INVESTIGASI FORENSIK JARINGAN DARI SERANGAN DDOS MENGGUNAKAN METODE NAÏVE BAYES

Skripsi

untuk memenuhi sebagian persyaratan mencapai derajat sarjana S-1

Program Studi Teknik Informatika

Disusun Oleh

Yogi Surya Nugroho

09650001

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA

YOGYAKARTA

2015

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : UIN.02/D.ST/PP.01.1/1707/2015

Skripsi/Tugas Akhir dengan judul : Investigasi Forensik Jaringan Dari Serangan Ddos Menggunakan Metode Naïve Bayes

Yang dipersiapkan dan disusun oleh :
Nama : Yogi Surya Nugroho
NIM : 09650001
Telah dimunaqasyahkan pada : Jum'at, 12 Juni 2015
Nilai Munaqasyah : A / B
Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Arief Ikhwan W, M.Cs
NIP .

Penguji I

Bambang Sugiantoro, M.T
NIP.19751024 200912 1 002

Penguji II

Nurochman, M.Kom
NIP. 19801223 200901 1 007

Yogyakarta, 17 Juni 2015
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

KEMENTERIAN AGAMA UIN SUNAN KALIJAGA FAKULTAS SAINS DAN TEKNOLOGI YOGYAKARTA

Dr. Malzer Said Nahdi, M.Si
NIP. 19550427 198403 2 001

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal :
Lamp :

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama :Yogi Surya Nugroho
NIM : 09650001
Judul Skripsi : **"Investigasi Forensik Jaringan dari Serangan DDOS dengan Menggunakan Metode *Naive Bayes*"**

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 28 Mei 2015
Pembimbing

Arief Ikhwan Wicaksono M.Cs
NIP.

PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama	: Yogi Surya Nugroho
NIM	: 09650001
Program Studi	: Teknik Informatika
Fakultas	: Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul **"Investigasi Forensik Jaringan dari Serangan DDOS dengan Menggunakan Metode Naive Bayes"** tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar sarjana di suatu Perguruan Tinggi, dan sepengetahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 18 Juni 2015

Yang Menyatakan,

Yogi Surya Nugroho
09650001

MOTTO

Keep moving forward ! **(**Meet the Robinson**)**

orang gagal bukan karena ia mengalami kegagalan tapi karena ia tidak bangkit dari kegagalannya tersebut. (Meet the Robinson**)**

In the middle of difficulty lies opportunity**.** (Bruce Lee)

Apabila di dalam diri seseorang masih ada rasa malu dan takut untuk berbuat suatu kebaikan, maka jaminan bagi orang tersebut adalah tidak akan bertemunya ia dengan kemajuan selangkah pun. (Bung Karno**)**

Belajarlah dari kesalahan orang lain. Anda tak dapat hidup cukup lama untuk melakukan semua kesalahan itu sendiri. (Martin Vanbee)

pejuang sejati tak pernah menyerah. Kalau ingin sukses dengan mimpi dan cita-cita, maka kita harus seperti pejuang sejati yang tak kenal menyerah. (Master Shifu)

kamu harus percaya, hanya percaya bahwa hal apapun bisa terjadi. (Master Oogway)

Yesterday is History, tomorrow is a mystery, but today is a gift, that is why it's called a present. (Master Oogway)

Your story might not have such a happy beginning, but that doesn't make you who you are!! It's the rest of your story who you choose to be!

The secret to be special is you have to believe you're special. (Ayah Po)

Kita harus pernah merasakan gagal karena dari situ kita akan bisa untuk bangkit dari kegagalan, kegagalan bukan akhir dari dunia ini. (Yogi Surya)

PERSEMBAHAN

Kupersembahkan karya ini untuk orang-orang spesial yang selalu ada saat aku jatuh dan bangkit...*This is my Spirit....*

× Untuk Mommy Inge... Terima kasih atas segalanya. Yang membuatku untuk bangkit saat aku jatuh, mungkin kejutan kecil saja tidak cukup untuk menggambarkan pengorbananmu. Akan kupersembahkan yang terbaik untukmu.....☺

× Untuk Pappy Penjarwanto yang semakin senja.... sudah cukup untuk bekerja keras saatnya sang striker ini yang harus meneruskan bola kehidupan ini.... *Leave it to me Captain, Let me score a goal in this life* ☺

× Untuk Adikku Yovita Wanda... Liatlah bagaimana sang striker ini akan mencetak gol dalam liga kehidupan ini dan akan membawa Penjarwanto Family menjadi juara.

× Untuk Bapak-Bapak dan Ibu-Ibu Dosen TIF UIN SUKA pak Didik, pak Agung, pak Agus, pak Sumarsono, pak Bambang, pak Awik, pak Imam, pak Mustakim, pak Aulia, pak Nasirudin, pak Taufik, ibu Uyun, ibu Ade, ibu Maria Ulfa terima kasih pak bu karena telah mengajarkan saya banyak hal.

× Untuk Sang gadis medan Nurul Febriani....Terima kasih karena telah membuatku bangkit dan bersemangat Tunggulah kedatanganku di kota Medanmu. ☺

× Untuk Teman-teman Canteen Squad yang sudah dulu mendahului saya seperti Dimas, Isnan, Iwey/Oki, Dellisa, Dissa, Indra, Ulin, Eko, Latif. Terima Kasih karena telah bisa membuatku bangkit dan tertawa setelah aku jatuh. Banyak senang, sedih, tawa, tangis.... Guys aku tunggu kalian di masa depan ini adalah awal petualangan kita jangan pernah kalian lupakan dari mana kita berawal. Buktikan mimpi yang pernah aku mimpikan dulu bahwa kita akan sukses semua.

× Untuk teman-teman di Prodi TIREX 09 senang bisa mengenal kalian semua. Terima kasih atas semua bantuannya.... Akan saya ingat selalu.

× Untuk Pasukan Pembela Bumi 2011 jangan patah semangat jika kalian gagal dan skripsi kalian di coret tetap berjuang all. ☺

× Untuk adek-adek angkatan bawah jangan meniru keburukan dari angkatan atas tiru lah yang baik-baiknya cepat lulus ya . ☺

× Untuk Kawan-Kawan KKN Kulon Progo Semangat selalu terima kasih atas semua cerita di tempat KKN

× Untuk Pemuda Kranggan 8 berjuanglah kalian karena hidup kalian masih panjang Banggakan orang yang kalian sayangi.

× Untuk Pak Wahdan Terima kasih pak karena sabar menghadapi angkatan-angkatan tua seperti saya sukses selalu pak piss....

× Untuk Teman-Teman BCS X PSS SLEMAN yang tetap ALE, serta teman-teman BCS X PSS SLEMAN Squadra Athena terima kasih aku bisa tertawa berkat kalian juga keep spirit guys.

× Untuk Teman-Teman Ragnarok Valhala Rising terima kasih guys kalian telah mengajarkan semua hal, khusus mas Pram, Roni, Farid, Kezia, Shin, Abam, dan Pandu(kalau ke jogja) yang selaluWOE bareng di puri setiap selasa jumat kalian luar binasa rebut juara dari ZVONE.

× Untuk Teman-Teman saya dari Nogotirto yang telah membantu Thanks Guys ayo kita berjuang bersama.

× Untuk Teman-Teman saya yang saya kenal makasih Guys semua ilmu yang sudah kalian berikan dari mengobrol.

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Alhamdulillahirabbil'alamin, puji syukur kehadirat Allah SWT atas limpahan rahmat, hidayah, inayah, serta petunjuk-Nya, sehingga penulis dapat menyelesaikan penelitian dengan judul ***Investigasi Forensik Jaringan dari Serangan DDOS Menggunakan Metode Naïve Bayes***. Shalawat serta salam semoga tercurah kepada rasulullah SAW. Dengan segala kerendahan hati, penulis pada kesempatan kali ini mengucapkan terima kasih kepada :

1. Bapak Prof. Drs. H. Akh. Minhaji, M.A., Ph.D. selaku Rektor Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
2. Orang tua penulis, Bapak Penjarwanto dan Ibunda Engelin Endah Sri Y, yang selalu menyayangi, mendoakan, mendukung, mengingatkan dan menasihati dalam setiap langkah.
3. Ibu Dr. Maizer Said Nahdi, M.Si selaku Dekan Fakultas Saintek dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
4. Bapak Sumarsono, ST., M. Kom. selaku Kepala Program Studi Teknik Informatika Universitas Islam Negeri Sunan Kalijaga Yogyakarta.
5. Bapak Agung Fatwanto, S.Si., M.Kom., Ph.D selaku pembimbing akademik.
6. Bapak Arief Ikhwan Wicaksono M.Cs., selaku dosen pembimbing yang sabar membimbing, mengarahkan, mengoreksi, memotivasi dan memberi nasihat serta saran selama penyusunan skripsi.

7. Seluruh dosen dan karyawan Program Studi Teknik Informatika, terima kasih atas segala ilmu dan bimbingannya selama masa perkuliahan.
8. Keluarga besar Tirex 2009 dan seluruh teman-teman Teknik Informatika UIN Sunan Kalijaga Yogyakarta.

Penulis menyadari masih banyak kekurangan dan kelemahan dalam penelitian ini. Oleh karena itu, segala saran dan kritik selalu penulis harapkan dari pembaca. Akhir kata, semoga penelitian ini dapat bermanfaat bagi pembaca.

Wassalamu'alaikum Wr. Wb.

Yogyakarta, 15 Juni 2015
Penulis

YOGI SURYA NUGROHO
NIM. 09650001

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INVESTIGASI FORENSIK JARINGAN DARI SERANGAN *DDOS* MENGGUNAKAN METODE *NAÏVE BAYES*

Yogi Surya Nugroho
09650001
Universitas Islam Negeri Sunan Kalijaga
Surel : giellua91@gmail.com

INTISARI

Forensik Jaringan atau biasa disebut *Network Forensic* adalah merupakan proses menangkap, mencatat, dan menganalisa aktivitas jaringan guna menemukan bukti digital (*Digital Evidence*) dari suatu serangan atau kejahatan yang dilakukan atau dijalankan menggunakan jaringan komputer. Contoh kejahatan yang menggunakan jaringan komputer adalah *Sniffing, Spoofing, DoS, DdoS, Phising, Carding,* serta *Malware.*

Penelitian ini merupakan penelitian *analisis* dimana tujuan penelitian ini untuk menginvestigasi dan menganalisa serangan *DdoS* dengan menggunakan Metode *Naïve Bayes* dengan cara mengumpulkan semua *log* data dan mengklasifikasikan waktu serangan. Digunakan metode *Naïve Bayes* dalam penelitian ini karena metode tersebut biasa digunakan untuk klasifikasi dokumen, deteksi spam atau *filtering spam*, dan masalah klasifikasi lainnya. Kegunaan dari penelitian ini adalah membantu orang-orang untuk menemukan bentuk serangan dari *Ddos Attacker.*

Hasil penelitian ini menunjukkan bahwa: (1) Penelitian ini telah berhasil mengklasifikasikan kecepatan dari serangan *DdoS* baik menggunakan TCP ataupun UDP. (2) Penelitian ini dapat menyimpulkan bahwa serangan *Ddos* menggunakan serangan TCP dan UDP dapat membuat kinerja server lebih berat dari biasanya karena server dikirimkan paket berulang kali. (3) Penelitian ini dapat menyimpulkan bahwa agar CPU dapat menyimpan *traffic log* yang akan digunakan sebagai barang bukti maka harus memiliki hardisk dengan kapasitas yang besar karena log yang tersimpan sangatlah besar.

Kata Kunci : DdoS, Investigation, *Naïve Bayes*, Network Forensics

NETWORK FORENSIC INVESTIGATION FROM *DDOS* HIJACKING USING *NAÏVE BAYES* METHOD

Yogi Surya Nugroho

09650001

Universitas Islam Negeri Sunan Kalijaga

Email: giellua91@gmail.com

ABSTRACT

Network Forensic is the process of catching, recording, and analyzing network activity that used for finding digital evidence from hijacking or crime using computer network. Various examples of crime using computer network are *Sniffing, Spoofing, DoS, DdoS, Phishing, Carding* and *Malware*.

This was a analytical research where the purpose of this research was for investigating and analyzing DdoS hijack by using *Naïve Bayes'* method. This research was done by collecting the entire data logs and classified the time of hijacking. *Naïve Bayes'* method was used because it famously used in classifying document, spam detection, or spam filtering, and many other classifications. The use of this research was for helping people in finding the form of hijacking from DdoS attacker.

The result from this research showed that: (1) This research has able to classify the speed of DdoS hijack from both TCP and UDP. (2) This research concluded that DdoS hijack using TCP and UDP can cause server overload. It was caused by server was sent many packages repeatedly. (3) This research also concluded that Traffic Log can be saved in CPU as a digital evidence, the Hard disk must be equipped with extra large capacity for saving the huge size of log.

Keywords: DdoS, Investigation, *Naïve Bayes*, Network Forensics

BAB I

PENDAHULUAN

1.1 Latar Belakang

Maraknya tindak kejahatan dan kriminalitas yang dilakukan saat ini secara langsung maupun tidak langsung banyak menggunakan teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon gengam, email, internet maupun website, secara luas telah mengundang berbagai pihak untuk melakukan tindak kejahatan dengan menggunakan teknologi elektronik dan digital. Seiring berjalannya waktu, lahirlah UU ITE pada tanggal 21 April 2008 yang bertujuan untuk mengatur transfer informasi elektronik agar berjalan sesuai dengan etika bertransaksi informasi elektronik. Oleh karena itu belakangan ini dikenal adanya ilmu"*computer forensics*" atau biasa dikenal forensik komputer. Forensik komputer adalah salah satu cabang ilmu dari forensik yang menangani segala macam kasus kejahatan dalam dunia IT. Dalam ilmu forensik komputer terdapat dua ilmu yaitu forensik digital dan forensik jaringan. Forensik digital adalah salah satu cabang ilmu forensik komputer yang berkaitan dengan pengumpulan bukti legal yang ditemui pada komputer dan media penyimpanan digital. Contoh dari kasus penyelidikan menggunakan forensik digital adalah kasus korupsi yang dilakukan pejabat dengan menyimpan data-data keuangan yang telah di korupsi dengan cara menyembunyikan data sehingga orang lain tidak bisa mengetahui isinya. Adapula forensik jaringan atau biasa disebut *Network Forensic* adalah merupakan proses menangkap, mencatat, dan menganalisa aktivitas jaringan guna menemukan bukti digital (*Digital Evidence*) dari suatu serangan atau

kejahatan yang dilakukan atau di jalankan menggunakan jaringan komputer. Contoh kejahatan yang menggunakan jaringan komputer adalah *Sniffing, Spoofing, DoS, DDoS, Phising, Carding,* serta *Malware.*

Denial of Service atau biasa disebut *dos* adalah salah satu serangan yang dilakukan melalui jaringan komputer. *Dos* merupakan jenis serangan terhadap sebuah komputer atau server didalam jaringan internet dengan cara menghabiskan sumber atau resource yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan baik dan benar, sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang di serang. *Distributed Denial of Service* adalah salah satu jenis serangan dari *Denial of Service* yang menggunakan banyak host penyerangan baik itu menggunakan komputer yang didedikasikan untuk melakukan penyerangan atau komputer yang dipaksa menjadi zombie untuk menyerang satu buah host target dalam sebuah jaringan. Dalam penelitian ini dilakukan investigasi terhadap *Distributed Denial of Service* karena banyak tindak kejahatan yang dilakukan untuk mematikan *server* atau membuat *server downtime*. Dalam serangan *Distributed Denial of Service* terdapat bermacam-macam jenis serangan seperti *Ping Flood, Ping of Death, Smurfing Attack, SYN Flood,* dan *Tear Drop*. Target dari serangan *Ddos* sendiri biasanya adalah *Routing Device, Web, Electronic Mail,* dan *Service Domain Name System.*

Kasus yang terjadi dan menjadi kasus terbesar dalam serangan *Distributed Denial of Service* yang dilakukan oleh Sven Olaf Kamphuis dengan melakukan serangan *DDoS* (300 Gigabits Data per Detik) terhadap perusahaan keamanan

jaringan Spamhaus. Di Indonesia sendiri serangan mematikan seperti *Distributed Denial of Service* terjadi 1,5 juta kali setiap hari. Biasanya serangan *Distributed Denial of Service* yang dilakukan di Indonesia sering diarahkan ke situs financial. Karena beberapa bank local di Indonesia menggunakan jaringan komputer dalam transaksi online.

Penelitian ini bertujuan untuk menginvestigasi, menganalisa, dan mengidentifikasi bentuk serangan *DDos* dengan menggunakan Metode *Naïve Bayes* dengan cara mengumpulkan semua *log* data dan mengklasifikasikan waktu serangan. Diharapkan penelitian ini dapat menjadi referensi mengenai langkah-langkah investigasi serangan *DDos.*

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, penulis dapat merumuskan permasalahan sebagai berikut :

1. Bagaimana menganalisa kecepatan dari serangan *Distributed Denial of Service.*
2. Bagaimana langkah-langkah investigasi forensik jaringan terhadap serangan *Distributed Denial of Service.*
3. Bagaimana memanfaatkan metode *Naïve Bayes* dalam analisa kecepatan serangan *Distributed Denial of Service.*

1.3 Batasan Masalah

Pada penelitian ini, penulis membatasi permasalahan sebagai berikut :

1. Serangan yang dilakukan hanya sebagai simulasi dengan menyerang *server* yang ada.
2. Serangan ini dilakukan dengan menggunakan 3 Skenario serangan yang berbeda antara lain: melakukan serangan dengan 1 *attacker*, 2 *attacker* dan 3 *attacker*.
3. Menganalisa kinerja *server* dalam menghadapi serangan dengan 2 skenario (selama pengukuran skenario 1 berlangsung dan selama pengukuran skenario 2 berlangsung).
4. Dalam mendapatkan *log traffic data* penulis hanya menggunakan software snort.
5. Dalam penelitiannya penulis menggunakan platform *Backtrack.*

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut :

1. Menemukan Ip yang melakukan serangan *Distributed Denial of Service.*
2. Melakukan analisa terhadap kecepatan serangan *Distributed Denial of Service*.
3. Menginvestigasi serangan *DdoS* dengan memanfaatkan metode *Naïve Bayes* untuk klasifikasi data-data yang ada.
4. Membandingkan antara serangan TCP dan UDP dengan menggunakan 3 skenario (1 *attacker, 2 attacker,* dan 3 *attacker*)
5. Membandingkan kinerja *server* dengan 2 skenario (selama pengukuran skenario 1 berlangsung dan selama pengukuran skenario 2 berlangsung).

1.5 Manfaat Penelitian

Sebagai bahan uji coba dan pembelajaran bagi penulis untuk menganalisa kecepatan serangan *DDoS* dengan memanfaatkan metode *Naïve Bayes* sehingga penulis dapat melakukan pencegahan sebelum terjadi serangan *DDoS*.

1.6 Keaslian Penelitian

Adapun keaslian dari penelitian ini sepengetahuan dari penulis belum adanya peneliti terdahulu yang melakukan penelitian berkaitan erat dengan investigasi forensik jaringan khususnya pada serangan *Ddos*. Selain itu penelitian yang berhubungan dengan forensik jaringan belum pernah dilakukan di Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang didapat setelah dilakukan penelitian adalah :

1. Bahwa ip penyerangan *DDoS* pada penelitian ini adalah 10.42.0.48, 10.42.0.85, serta 10.42.0.98.
2. Pada penelitian ini yang di cari adalah kecepatan serangan *DDoS* supaya dapat menangkal serangan *DDoS* sebelum terjadi serangan.
3. Digunakan Algorithma *Naïve Bayes* karena keunggulannya adalah untuk klasifikasi data yang ada.
4. Skenario pertama didapatkan kesimpulan dari tabel testing yang ada bahwa serangan TCP lebih cepat dibanding serangan UDP karena 2 dari 3 ujicoba serangan TCP mendapatkan waktu cepat 21 detik dan 34.970906 dan untuk 1 serangan memerlukan waktu 72.862579 detik sementara serangan UDP lebih lambat karena 1 diantara 3 ujicoba mendapatkan hasil cepat dengan durasi waktu 19.994434 detik dan 2 mendapatkan hasil lambat dengan waktu 38.87256 detik dan 70.160163 detik.
5. Skenario kedua didapatkan kesimpulan bahwa serangan UDP lebih cepat dibandingkan dengan serangan TCP karena 2 dari 3 ujicoba serangan UDP mendapatkan waktu cepat dengan durasi waktu 20.899021 detik dan 34.703955 detik, sementara untuk 1 serangan memerlukan waktu 69.32418 detik. Sementara untuk serangan TCP semua ujicoba dinyatakan lambat

dengan durasi waktu 23.595704 detik, 37.841365 detik dan 71.125064 detik

6. Skenario ketiga didapatkan kesimpulan bahwa serangan UDP lebih cepat dibandingkan dengan serangan TCP karena 3 dari ujicoba serangan UDP semua dinyatakan serangan cepat dengan durasi waktu 20.766546 detik, 35.81911 detik dan 73.699598 detik. Untuk serangan TCP 1 diantara 3 ujicoba dinyatakan serangan lambat dengan durasi 30 detik dan 2 serangan dinyatakan cepat dengan durasi 36.831271 detik dan 69.569092 detik.
7. Skenario keempat didapatkan kesimpulan bahwa serangan TCP lebih membuat kinerja laptop menjadi lebih berat karena untuk kinerja CPU 77.5% dan 29.3%, serta untuk kinerja memory sebesar 0.1% dan 0.5% dengan 2 Gigabytes memory hardisk untuk melakukan penyimpanan log.
8. Skenario kelima didapatkan kesimpulan bahwa serangan TCP dengan menggunakan 2 laptop lebih membuat kinerja laptop menjadi lebih berat dibanding dengan serangan UDP dengan menggunakan 2 laptop karena untuk kinerja CPU 73.0% dan 27.2%, serta untuk kinerja memory sebesar 0.1% dan 0.5% dengan 1 Gigabytes memory hardisk untuk melakukan penyimpanan log.

5.2 Saran

Penelitian *forensic network* ini tentunya masih memiliki kekurangan.. Saran untuk penelitian selanjutnya, perlu diperhatikan beberapa hal berikut :

1. Dapat digunakan rules-rules yang ada di Snort untuk menangkap segala serangan jadi analisa menjadi lebih gampang lagi.
2. Coba untuk melakukan serangan secara Live menggunakan Wireless sehingga dapat mengetahui peluang dari serangan DDoS secara langsung .
3. Penelitian selanjutnya dapat membuat aplikasi pemfilter spam untuk serangan DDoS.
4. Untuk penelitian berikutnya dapat menggunakan *Operating System* selain Linux/Unix untuk menangkap serangan jadi dapat membandingkan 2 kinerja *Operating System* berbeda. Dan dapat mengetahui kelebihan dan kelemahan dari *Operating System* Windows.

DAFTAR PUSTAKA

A. R. Arasteh, M. D. (2007). Analyzing Multiple Logs for Forensic Evidence. *Digital Investigation, Vol. 4S* , S82-S91.

Abatishchev. (2009, June 24). *LOIC* . Retrieved January 1, 2015, from SourceForge: http://sourceforge.net/projects/loic/

Backtrack. (2011). *Backtrack 5 R2 Released*. Retrieved Marc 10, 2015, from backtrack-linux: http://www.backtrack-linux.org/backtrack/backtrack-5-r2-released/

Backtrack. (2011, May 10). *Backtrack Linux*. Retrieved March 10, 2015, from backtrack-linux.org: http://www.backtrack-linux.org/

Berger, J.O. *Statistical Decision Theory and Bayesian Analysis 2nd with 23*

Bustami. *Penerapan Algoritma Naive Bayes Untuk Mengklasifikasi Data Nasabah Asuransi.*

Carier, B. D. (2006, June 07). Basic Digital Forensic Investigation Concepts. *Digital Evidence* .

Carrier, B. (2002). Defining Digital Forensic Examination and Analysis Tools. *International Journal of Digital Evidence* .

Casey, E. (2004). Network Traffic as a Source of Evidence : Tool Strengths, Weaknesses, and Future Needs. *Journal of Digital Investigation, Vol. 1, No. 1* , 28-43.

Casey, E. (2010). *Handbook of Digital Forensics and Investigation.* London: Elsevier Inc.

Herlambang, M. (2009). *Buku Putih Cracker : Kupas Tuntas DOS Attack + Cara Penanggulangannya.* Indonesia: Andi Publisher.

Herlambang, M. L. (2010). *Buku Putih Cracker*. Penerbit: Andi Publisher.

Hermawan, Rudi. 2012. *Analisis Konsep dan Cara Kerja Serangan Komputer Distributed Denial of Service(DDOS).* Skripsi Teknik Informatika Universitas Indrprasta PGRI: Jakarta

illustrations, Springer NY, 1985

Masdian. 2012. *Implementasi dan Analisa HIDS (Host Based Intrusion Detection System)Dengan Snort Untuk Mencegah DDOS(Distributed Denial of Service)*. Skripsi Teknik Informatika Universitas Trunojoyo: Bangkalan.

Meshram, K. K. (2012). Digital Forensics and Cyber Crime Datamining. *Journal of Information Security Vol. 3, No. 3* , 198.

Muhammad, Faris.2010. *Analisa Serangan DDOS Pada Server Ubuntu yang Beroperasi Dalam Wireless Local Area Network.* Skripsi Elektro dan Komunikasi Institut Teknologi Telkom : Bandung

Natalius, S. (2010). *Metode Naive Bayes Classifier dan Penggunanya pada Klasifikasi Dokumen.* Bandung: Program Studi Sistem dan Teknologi Informasi, Sekolah Teknik Elektro dan Informatika,Institut Teknologi Bandung.

Palmer, G. (2001). A Road Map for Digital Forensics Research. *First Digital Forensic Research* , 27-30.

Pribadi, M. (2009).*Melindungi Jaringan dari DDoS Menggunakan Linux + Mikrotik*. Penerbit: Andi Publisher.

Rafiudin, Rahmat. (2010). *Mengganyang Hacker dengan Snort*. Penerbit: Andi Publisher.

Sanfilippo, S. (2006). *Hping*. Retrieved May 29, 2015, from Hping: http://www.hping.org/

Sanmorino, Ahmad. 2013. *DDOS Attack Detection Simulation And Handling Mechanism.* Paper Komputer Sains Universitas Indonesia : Depok

Security, O. (2012, December 12). *Kali Linux Official Documentation*. Retrieved May 2015, 28, from Kali Linux: http://docs.kali.org/introduction/what-is-kali-linux

Security, O. (2012, December 12). *The Birth of Kali Linux*. Retrieved May 2015, 28, from Kali Linux: https://www.kali.org/news/birth-of-kali/

Seng, C. B. (2009). *Windows 7 Ultimate.* Jakarta: Jasakom.

Singh, O. (2009). *Network Forensics.* New Delhi, India: Indian Computer Response Team (CERT-In) Department of Information Technology.

Sulianta, F. (2008). *Komputer Forensik.* Jakarta: Elex Media Komputindo.

Zamrudiah, M. (2009). *Analisa Mekanisme Pertahanan DOS dan DDOS(Distributed Denial of Service) Pada Virtual Machine dengan Menggunakan IDS Center*. Jakarta: Universitas Indonesia.

LAMPIRAN

Data pengambilan untuk skenario keempat dan kelima dapat dilihat pada lampiran dibawah

Lampiran 1. TCP pengukuran Skenario 1

TCP pengukuran skenario 1

```
top - 15:44:59    up :1:14,  3 users,  load average: 0.81, 0.99, 1.07
Tasks: 150 total,   3 running, 147 sleeping,   0 stopped,   0 zombie
%Cpu(s): 17.7 us, 17.9 sy,  0.0 ni, 45.5 id,  0.6 wa,  0.4 hi, 18.0 si,  0.0 st
KiB Mem:   3041512 total,  2922068 used,   119444 free,   689456 buffers
KiB Swap:  1931260 total,    36136 used,  1895124 free,  1927976 cached
PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+ COMMAND
  3729 root      20   0  3592 2988 1888 R  77.5  0.1  42:51.29 mount.ntfs
  4266 root      20   0 29720  13m 6184 R  29.3  0.5  16:58.17 snort
  2622 root      20   0 69748  13m 8328 S   0.7  0.4   1:16.67 Xorg
     3 root      20   0     0    0    0 S   0.3  0.0   0:13.75 kssoftirqd/0
     7 root      20   0     0    0    0 S   0.3  0.0   0:13.09 rcu_sched
    13 root      20   0     0    0    0 S   0.3  0.0   0:16.52 kssoftirqd/1
  3388 root      20   0  178m  21m  16m S   0.3  0.7   0:12.64 gnome-terminal
  3783 root      20   0     0    0    0 S   0.3  0.0   0:06.03 kworker/1:1
  4321 root      20   0  4596 2120 1744 R   0.3  0.1   0:09.44 top
     1 root      20   0  2296 1372 1352 S   0.0  0.0   0:01.02 init
     2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
     5 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/0:0H
     8 root      20   0     0    0    0 S   0.0  0.0   0:00.00 rcu_bh
     9 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
    10 root      rt   0     0    0    0 S   0.0  0.0   0:00.04 watchdog/0
    11 root      rt   0     0    0    0 S   0.0  0.0   0:00.03 watchdog/1
    12 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/1
    15 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/1:0H
    16 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
    17 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
    18 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
    19 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 perf
    20 root      20   0     0    0    0 S   0.0  0.0   0:00.00 khungtaskd
    21 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 writeback
    22 root      25   5     0    0    0 S   0.0  0.0   0:00.00 ksmd
    23 root      39  19     0    0    0 S   0.0  0.0   0:00.00 khugepaged
```

32. 25 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 crypto
33. 26 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kintegrityd
34. 27 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 bioset
35. 28 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kblockd

29 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 devfreq_wq

Lampiran 2. UDP pengukuran Skenario 1

UDP pengukuran skenario 1

top - 02:17:41 up 5:28, 3 users, load average: 0.13, 0.15, 0.21

Tasks: 140 total, 2 running, 138 sleeping, 0 stopped, 0 zombie

%Cpu(s): 5.6 us, 2.0 sy, 0.0 ni, 90.9 id, 1.5 wa, 0.0 hi, 0.0 si, 0.0 st

KiB Mem: 3041512 total, 2870572 used, 170940 free, 224568 buffers

KiB Swap: 1931260 total, 29104 used, 1902156 free, 2028276 cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND

25169 root 20 0 29720 13m 6460 S 5.0 0.5 1:58.30 snort

2532 root 20 0 87620 20m 10m S 4.0 0.7 6:49.34 Xorg

5470 root 20 0 177m 24m 19m S 1.7 0.8 1:02.18 gnome-terminal

3270 root 20 0 258m 90m 24m S 1.0 3.0 0:39.95 gnome-panel

3261 root 20 0 130m 20m 15m S 0.7 0.7 0:14.39 metacity

3404 root 20 0 989m 254m 63m S 0.7 8.6 63:40.45 iceweasel

25418 root 20 0 192m 98m 75m S 0.7 3.3 0:03.93 soffice.bin

3232 root 20 0 228m 26m 20m S 0.3 0.9 0:10.58 gnome-settings-

3319 root 20 0 217m 44m 30m S 0.3 1.5 3:42.12 nautilus

25473 root 20 0 0 0 0 R 0.3 0.0 0:00.36 kworker/1:0

1 root 20 0 2296 1368 1340 S 0.0 0.0 0:01.15 init

2 root 20 0 0 0 0 S 0.0 0.0 0:00.00 kthreadd

3 root 20 0 0 0 0 S 0.0 0.0 0:02.37 ksoftirqd/0

5 root 0 -20 0 0 0 S 0.0 0.0 0:00.00 kworker/0:0H

7 root 20 0 0 0 0 S 0.0 0.0 0:11.93 rcu_sched

8 root 20 0 0 0 0 S 0.0 0.0 0:00.00 rcu_bh

Lampiran 3. TCP pengukuran Skenario 2

TCP pengukuran skenario 2

```
top - 17:43:05 up  3:30,  3 users,  load average: 0.53, 0.42, 0.37
Tasks: 164 total,   1 running, 163 sleeping,   0 stopped,   0 zombie
%Cpu(s): 26.5 us,  18.4 sy,  0.0 ni, 35.4 id,  0.7 wa,  0.02hi,  18.1 si,  0.0 st
KiB Mem:   3041512 total,  2893760 used,   147752 free,   617452 buffers
KiB Swap:  1931260 total,    158980 used,  1780288 free,  1757564 cached
  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
 7036 root      20   0  3080 1888 1492 S  73.0  0.1  30:23.86 mount.ntfs
 7199 root      20   0 29720  13m 6516 S  27.2  0.5   6:52.09 snort
 3860 root      20   0  860m 270m  71m S  16.9  9.1  19:40.36 iceweasel
 2537 root      20   0 82776  15m 9548 S   0.7  0.5   2:18.34 Xorg
 2463 root      20   0 28008 7696 7212 S   0.3  0.3   0:01.47 NetworkManager
 6966 root      20   0  178m  25m  19m S   0.3  0.8   0:07.18 gnome-terminal
 7294 root      20   0     0    0    0 S   0.3  0.0   0:01.29 kworker/0:0
    1 root      20   0  2296 1348 1324 S   0.0  0.0   0:01.07 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:01.70 ksoftirqd/0
    5 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0     0    0    0 S   0.0  0.0   0:05.40 rcu_sched
    8 root      20   0     0    0    0 S   0.0  0.0   0:00.01 rcu_bh
    9 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
   10 root      rt   0     0    0    0 S   0.0  0.0   0:00.05 watchdog/0
   11 root      rt   0     0    0    0 S   0.0  0.0   0:00.04 watchdog/1
   12 root      rt   0     0    0    0 S   0.0  0.0   0:00.02 migration/1
   13 root      20   0     0    0    0 S   0.0  0.0   0:02.72 ksoftirqd/1
   14 root      20   0     0    0    0 S   0.0  0.0   0:09.33 kworker/1:0
   15 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/1:0H
   16 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
   17 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
   18 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
```

```
 19 root      0 -20     0    0    0 S   0.0  0.0   0:00.00 perf
 20 root     20   0     0    0    0 S   0.0  0.0   0:00.00 khungtaskd
 21 root      0 -20     0    0    0 S   0.0  0.0   0:00.00 writeback
 22 root     25   5     0    0    0 S   0.0  0.0   0:00.00 ksmd
 23 root     39  19     0    0    0 S   0.0  0.0   0:00.00 khugepaged
 25 root      0 -20     0    0    0 S   0.0  0.0   0:00.00 crypto
 26 root      0 -20     0    0    0 S   0.0  0.0   0:00.00 kintegrityd
 27 root      0 -20     0    0    0 S   0.0  0.0   0:00.00 bioset
```

Lampiran 4. UDP pengukuran Skenario 2

UDP pengukuran skenario 2

```
top - 17:43:05 up  3:30,  3 users,  load average: 0.53, 0.42, 0.37
Tasks: 157 total,   1 running, 156 sleeping,   0 stopped,   0 zombie
%Cpu(s): 10.4 us,  5.7 sy,  0.0 ni, 81.9 id,  0.9 wa,  0.0 hi,  1.1 si,  0.0 st
KiB Mem:   3041512 total, 2910124 used,   131388 free,   569788 buffers
KiB Swap:  1931260 total,   30404 used, 1900856 free, 1752496 cached
  PID USER      PR  NI  VIRT  RES  SHR S  %CPU %MEM    TIME+  COMMAND
 7036 root      20   0  3080 1888 1492 S  23.9  0.1  13:23.86 mount.ntfs
 7199 root      20   0 29720  13m 6516 S  12.0  0.5   6:05.09 snort
 3860 root      20   0  860m 270m  71m S  10.0  9.1  19:40.36 iceweasel
 2537 root      20   0 82776  15m 9548 S   0.7  0.5   2:18.34 Xorg
 2463 root      20   0 28008 7696 7212 S   0.3  0.3   0:01.47 NetworkManager
 6966 root      20   0  178m  25m  19m S   0.3  0.8   0:07.18 gnome-terminal
 7294 root      20   0     0    0    0 S   0.3  0.0   0:01.29 kworker/0:0
    1 root      20   0  2296 1348 1324 S   0.0  0.0   0:01.07 init
    2 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kthreadd
    3 root      20   0     0    0    0 S   0.0  0.0   0:01.70 ksoftirqd/0
    5 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/0:0H
    7 root      20   0     0    0    0 S   0.0  0.0   0:05.40 rcu_sched
    8 root      20   0     0    0    0 S   0.0  0.0   0:00.01 rcu_bh
    9 root      rt   0     0    0    0 S   0.0  0.0   0:00.00 migration/0
   10 root      rt   0     0    0    0 S   0.0  0.0   0:00.05 watchdog/0
```

```
11 root      rt   0     0    0    0 S   0.0  0.0   0:00.04 watchdog/1
12 root      rt   0     0    0    0 S   0.0  0.0   0:00.02 migration/1
13 root      20   0     0    0    0 S   0.0  0.0   0:02.72 ksoftirqd/1
14 root      20   0     0    0    0 S   0.0  0.0   0:09.33 kworker/1:0
15 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kworker/1:0H
16 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 khelper
17 root      20   0     0    0    0 S   0.0  0.0   0:00.00 kdevtmpfs
18 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 netns
19 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 perf
20 root      20   0     0    0    0 S   0.0  0.0   0:00.00 khungtaskd
21 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 writeback
22 root      25   5     0    0    0 S   0.0  0.0   0:00.00 ksmd
23 root      39  19     0    0    0 S   0.0  0.0   0:00.00 khugepaged
25 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 crypto
26 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 kintegrityd
27 root       0 -20     0    0    0 S   0.0  0.0   0:00.00 bioset
```

DAFTAR RIWAYAT HIDUP

Nama	: Yogi Surya Nugroho
Tempat, tanggal lahir	: Sleman, 1 Maret 1991
Jenis Kelamin	: Laki-laki
Agama	: Islam
Alamat Asal	:Perumahan Nogotirto III Jalan Semeru C.142, Trihanggo, Gamping, Sleman, Yogyakarta
No. HP	: 082226323825
Email	: giellua91@gmail.com

Riwayat Pendidikan

1. SDN Petinggen II (1996-2002)
2. SMP Muhammadiyah 1 Yogyakarta (2002-2005)
3. SMA Muhammadiyah 3 Yogyakarta (2005-2008)
5. S1 Teknik Informatika UIN Sunan Kalijaga Yogyakarta (2009-2015)