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1–5.

[4] N. S. S. S. C. S. Surabhi Malav, Medankar Sanika Avinash, "Network security using ids, ips honeypot,"" International Journal of Recent Research in Mathematics Computer Science and Information Technology Vol. 2, Issue 2, pp: (27-30), Month: October 2015 15 March 2016,

[5] Dr. S.Vijayarani1, Ms. Maria Sylviaa.Sl, "INTRUSION DETECTION SYSTEM A STUDY," International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015, 2015.

[6] B. M Beigh., "Intrusion Detection and Prevention System: Classification and Quick Review," ARPN Journal of Science and Technology, 2013

[7] B. Prabadevi and N. Jeyanthi, "Distributed Denial of service attacks and its effects on Cloud environment- a survey," The 2014 International Symposium on Networks, Computers and Communications, Hammamet, 2014, pp. 1-5. doi: 10.1109/SNCC.2014.6866508

[8] W. Bhaya and M. EbadyManaa, "DDoS attack detection approach using an efficient cluster analysis in large data scale," 2017 Annual Conference on New Trends in Information Communications Technology Applications (NTICT), Baghdad, Iraq, 2017, pp. 168-173. doi: 10.1109/NTICT.2017.7976110