PEMBUKTIAN *ANOMALY TRAFFIC* PADA GAME *COUNTER STRIKE: GLOBAL OFFENSIVE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

OLEH:

M. ANDRE SOFYAN

09011281520130

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA

2020

PEMBUKTIAN *ANOMALY TRAFFIC* PADA GAME *COUNTER STRIKE: GLOBAL OFFENSIVE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat Memperoleh
Gelar Sarjana Komputer

OLEH:

M. ANDRE SOFYAN

09011281520130

JURUSAN SISTEM KOMPUTER
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2020

LEMBAR PENGESAHAN

PEMBUKTIAN *ANOMALY TRAFFIC* PADA GAME *COUNTER STRIKE: GLOBAL OFFENSIVE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh:

M. ANDRE SOFYAN
09011281520130

Indralaya, 31 Desember 2020

Mengetahui,
Ketua Jurusan Sistem Komputer

Pembimbing

Dr. Ir. H. Sukemi, M.T.
NIP. 196612032006041001

Deris Stiawan, M. T., Ph. D.
NIP. 197806172006041002

HALAMAN PERSETUJUAN

Telah diuji dan lulus pada :

Hari : Kamis

Tanggal : 31 Desember 2020

Tim Penguji :

1. **Ketua : Rossi Passarella, M. Eng.**
2. **Anggota : Ahmad Heryanto, M. T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

Dr. Ir. H. Sukemi, M.T.

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama	: M. Andre Sofyan
NIM	: 090112815020130
Progam Studi	: Sistem Komputer
Judul Skripsi	: Pembuktian *Anomaly Traffic* pada Game *Counter Strike: Global Offensive* menggunakan Metode *Deep Packet Inspection*

Hasil Pengecekan Software *iThenticate/Turnitin* : 14%

Menyatakan bahwa laporan Skripsi yang telah saya buat merupakan hasil dari karya saya sendiri dan bukan hasil penjiplakan/*plagiat*. Apabila ditemukan unsur penjiplakan/*plagiat* didalam laporan skripsi ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian lah pernyataan ini saya buat dengan sebenar-benarnya dan tidak ada paksaan oleh siapapun.

Inderalaya, 31 Desember 2020

M. Andre Sofyan
NIM. 09011281520130

HALAMAN PERSEMBAHAN

Quote :

“Setiap orang pasti mempunyai waktunya masing-masing.”

Ini bukan tentang siapa yang duluan dan siapa yang belakangan, tetapi semua sudah ada yang mengatur semuanya sejak dari awal.

Dengan mengucapkan syukur Alhamdulillah atas Rahmat dan Karunia dari Allah Subhanahu Wa Ta’ala, Karya ini penulis persembahkan kepada :

- Kedua Orang tua saya yang saya cintai.
- Kakakku, drg. Sri Rahmawati.
- Keluarga besar Abdul Somad.
- Teman-teman seperjuangan Sistem Komputer 2015 dan juga khususnya kelas C.
- Dan semua teman-teman yang ada di lab COMNETS.

KATA PENGANTAR

Terima kasih atas kehadirat Allah Subahanhu Wa Ta' Ala atas segala rahmat dan Karunia yang telah di berikan sehingga dalam kesempatan kali ini penulis dapat menyelasaikan laporan Tugas Akhir yang diajukan untuk memperoleh gelar Sarjana (S1) Pada Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya dengan berjudul **"Pembuktian *Anomaly Traffic* pada Game *Counter Strike: Global Offensive* menggunakan Metode *Deep Packet Inspection*".**

Penulis berharap laporan ini nantinya kelak dapat bermanfaat bagi perkembangan ilmu pengetahuan, khususnya di dalam bidang teknologi informasi dan komunikasi yang akan bermanfaat bagi adik-adik tingkat yang nantinya akan mengerjakan tugas akhir juga.

Terima kasih penulis ucapkan kepada :

1. ALLAH Subhanahu Wa Ta'Ala, yang telah memberikan kesehatan dan kesempatan selama ini.
2. Kedua orang tua saya yang sangat saya cintai, dan juga kepada satu-satunya saudara kandung saya, drg. Sri Rahmawati yang selalu memberikan dukungan dalam bentuk moral, material, maupun spritiual.
3. Keluarga besar Abdul Somad, dan juga saudara saudara saya yang tidak bisa saya sebutkan satu persatu.
4. Pak Dr. Ir. H. Sukemi, M. T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
5. Pak Deris Stiawan, M. T., Ph. D. selaku Pembimbing Tugas Akhir yang telah memberikan dukungan, nasehat, dan kemudahan selama dalam masa perkuliahan dan juga dalam masa bimbingan selama ini.
6. Pak Ahmad Heryanto, M. T. selaku Pembimbing Akademik dan juga Penguji Sidang Tugas Akhir yang telah memberikan nasehat, kritikan, dan saran sehingga isi laporan dari Tugas Akhir ini menjadi lebih baik.

7. Seluruh Dosen Jurusan Sistem Komputer yang telah memberikan ilmu dan inspirasi selama masa perkuliahan.
8. Teman-teman Angkatan 2015, khususnya Kelas C.
9. Azwar Hidayat, S. Kom, M. Ilyastommy H. S., S. T. Alfiansyah, S. Kom, Nabillah Humairah, S. Kom. dan teman-teman lain yang tidak bisa saya sebutkan namanya satu persatu selaku ‘Guru’ penulis dalam menyelesaikan laporan tugas akhir ini.
10. Dan semua teman-teman yang ada di Lab COMNETS.

Dan pihak-pihak lain yang telah membantu penulis selama ini dalam menyelasikan studi di Jurusan Sistem Komputer dan mendapatkan gelar Sarjana di Universitas Sriwijaya.

Inderalaya, Desember 2020

Penulis

PEMBUKTIAN *ANOMALY TRAFFIC* PADA GAME *COUNTER STRIKE: GLOBAL OFFENSIVE* MENGGUNAKAN METODE *DEEP PACKET INSPECTION*

M. Andre Sofyan
Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : m.andresofyan@gmail.com

Abstrak

Counter-Strike merupakan permainan penembak dari sudut pandang orang pertama, game ini berbasis tim antara *Terrorists* dan *Counter-Terrorists* yang terdiri dari beberapa pemain didalamnya. *Counter-Strike: Global Offensive* adalah seri yang rilis keempat di seri *Counter-Strike* utama yang dikembangkan oleh Valve di 2012 dan seri ini adalah seri yang paling banyak dimainkan sampai saat ini diseluruh kalangan yang ada di dunia. Seiring berjalannya waktu pemain yang kalah banyak menggunakan cara yang tidak adil, seperti menggunakan program *cheat* atau injeksi *script*. Hal ini dilakukan untuk memenangkan suatu pertandingan dengan cara yang lebih mudah. Seperti contoh penggunaan program cheat untuk mengetahui posisi lawan, agar lebih mudah membunuhnya dan berbagai macam bentuk kecurangan lainnya. Pada penelitian ini, pengamatan dilakukan pada *traffic* yang ada pada *Counter Strike:Global Offensive* guna untuk menemukan *traffic* dan membuktikannya dengan menggunakan DPI (*Deep Packet Inspection*). DPI adalah salah satu cara untuk memeriksa paket yang ada didalam jaringan. Disini jenis DPI yang digunakan adalah String Matching, Algoritma pencarian untuk melakukan pencarian semua kemunculan string pendek dan dan panjang, untuk mendapatkan pola anomaly disini menggunakan 4 tahap yaitu, pembuatan dataset, feature extraction, pengenalan pola serangan, dan yang terakhir klasifikasi menggunakan string matching yang merupakan bagian dari DPI. Hasil yang didapatkan berupa serangan SYN Flood, yang mempunyai atribut TTL 56-128 dan checksum 30.000-60.000.

Kata Kunci : *Deep Packet Inspection*, *String Matching*, Serangan *SYN Flood*, *Counter-Strike*, *Counter Strike:Global Offensive*, MMOFPS.

PROOF OF ANOMALY TRAFFIC IN COUNTER STRIKE: GLOBAL OFFENSIVE GAME USING DEEP PACKET INSPECTION METHOD

M. Andre Sofyan
Departement of Computer Engineering, Faculty of Computer Science, Sriwijaya University
Email : m.andresofyan@gmail.com

Abstract

Counter-Strike is a first-person shooter game, based on a team between Terrorists and Counter-Terrorists consisting of several players inside. Counter-Strike: Global Offensive is the fourth major Counter-Strike series developed by Valve in 2012 and is the most played series to date worldwide. Over time, players who lose a lot use unfair means, such as using cheat programs or script injection. This is done to win a match in an easier way. Such as the use of cheat programs to find out the position of the opponent, to make it easier to kill him and various other forms of cheating. In this study, observations were made on traffic in Counter Strike:Global Offensive in order to find traffic and prove it by using DPI (Deep Packet Inspection). DPI is one way to check packages on the network. Here the type of DPI used is String Matching, a search algorithm to search for all occurrences of short and long strings, to get anomaly patterns here using 4 stages namely, dataset creation, feature extraction, attack pattern recognition, and the latter classification using matching strings that are part of DPI. The results obtained are SYN Flood attack, which has attribute TTL 56-128 and checksum 30.000-60.000.

Keywords : *Deep Packet Inspection, String Matching, SYN Flood Attack, Counter-Strike, Counter Strike:Global Offensive*, MMOFPS.

DAFTAR ISI

Halaman

Halaman Judul ……. i

Halaman Pengesahan …….. ii

Halaman Persetujuan ……...…….. iii

Halaman Pernyataan ……...……... iv

Halaman Persembahan …… v

Kata Pengantar ……...…… vi

Abstrak …….…… vii

Abstract ……... viii

Daftar isi …….…… x

Daftar Gambar …….…… xiv

Daftar Tabel …….…… xvi

BAB I. PENDAHULUAN

1.1. Latar Belakang ……..…….. 1

1.2. Tujuan ……..……... 3

1.3. Manfaat ……..…… 3

1.4. Perumusan Masalah dan Batasan Masalah ……..…….…….. 3

1.4.1. Perumusan Masalah ……..…….. 3

1.4.2. Batasan Masalaah …… 4

1.5. Metodologi Penulisan …… 4

1.6. Sistematik Penulisan ……... 5

BAB II. TINJAUAN PUSTAKA

2.1. Pendahuluan …… 7

2.2. *Online Game* ……... 7

2.3. *Genre Game* …… 8

2.3.1. *Game* Aksi(*Action Game*)...……... 8

2.3.2. *Game* Menembak(*Shooter Game*) …….…… 8

2.3.3. *Game* Aksi-Petualangan(*Action-Adventure Game)*……... 9

2.3.4. *Game* Petualangan(*Adventure Game*) ……... 9
2.3.5. *Game* Peran(*Role Playing Game*) ……..……..... 9
2.3.6. *Game* Simulasi(*Simulation Game*) ……..……..... 9
2.3.7. *Game* Strategi(*Strategy Game*) ……..……. 10
2.3.8. *Game* Olahraga (*Sport Game*) ……..…... 10
2.3.9. MMO (*Massively Multiplayer Online Game*) ……..... 10
2.3.9.1. MMORPG (*Massively Multiplayer Online Role-Playing Game*)…….…… 10
2.3.9.2. MMORTS (*Massively Multiplayer Online Real-Time Strategy*) ...…….……..……. 11
2.3.9.3. MMOFPS (*Massively Multiplayer Online First Person Shooter*) …….. 11
2.4. *Counter-Strike*
2.4.1. *Counter-Strike*(1994) ……...……... 12
2.4.2. *Counter-Strike: Condition Zero* (2004) ……... 12
2.4.3. *Counter-Strike: Source* (2004) ..…….. 13
2.4.4. *Counter-Strike Neo* (2004) …….. 13
2.4.5. *Counter-Strike Online* (2007) ……..... 13
2.4.6. *Counter-Strike: Global Offensive* (2012) …… 13
2.4.6.1. *Competitive Mode* …… 14
2.4.6.2. *Wingman* …….. 14
2.4.6.3. *Casual* …….. 14
2.4.6.4. *Deathmatch* ……..…. 14
2.4.6.5. *Arms Race* …… 15
2.4.6.6. *Demolition* …… 15
2.4.6.7. *Flying Scoutsman* ……. 15
2.4.7. *Counter-Strike Online* 2 (2013) ……... 15
2.4.8. *Counter-Strike Nexon: Zombies* (2014) ……... 16
2.5. TCP/IP …….. 16
2.5.1. *Link Layer* ……... 17
2.5.2. *Internet Layer* ……. 17
2.5.3. *Transport Layer* …….. 17

2.5.4. *Application Layer* 17
2.6. Arsitektrur *Server-Client* 18
2.7. TCP (*Transmission Control Protocol*) 18
2.8. UDP (*User Datagram Protocol*) 18
2.9. *Feature Extraction* 19
2.10. Snort 19
2.11. DPI (*Deep Packet Inspection*) 19
2.12. *String Matching* 20
2.13. SYN Flood 21

BAB III. METODOLOGI PENILITIAN
3.1. Pendahuluan 22
3.2. Kerangka Kerja Penilitian 22
3.3. Perancangan Sistem 24
3.3.1. Kebutuhan Perangkat Keras 24
3.3.2. Kebutuhan Perangkat Lunak 25
3.4. Skenario Pengambilan Dataset 25
3.5. *Data Extraction* 27
3.6. *Deep Packet Inspection* (DPI) 30
3.7. *String Matching* 30

BAB IV. HASIL DAN PEMBAHASAN
4.1. Pendahuluan 31
4.2. Analisa Dataset 31
4.2.1. Dataset Normal 35
4.2.2. Dataset Anomali/Serangan 35
4.3. Korelasi Data Hasil Data Extraction 36
4.4. Pengenalan Pola Anomaly Traffic didalam Game *Counter Strike: Global Offensive* 39

BAB V. KESIMPULAN DAN SARAN
5.1. Kesimpulan ……... 49
5.2. Saran ……. 50
DAFTAR PUSTAKA
LAMPIRAN

DAFTAR GAMBAR

Halaman

Gambar 2.1. Timeline Release Counter-Strike …….. 12
Gambar 2.2. Model Layer TCP/IP ……. 16
Gambar 3.1. Kerangka Kerja Tugas Akhir ……..... 23
Gambar 3.2. Topologi penelitian ……... 26
Gambar 3.4. *Flowchart* program *Data Extraction* ……. 29
Gambar 4.1. Statistik Total *Sniffer* Paket Data ……... 33
Gambar 4.2. Grafik perbandingan Jumlah Dataset …… 34
Gambar 4.3. Korelasi data hasil *Data Extraction* dengan *Raw Data* UDP …… 36
Gambar 4.4. Korelasi data hasil *Data Extraction* dengan *Raw Data* TCP ……. 37
Gambar 4.5. Tampilan user normal saat berada didalam lobby game …… 39
Gambar 4.6. TCP Stream di Lobby normal …… 40
Gambar 4.7. Tampilan saat Game normal …….. 40
Gambar 4.8. UDP Stream pada game normal ……..... 41
Gambar 4.9. Hasil Log Alert Snort dari data normal ……..… 41
Gambar 4.10. Tampilan saat user berada dilobby dengan program cheat …… 42
Gambar 4.11. TCP Stream saat di Lobby menggunakan cheat ……..... 43
Gambar 4.12. Tampilan saat berada didalam permainan menggunakan program cheat ……... 43
Gambar 4.13. Tampilan saat berada didalam permainan menggunakan program cheat ……... 44
Gambar 4.14. UDP Stream pada game anomaly …… 44
Gambar 4.15. Hasil Log Alert Snort dari data anomali …… 45
Gambar 4.16. Raw data *Anomaly Traffic* ……..… 46
Gambar 4.17. Program pencarian String Matching ……...… 47
Gambar 4.18. String Matching data Normal ……..…47
Gambar 4.19. String Matching data Anomali …….. 48

DAFTAR TABEL

Halaman

Tabel 1. Spesifikasi kebutuhan perangkat keras ……..….. 24
Tabel 2. Spesifikasi kebutuhan perangkat lunak ……..…. 25
Tabel 3. Skenario Pembuatan Dataset ……..…. 27
Tabel 4. Atribut *Data Extraction* ……..…. 28
Tabel 5. Dataset Hasil *Sniffing* ……..… 31
Tabel 6. Dataset Normal ……... 35
Tabel 7. Dataset Serangan ……..... 35
Tabel 8. Atribut Pola Serangan SYN Flood ……..… 48

DAFTAR LAMPIRAN

Lampiran 1. Koding *Data Extraction*

Lampiran 2. Program Pencarian *String Matching*

Lampiran 3. Berkas Revisi Tugas Akhir

Lampiran 4. Hasil Cek Plagiat

BAB I

PENDAHULUAN

1.1. Latar Belakang

Online game adalah video game yang dimainkan di dalam jaringan computer. *Online game* dapat membuat seseorang bermain Bersama, atau melawan satu sama lain dari 2 sampai ratusan ribu pemain [1]. Saat ini, salah satu genre dari game online yang sedang popular saat ini adalah First Shooter Person (FPS). Di dalam game yang menggunakan genre ini, memiliki unsur utama yaitu pertempuran yang menggunakan senjata api. FPS dimainkan dengan menggunakan perspektif sebagai orang pertama untuk memberikan sensasi yang nyata seolah-olah pemain berada langsung didalam pertempuran tersebut. Dibutuhkannya refleks cepat dalam hal gerakan untuk membidik dan menembak musuh.

Salah satu game online yang ber-*genre* First Shooter Person yang sempat popular di Indonesia ialah Counter Strike:Global Offensive. Permainan ini didesain layak adanya pertempuran antara Teroris dengan Counter Teroris di suatu tempat yang sudah dirancang dimana misi dari tim Teroris mencoba untuk meledakkan suatu area menggunakan bom yang dilindungi oleh Counter Teroris atau membunuh semua Counter Teroris untuk memperoleh kemenangan disetiap ronde, kebalikan dari Teroris, Counter Teroris mempunyai misi untuk mencegah dan menghalangi peledakkan yang akan dilakukan Teroris atau membunuh semua Teroris. Selama game berjalan salah satu tim harus memenangkan 16 babak, dari 30 babak yang ada. Karena game ini menggunakan senjata, maka dari itu senjata didapatkan dari pembelian ditoko yang ada dimarkas masing-masing. Uang yang digunakan didapatkan dari setiap assist, kill, dan death yang terjadi selama game berjalan [2].

Seiring berjalannya waktu pemain yang kalah banyak menggunakan cara yang tidak adil, seperti menggunakan program cheat atau injeksi script. Hal ini dilakukan untuk memenangkan suatu pertandingan dengan cara yang lebih mudah.

Seperti contoh penggunaan program cheat untuk mengetahui posisi lawan, agar lebih mudah membunuhnya, mendapatkan uang yang lebih banyak untuk membeli senjata yang kuat, bahkan sampai ada yang tidak masuk diakal seperti membunuh dengan satu kali tembakan, peluru yang langsung mengenai tanpa harus membidik kesasaran dan peluru yang bias menembus di setiap dinding yang ada pada game tersebut.

Deep Packet Inspection (DPI) adalah suatu cara untuk memeriksa suatu aliran paket data di dalam sebuah jaringan. Bahkan, *Deep Packet Inspection* (DPI) mampu secara akurat mengklasifikasikan dan mengkontrol lalulintas di dalam aplikasi dan konten dengan kata lain DPI dapat menganalisa paket konten dan menawarkan pemrosesan konten[3].

Pada penelitian [4], Pada game Fortnite Battle Royale, jaringan dari client dan client yang lain dimana bertemu dalam suatu area tertentu dianalisa setiap perilakunya. Berdasarkan data analisa jaringan dan gerakan pemain yang dihasilkan, jejak jaringan dapat di ekstrapolasi untuk semua pemain yang berada digame tersebut.

Pada Penelitian [5], membahas tentang pengenalan pola pada game Dragon Nest yang ber-genre MMORPG. Penelitian tersebut dilakukan dengan cara menganalisa dan menemukan pola pada traffic game tersebut, menganalisa user behavior, lalu memvisualisasikan data yang di dapat dalam bentuk grafik yang menggunakan metode Bloom Filter.

Pada penelitian berikutnya [6], menyajikan pendekatan baru untuk mengklasifikasikan traffic jaringan di dalam game, yang menggunakan *protocol filtering* dan *IP filtering* untuk *pre-processing* menta untuk mengurangi gangguan.

Pada penelitian berikutnya [7], telah melakukan penelitian dengan menggunakan metode deep packet inspection (DPI) untuk mendeteksi private data exfiltration di dalam platform-independent. Penelitian telah menunjukkan keefektifan tools ini dalam mendeteksi exfiltration data yang disebabkan oleh aplikasi yg jahat, yang dapat digunakan oleh user untuk membantu mendeteksi exfiltrasi data lebih awal, di berbagai platform.

Dari penilitian yang telah dikemukakan diatas, penulis akan melakukan pembuktian pola traffic anomaly dan normal pada game Counter Strike: Global Offensive menggunakan Deep packet inspection (DPI).

1.2. Tujuan

Adapun tujuan dari penelitian ini adalah :

1. Menggunakan Deep packet Inspection (DPI) untuk mendapatkan paket data.
2. Menggunakan *feature extraction* untuk membongkar paket data yg di dapat.
3. Menganalisa perbedaan pola paket data traffic anomaly dan normal yang terjadi dalam game.

1.3. Manfaat

Adapun manfaat yang dapat di ambil dari penelitian ini adalah:

1. Mampu menjelaskan pola traffic anomaly dan normal yang terjadi di dalam game Counter Strike: Global Offensive
2. Mampu menvisualkan paket data yang di dapat menggunakan Bloom Filter.

1.4. Perumusan dan Batasan masalah

Berdasarkan latar belakang yang telah di jelaskan, maka rumusan dan Batasan masalah yang ada pada penelitian ini adalah :

1.4.1. Perumusan Masalah

1. Pemahaman tentang Deep Packet Inspection mengklarifikasi pola traffic anomaly dan normal di dalam game Counter Strike: Global Offensive
2. Bagaimana hasil traffic anomaly pada penggunaan metode string matching.

1.4.2. Batasan Masalah

1. Hanya melakukan pengenalan pola traffic anomaly dan normal menggunakan game Counter Strike: Global Offensive.
2. Data yang di ambil dalam penilitian ini berupa hanya traffic game Counter Strike: Global Offensive.
3. Data yang diambil menggunakan Deep packet inspection.
4. Data yang sudah di dapat akan di filter menggunakan metode string matching
5. Tidak membahas keamanan yang ada di dalam game Counter Strike: Global Offensive.
6. Data yang di visualkan tidak dilakukan secara real-time.

1.5. Metodologi Penulisan

Metodologi yang digunakan dalam penulisan tugas akhir ini, akan melewati beberapa tahapan sebagai berikut:

1. Tahap Pertama (Perumusan Masalah)

   Tahap ini menentukan permasalahan yang relevan dan dapat dijadikan penelitian yaitu bagaimana menemukan pola yang ada di dalam suatu trafik dan kemudian memvisualkan informasi yang didapat.

2. Tahap Kedua (Study Pustaka)

   Tahap ini ialah tahap mencari referensi atau literature ilmiah yang berhubu ngan dengan judul tugas akhir untuk menunjang penelitian yang dilakukan.

3. Tahap Ketiga (Perancangan)

   Tahap ini adalah tahap perancangan sistem yang akan dibuat sesuai dengan rumusan masalah penelitian. Dalam tahap ini melakukan instalasi software pendukung untuk penelitian, membuat topologi, dan menerapkan metode yang akan digunakan.

4. Tahap Keempat (Pengujian)

   Tahap ini ialah tahap pengujian dari system yang telah di rancang. Mengambil data, membongkar data yang di dapat

menggunakan *feature extraction* dan kemudian memvisualkannya.

5. Tahap Kelima (Analisis)

   Tahap ini adalah tahap analisa dari hasil pengujian. Disini akan dianalisa bagaimana mengenali pola trafik perbandingan yang didapat dari game Counter Strike-Global Offensive yang menggunakan Cheat dengan tidak menggunakan cheat(anomaly dan normal).

6. Kesimpulan Dan Saran

   Pada tahap ini ditarik kesimpulan dari hasil analisa penelitian dan dibuat saran sebagai referensi apabila penelitian ini dapat dilanjutkan.

1.6. Sistematik Penulisan

Berikut ini adalah sistematik penulisan yang digunakan untuk memperjelas dan mempermuda penyusunan tugas akhir pada laporan ini :

BAB I PENDAHULUAN

Pada bab ini menjelaskan secara sistematik mengenai topik yang di ambil.

BAB II TINJAUAN PUSTAKA

Pada bab ini berisi semua penjelasan tentang komponen – komponen hardware-software yang digunakan, untuk mendapatkan data, dan penjelasan tentang metodologi Bloom Filter sebagai landasan untuk memvisualkan data yang di dapat.

BAB III METODOLOGI PENELITIAN

Pada bab ini menjelaskan secara sistematis mengenai langkah- langkah yang digunakan untuk mencari, mengumpulkan, dan menganalisa tema dalam penulisan tugas akhir.

BAB IV PENGUJIAN DAN ANALISA

Pada bab ini dilakukan pengujian dan analisa data yang didapat dari hasil pengujian yang dilakukan

BAB V KESIMPULAN

Pada bab ini memberikan kesimpulan dari pengujian dan Analisa data yang dilakukan, dan memberikan saran untuk penelitan lanjutan.

DAFTAR PUSTAKA

[1] E. Adams, "*Fundamentals of Game Design"*. 2013.

[2] J. Jansz, M. Tanis, "Appeal of Playing Online First Person Shooter Games" Vol 10. 2007.

[3] J. Svoboda,"Network Traffic Analysis with Deep Packet Inspection Method," 2014.

[4] J. S. Komputer, F. I. Komputer, and U. Sriwijaya, "Visualisasi dan Pengenalan Pola Trafik Game Apex Legends menggunakan metode K-Means," 2019.

[5] J. S. Komputer, F. I. Komputer, and U. Sriwijaya, "Pengenalan Pola Behavior Game Dragon Nest Menggunakan Metode Bloom Filter," 2017.

[6] J. Yan, B. Randell, "A Systematic Classification of Cheating in Online Games", 2005.

[7] S. Dharmapurikar, P. Krishnamurthy, T.S. Sproull, and J. W. Lockwood, "Deep Packet Inspection Methods," IEEE Micro, Vol. 24, no. 1, pp.52-64, 2004.

[8] X. Che and B. Ip, "Packet level traffic analysis of online games from the genres characteristics perspective," J. Netw. Comp. Appl., vol. 35, no.1, pp. 239-253, 2012.

[9] Steamcommunity.com, "The history of Counter Strike" 2012. [Online], Available at: http://steamcommunity.com/sharedfiles/filesdetails/?id=1455534283. [Accessed at: 18 Oktober 2020].

[10] Snort.org, “Rule Documentation Sid 1-402 Protocol ICMP”, 2005 [Online], Available at: https://www.snort.org/rule_docs/1-402. [Accessed at: 27 Oktober 2020].

[11] Snort.org, “Rule Documentation Sid 1-8081 INDICATOR SCAN UPnP”, 2007 [Online], Available at: https://www.snort.org/rule_docs/1-8081. [Accessed at: 27 Oktober 2020].

[12] C. Xu, S. Chen, J. Su, S. M. Yiu, and L. C. K. Hui, ―A Survey on Regular Expression Matching for Deep Packet Inspection : Applications, Algorithms and Hardware platforms,‖ vol. 13, no. 9, 2016.