Sistem Pencegahan Serangan SQL Injection Pada Platform Pembelajaran Online Menggunakan Metode Bayesian Network

OLEH :

Juan Alkasar

09011281520092

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

Sistem Pencegahan Serangan SQL Injection Pada Platform Pembelajaran Online Menggunakan Metode Bayesian Network

PROPOSAL TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

OLEH :

JUAN ALKASAR

09011281520092

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2020

LEMBAR PENGESAHAN

Sistem Pencegahan Serangan SQL Injection Pada Web *Penetration Testing Damn Vulnerable Web Attack* DVWA Menggunakan Metode Bayesian Network

TUGAS AKHIR

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

JUAN ALKASAR
09011281520092

Indralaya, 31 Desember 2020

Mengetahui,
Ketua Jurusan Sistem Komputer

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

Pembimbing Tugas Akhir

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 : Kemahyanto Exaudi, M.T.**
2. **Sekretaris : Rendyansyah, S.Kom., M.T.**
3. **Anggota : Ahmad Heryanto, M.T.**

Mengetahui,

Ketua Jurusan Sistem Komputer

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

NIP. 196612032006041001

iii

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	: Juan Alkasar
NIM	: 09011281520092
Program Studi	: Sistem Komputer
Judul	: Sistem Pencegahan Serangan SQL Injection Pada Web Penetration Testing Damn Vulnerable Web Attack DVWA Menggunakan Metode Bayesian Network

Menyatakan bahwa laporan Tugas Akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan atau plagiat. Apabila ditemukan unsur penjiplakan atau plagiat dalam laporan Tugas Akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya. Demikian, pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan.

Palembang, Desember 2020

Juan Alkasar

iv

HALAMAN PERSEMBAHAN

“No matter how hard a stone will be crushed by water, No matter how hard the problem will be solved with effort and hard work accompanied by sincerity”

Tugas akhir ini saya persembahkan untuk :

- ***Kedua Orang tua dan Adik – adik saya***

  Dosen Pembimbing dan Penguji
- ***Sahabat – sahabat saya***
- **Teman Seperjuangan Sistem Komputer 2015**

Almamaterku

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Puji dan syukur saya panjatkan atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga saya dapat menyelesaikan penyusunan Proposal tugas akhir ini dengan judul "Sistem Pencegahan Serangan SQL Injection Pada Platform Pembelajaran Online Menggunakan Metode Bayesian Network .

Shalawat dan salam tak lupa kita junjungkan kepada Nabi kita Rasulullah SAW beserta keluarga, sahabat dan para pengikutnya hingga akhir zaman.

Pada penyusunan proposal ini, saya menyampaikan banyak ucapan terima kasih kepada semua pihak yang telah memberikan segala kemudahan serta dukungan, semangat, pengarahan, dorongan, bantuan, bimbingan, ide dan saran berupa nasehat baik moril maupun materil selama penyusunan Proposal tugas akhir ini. Untuk itu saya mengucapkan banyak terimakasih kepada :

1. Allah SWT yang telah memberikan kesehatan kepada penulis sehingga penulis dapat menyelesaikan Proposal tugas akhir ini dengan tepat waktu.
2. Kedua orang tua serta keluarga yang telah memberikan dukungan dan doa untuk kelancaran pengerjaan Proposal tugas akhir ini.
3. Bapak Jaidan Jauhari, S.Pd., M.T., selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Bapak Dr. Ir. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Universitas Sriwijaya.
5. Dosen Pembimbing Akademik Bapak Sutarno, S.T., M.T.
6. Bapak Deris Stiawan, M.T., Ph.D. selaku pembimbing tugas akhir di jurusan Sistem Komputer.
7. Seluruh teman-teman angkatan 2015 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
8. Seluruh teman-teman angkatan 2015 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
9. TIM TA, M.Afria Alim Saputra dan Rizky Soufi Gustiawan yang saling memberikan dukungan dan semangat dan waktunya yang sangat berarti untuk diingat

10. TIM TA, M.Afria Alim Saputra dan Rizky Soufi Gustiawan yang saling memberikan dukungan dan semangat dan waktunya yang sangat berarti untuk diingat
11. Mbak Winda Kurnia Sari, sebagai Admin Jurusan yang ikut berperan penting dalam mengurus berkas sidang.
12. Teman teman seperjuangan Dimas Rangga Nugraha, Adhe Eka Prasetya, Ridholahi, Bagus Trismadani, Anjar, Tomo, Wawan, Hadi, Herdi, Elul dan berapa orang lagi yang tidak bisa saya sebut kan namanya satu persatu

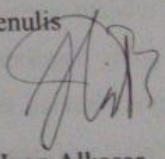
saya menyadari bahwa masih banyak kekurangan dalam pembuatan laporan ini dan masih jauh dari kesempurnaan. Mengingat kurangnya pengetahuan dan pengalaman penulis. Untuk itu segala kritik dan saran, sangatlah penting bagi penulis.

Semoga tugas akhir ini bisa bermanfaat bagi pembaca ataupun bagi penulis sendiri. Demikian yang bisa penulis sampaikan.

Wassalamu'alaikum Wr. Wb.

Indralaya, 31 Desember 2020

Penulis



Juan Alkasar

vii

Sistem Pencegahan Serangan SQL Injection Pada Web *Penetration Testing Damn Vulnerable Web Attack* DVWA Menggunakan Metode Bayesian Network

Juan Alkasar (0901281520092)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya
Email : juan.alkasar123@gmail.com

ABSTRAK

Intrusion Prevention System (IPS) adalah perkembangan dari *Intrusion Detection System* dimana suatu sistem (*hardware*, *software*, maupun kombinasi *hardware* dan *software*) yang memiliki kemampuan untuk memonitor jaringan dan melakukan tindakan pencegahan dari aktivitas mencurigakan di dalam jaringan. *Bayesian Network* adalah salah satu *machine learning* yang memanfaatkan hubungan probabilitas antara suatu variabel dengan variabel lain. Metode *bayesian network* dapat digunakan untuk mendeteksi paket serangan SQL *Injection* melalui URI pada HTTP *Request.* SQL *Injection* merupakan teknik serangan yang memanfaatkan celah keamanan pada sebuah aplikasi web. Target *server* yang digunakan dalam melakukan penelitian adalah DVWA yang memiliki celah keamanan *database.* Pada penerapan metode *Bayesian Network* terhadap pola serangan SQL *Injection* dapat dibagi menjadi dua, yaitu pola serangan *Character Query* dan pola serangan *Percent Encoding.*

Kata Kunci : *Intrusion Prevention System* (IPS) SQL *Injection*, *Bayesian Network*, URI, HTTP *Request*

SQL Injection Attack Prevention System On Web Penetration Testing Damn Vulnerable Web Attack DVWA Using Bayesian Network Method

Juan Alkasar (0901281520092)

Dept of Computer Engineering, Faculty of Computer Science,
Sriwijaya University
Email : juan.alkasar123@gmail.com

Abstract

Intrusion Prevention System (IPS) is a development of Intrusion Detection System where a system (hardware, software, or a combination of hardware and software) that has the ability to monitor the network and take precautions from suspicious activity in the network. Bayesian Network is one of the machine learning that utilizes the probability relationship between a variable and another variable. Bayesian network method can be used to detect SQL Injection attack package via URI in HTTP Request. SQL Injection is an attack technique that exploits security gaps in a web application. The target server used in conducting the research is the DVWA which has a database security loophole. In the application of Bayesian Network method to SQL Injection attack pattern can be divided into two, namely Character Query attack pattern and Percent Encoding attack pattern.

Keywords: Intrusion Prevention System (IPS) SQL Injection, Bayesian Network, URI, HTTP Request

DAFTAR ISI

Halaman

HALAMAN JUDUL i

HALAMAN PENGESAHAN.....ii

KATA PENGANTAR iii

ABSTRAK v

DAFTAR ISI vi

DAFTAR GAMBAR.....ix

DAFTAR TABEL.....xi

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Tujuan 2

1.3 Manfaat 3

1.4 Rumusan Masalah 3

1.5 Batasan Masalah.....3

1.6 Metodologi Penelitian 4

1.7 Sistematika Penelitian 6

BAB II TINJAUAN PUSTAKA

2.1 Penelitian Sebelumnya.....7

2.2 Forensik Digital.....7

2.3 Klasifikasi Forensik Digital 8

2.3.1 Forensik Komputer.....8

2.3.2 Forensik Mobile 8

2.3.3 Forensik Audio 8

2.3.4 Forensik Video 8

2.3.5 Forensik Gambar 8

2.3.6 Forensik Jaringan 8

2.4 Klasifikasi Barang Bukti 8

2.4.1 Barang Bukti Elektronik.....8

2.4.2 Barang Bukti Digital 9

2.5 NTFS 9

2.6 Timestamp.....10

2.7 PDF 10

2.8 Metadata.....11

2.9 Hexadecimal.....11

2.10 Algoritma String Matching 12

BAB III METODOLOGI PENELITIAN

3.1 Pendahuluan 21

3.2 Kerangka Kerja Penelitian 21

3.3 Perancangan Sistem 23

3.3.1 Kebutuhan Perangkat Keras (*Hardware*) 23

3.3.2 Kebutuhan Perangkat Lunak (*Software*) 23

3.3.3 Pembuatan *Dataset* 24

3.3.3.1 Pembuatan *Dataset* .PDF 16

3.4 Pengecekan *Timestamp* 16

3.5 Manipulasi *Timestamp* 17

3.6 Menampilkan Metadata *File* 18

3.7 Langkah Pengujian 19

3.8 Analisa Forensik *File Timestamp Manual* 22

3.9 Hasil dan Analisis 22

BAB IV HASIL DAN ANALISA

4.1 Pendahuluan 23

4.2 Hasil Pembuatan *Dataset* 23

4.2.1 Dokumen *File* .PDF 27

4.2.1.1 *Timestamp* Data .PDF 26

4.3 Menampilkan Metadata *Dataset* 29

4.4.2 Metadata Data .PDF 29

4.4 Hasil Pemalsuan *Timestamp* Data .PDF Kondisi Waktu Maju 34

4.5 Hasil Pemalsuan *Timestamp* Data .PDF Kondisi Waktu Mundur 39

BAB V KESIMPULAN DAN SARAN SEMENTARA

5.1 Kesimpulan 44

5.2 Saran 45

DAFTAR PUSTAKA 46

DAFTAR GAMBAR

Halaman

Gambar 1.1 Diagram Air Metodologi Penelitian 5

Gambar 2.1 Struktur NTFS 10

Gambar 3.1 Kerangka Kerja Penelitian 14

Gambar 3.2 Perintah Menampilkan *Timestamp* 17

Gambar 3.3 Manipulasi *Timestamp* dengan tools *Attribute Magic* 17

Gambar 3.4 Instalasi Hexeditor 18

Gambar 3.5 Menampilkan Metadata *File* 19

Gambar 3.6 *Flowchart* Langkah Pengujian 21

Gambar 4.1 Dokumen data1.pdf 24

Gambar 4.2 Dokumen data2.pdf 24

Gambar 4.3 Dokumen data3.pdf 25

Gambar 4.4 Dokumen data4.pdf 25

Gambar 4.5 Dokumen data5.pdf 26

Gambar 4.6 *Timestamp* data1.pdf 26

Gambar 4.7 *Timestamp* data2.pdf 27

Gambar 4.8 *Timestamp* data3.pdf 27

Gambar 4.9 *Timestamp* data4.pdf 28

Gambar 4.10 *Timestamp* data5.pdf 28

Gambar 4.11 Metadata data1.pdf 29

Gambar 4.12 Metadata data2.pdf 30

Gambar 4.13 Metadata data3.pdf 31

Gambar 4.14 Metadata data4.pdf 32

Gambar 4.15 Metadata data5.pdf 33
Gambar 4.16 Pemalsuan *Timestamp* data1.pdf 34
Gambar 4.17 Hasil Pemalsuan *Timestamp* data1.pdf 34
Gambar 4.18 Pemalsuan *Timestamp* data2.pdf 35
Gambar 4.19 Hasil Pemalsuan *Timestamp* data2.pdf 35
Gambar 4.20 Pemalsuan *Timestamp* data3.pdf 36
Gambar 4.21 Hasil Pemalsuan *Timestamp* data3.pdf 36
Gambar 4.22 Pemalsuan *Timestamp* data4.pdf 37
Gambar 4.23 Hasil Pemalsuan *Timestamp* data4.pdf 37
Gambar 4.24 Pemalsuan *Timestamp* data5.pdf 38
Gambar 4.25 Hasil Pemalsuan *Timestamp* data5.pdf 38
Gambar 4.26 Pemalsuan *Timestamp* data1.pdf 39
Gambar 4.27 Hasil Pemalsuan *Timestamp* data1.pdf 39
Gambar 4.28 Pemalsuan *Timestamp* data2.pdf 40
Gambar 4.29 Hasil Pemalsuan *Timestamp* data2.pdf 40
Gambar 4.30 Pemalsuan *Timestamp* data3.pdf 41
Gambar 4.31 Hasil Pemalsuan *Timestamp* data3.pdf 41
Gambar 4.32 Pemalsuan *Timestamp* data4.pdf 42
Gambar 4.33 Hasil Pemalsuan *Timestamp* data4.pdf 42
Gambar 4.34 Pemalsuan *Timestamp* data5.pdf 43
Gambar 4.35 Hasil Pemalsuan *Timestamp* data5.pdf 43

DAFTAR TABEL

Halaman

Tabel 2.1 Tabel Perbandingan Hexadesimal 11

Tabel 3.1 Spesifikasi Kebutuhan Perangkat Keras..... 15

Tabel 3.2 Kebutuhan Perangkat Lunak 16

BAB I. PENDAHULUAN

I. LATAR BELAKANG

Intrusion Prevention System (IPS) adalah perkembangan dari *Intrusion Detection System* dimana suatu sistem (*hardware, software*, maupun kombinasi *hardware* dan *software*) yang memiliki kemampuan untuk memonitor jaringan dan melakukan tindakan pencegahan dari aktivitas mencurigakan di dalam jaringan. Banyaknya aktivitas serangan yang terjadi sebelumnya membuat beberapa serangan yang terdeteksi, hanya menghasilkan sebuah serangan palsu dan tidak terdeteksi pada sistem akan tetapi tetap mengganggu lalulintas jaringan yang normal[11]. Penelitian ini tidak hanya ditujukan pada bagian teknis saja tetapi juga bisa digunakan untuk melindungi sistem keamanan pada website Pemerintah seperti Pendidikan, Militer, Kesehatan, Bank dan bidang-bidang yang lainnya untuk melindungi informasi-informasi penting didalamnya dan mencegah bentuk serangan yang datang walaupun itu berupa ancaman ataupun serangan langsung yang akan mengganggu kestabilan jaringan yang kita lindungi.

Menurut penulis[15] terdapat sebuah kekurangan pada saat melakukan monitoring sistem keamanan yang terbagi menjadi dua yaitu cara mendeteksi serangan dan melakukan tindakan apabila terjadi serangan pada jaringan. keamanan sangat dibutuhkan agar server dalam kondisi yang baik. Jika dalam kondisi yang kurang baik serangan dapat dengan mudah masuk dan menyerang jaringan komputer, jika pada jaringan komputer tersebut tidak terdapat sistem keamanan untuk mengatasi serangan yang masuk.

Penelitian sebelumnya [6] yaitu Intrusion Detection System (IDS) menggunakan *Metode Bayesian Network* menjelaskan bahwa sistem deteksi yang digunakan bisa mendeteksi serangan *SQL Injecton* dengan cara pengenalan *Payload* HTTP berupa HTTP Request pada bagian URI. Dengan penerapan *Bayesian Network, SQL Injection* dapat dideteksi dan dikelompokkan berdasarkan *query* yang digunakan. Cara kerjanya dengan mendeteksi serangan *query SQL Injection* menggunakan *Wireshark*, karena masih terdapat beberapa serangan yang tidak dianggap serangan oleh sistem deteksi yang tetap mengganggu jaringan, karena itulah penulis bertujuan menerapkan *Intrusion Prevention System* (IPS) sebagai sistem pencegahan pada penelitian ini.

Terdapat dua bentuk dari IPS, yaitu *Network Based Intrusion Prevention System* (NIPS) dan *Host Based Intrusion Prevention System* (HIPS). NIPS digunakan untuk memantau aliran data yang keluar masuk jaringan dan biasanya diletakkan di depan atau dibelakang *router, firewall*, maupun VPN *gateway*. Sedangkan HIPS merupakan jenis

IPS yang dipasang pada host untuk memantau aliran data yang terjadi pada host tersebut. Untuk mendeteksi dan mencegah usaha serangan ke dalam jaringan atau host, IPS menggunakan beberapa metode yaitu, *signature matching, protocol analysis, dan anomaly detection.*

Pada penelitian [7] *Snort* adalah alat deteksi intrusi ringan yang mencatat paket yang datang melalui jaringan dan menganalisis paket. Snort memeriksa paket yang melanggar aturan yang ditulis oleh pengguna dan menghasilkan peringatan jika ada kecocokan yang ditemukan. Snort juga memungkinkan untuk membantu membuat sistem pencegahan secara realtime (IPS) karena Snort bisa mengenali pola serangan secara *real-time* berdasarkan aturan yang ditulis oleh pengguna dalam file teks yang dihubungkan dengan file *snort.conf* di mana semua konfigurasi snort disebutkan. Ada beberapa perintah yang digunakan untuk menjalankan Snort sehingga dapat menganalisis perilaku jaringan.Snort juga memiliki arsitektur yang modular yang memungkinkan *Intrusion Detection System* IDS ini dapat di *enhanced* penggunaannya.

Menurut [12] Dalam melakukan deteksi serangan, terdapat dua teknik deteksi yang digunakan yaitu *misuse detection* dan *anomaly detection*. *Misuse detection* merupakan suatu teknik deteksi serangan yang telah diketahui oleh sistem dengan melakukan pencocokan data yang diamati, tetapi saat terjadi serangan tipe baru teknik ini tidak dapat mendeteksinya. Sedangkan *anomaly detection* merupakan sistem deteksi yang menggunakan profil tingkah laku normal sebagai acuan dalam melakukan deteksi serangan yang menggunakan profil tingkah laku norma sebagai acuan dalam melakukan deteksi serangan yang terjadi pada *host* atau *network*.*Anomaly detection* sangat tepat digunakan untuk mendeteksi serangan-serangan baru yang belum diketahui pada suatu sistem keamanan

Pada penelitian sebelumnya [8] mengatakan bahwa pada saat melakukan pendeteksian menggunakan *misuse detection,* serangan *SQL Injection* dapat terbaca dengan melakukan pencocokan tipe pola serangan yang terdaftar dengan sistem. Namun *string* yang ada pada *SQL Injection* tersebut bisa diubah dengan berbagai macam teknik, contoh seperti teknik *alternative encoding* yang mengubah *string* yang telah ada di sistem tersebut menjadi biner sehingga serangan *SQL Injection* tidak bisa dibaca oleh *misuse detection*. Serangan tersebut merupakan serangan tipe baru yang mengakibatkan serangan terebut dapat memasuki database yang ditargetkan.

Menurut [6] Solusi dari permasalahan tersebut adalah *anomaly detection*, yang dapat mendeteksi serangan-serangan tipe baru. Pada saat melakukan query IDS

memberikan sebuah peringatan dan snort yang memperkuat dengan menerangkan bahwa serangan telah terjadi pada suatu *website*, lebih baik lagi dengan menggunakan bantuan *Machine Learning*. Metode *Machine Learning* yang digunakan adalah *Bayesian Network* karena berdasarkan hasil peneltian dinyatakan tingkat deteksi anomaly menggunakan *Bayesian Network* tersebut rata-rata lebih dari 90%.

Pada penelitian ini penulis berharap dan berusaha agar bisa membuat sistem pencegahan serangan secara *real-time* yaitu *Intrusion Prevention System* (IPS) dan mengantisipasi dari serangan palsu yang mengganggu, mencegah serangan yang tidak terdeteksi oleh sistem dan mengakibatkan banyak alarm palsu yang mengganggu *traffic* jaringan. berdasarkan ulasan diatas, serangan *SQL Injection* dapat dideteksi dengan cara pengenalan *payload* HTTP berupa HTTP *request* pada bagian URI. Dengan Snort dan penerapan metode *Bayesian Network, SQL Injcetion* dapat dideteksi dan dicegah serta dikelompokan berdasarkan query yang digunakan.

II. Tujuan

Adapun tujuan yang akan dicapai dari penelitian ini adalah:

1. Mengenali Serangan *System Query Language Injection* (SQLI)
2. Mempelajari serangan *System Query Language Injection* (SQLI) secara realtime dengan menggunakan metode *Bayesian Network*.
3. Memblokir serangan *System Query Language Injection* (SQLI) secara realtime menggunakan Snort.
4. Menghasilkan sistem keamanan yang dapat mencegah serangan *SQL Injection* secara langsung.

III. Manfaat

Adapun manfaat yang dapat diambil dari penelitian ini adalah:

1. Dapat mempelajari raw paket data pada serangan *SQL Injection*.
2. Memberikan perlindungan dari serangan *SQL Injection*.
3. Apabila terjadi serangan *SQL Injection*, serangan dapat dihalau dengan *IPS*(*Intrusion Prevention System*).
4. Dapat membangun sistem keamanan yang handal baik didalam pendeteksian maupun pencegahan serta dapat memberikan rasa aman terhadap ancaman serangan yang datang.

IV. Rumusan dan Batasan Masalah

Berdasarkan latar belakang yang telah dikemukakan, maka rumusan masalah dan batasan masalah yang ada pada tugas akhir ini adalah

1. Bagaimana merancang topologi *system pencegahan* dengan menggunakan *Snort* ?
2. Bagaimana hasil yang didapatkan menggunakan metode *Snort* dan IDS (*Intrusion Detection System)* ?
3. Bagaimana proses pencegahan pada *intrusion prevention system* ?

V. Batasan Masalah

1. Pencegahan pada serangan SQL Injection secara online atau didalam suatu jaringan *Local Area Network* (LAN) yang sama.
2. Sistem pencegahan yang dibuat menggunakan Snort.
3. Serangan yang dicegah *Intrusion Prevention System* (IPS) hanya di *website* yang sudah disiapkan untuk menerima serangan.
4. hasil dari pencegahan yang dianalisa berupa *Payload* dari serangan yang diterima.
5. Snort hanya bisa mencegah serangan secara *realtime* menggunakan *rule* yang sudah diatur sebelumnya.

VI. Metodologi Penelitian

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

1. Tahap Pertama (studi pustaka/literatur)

Tahap ini ialah tahap yang menentukan permasalahan yang ada tentang *Intrusion Prevention System* (IPS) yang akan muncul pada penelitian sebelumnya tentang *Intrusion Detection System* (IDS) dengan menggunakan serangan *SQL injection* dan menggunakan metode *Bayesian Network* untuk mendeteksi tingkat keakuratan dari bentuk serangan dan melakuakan pencegahan agar serangan tersebut tidak terjadi .

2. Tahap kedua (Study Pustaka/literature)

Tahap ini ialah tahap yang mencari referensi atau menyiapkan perangkat-perangkat yang bertujuan untuk menunjang pada penelitian yang dilakukan.

3. Tahap ketiga (Perancangan)

Tahap ini ialah tahap perancangan system yang dibuat berdasarkan perumusan masalah yang dicari dalam penelitian. Dalam tahap ini melakukan konfigurasi installasi

dan beberapa tools yang digunakan seperti *OS linux*, *Wireshark*, DVWA, *Apache*, *Mysql*, *SQLMap*, *Snort*

4. Tahap keempat (Pengujian)

Tahap ini dilakukan dengan pengujian terhadap jaringan yang terdiri dari pc1 sebagai user dan komputer 2 sebagai server yang sudah diletakkan IPS yang berfungsi untuk menerima serangan dari komputer 1 sebagai user yang melakukan serangan.

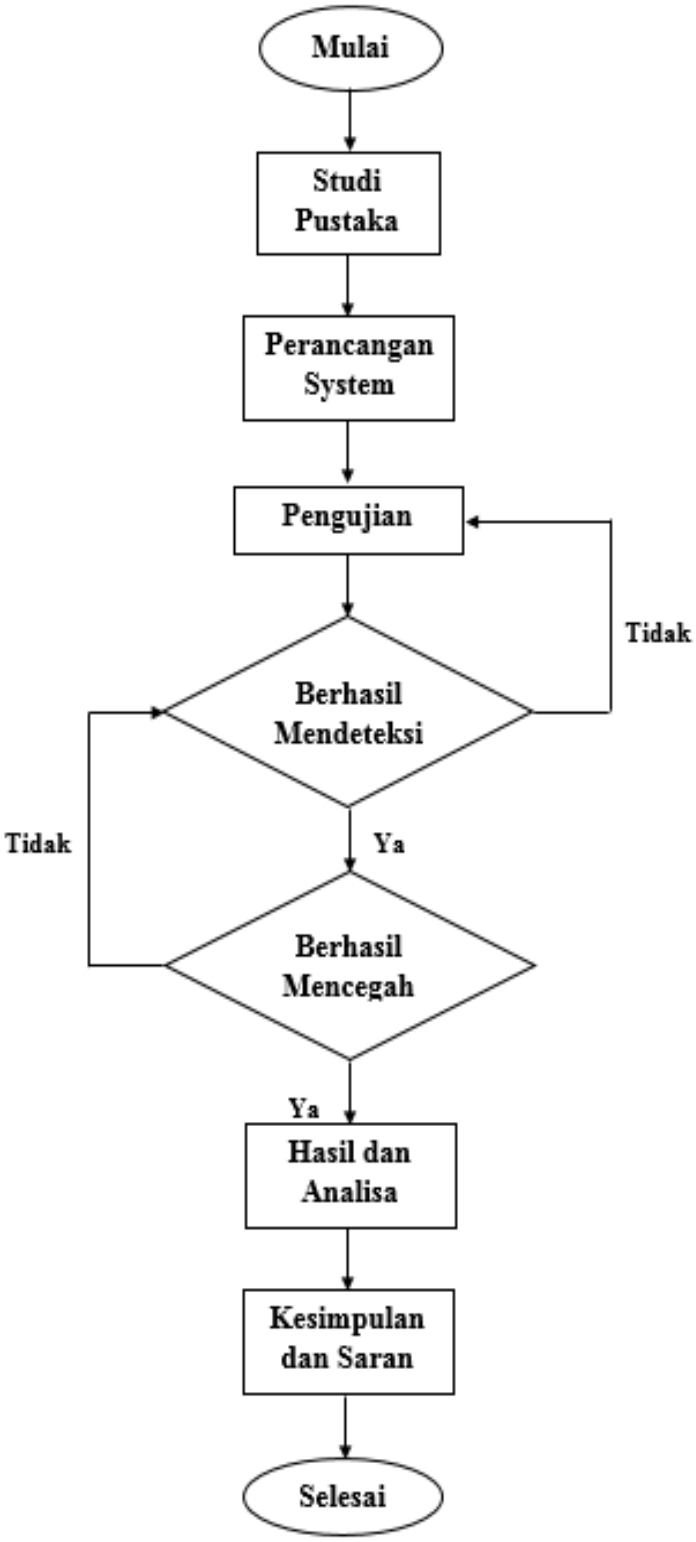
4. Tahap kelima (Analisis)

Tahap ini dilakukan dengan mengambil data dan menganalisa data yang didapatkan dari tahap ketiga yaitu tahap pengujian yang bertujuan apakah sistem berjalan dengan baik atau masih ada kekurangan, jika hasil yang didapatkan dari pengujian maka tahap ini bisa mengulangi tahap pengujian kembali dengan mengambil data yang belum sesuai dengan yang diharapkan.

5. Kesimpulan dan Saran

Tahap ini dilakukan dengan menarik kesimpulan dari analisa dan studi literature serta saran untuk penulis selanjutnya jika akan dijadikan bahan referensi.

Pada gambar 1.1 dijelaskan metodologi penelitian dalam bentuk diagram alir yang mengambarkan proses pelaksanaan penelitian.



Gambar 1.1 Diagram Alir Metodologi Pengujian

VII. SISTEMATIKA PENELITIAN

Untuk memudahkan dalam melakukan proses penyusunan tugas akhir dan memperjelas isi pada setiap bab maka dibuat sistematika penulisan sebagai berikut:

BAB I. PENDAHULUAN

Bab ini terdiri dari beberapa penjelasan secara sistematis mengenai landasan topik penelitian yang meliputi latar belakang , tujuan, manfaat, rumusan masalah, dan batasan masalah kemudian metodologi penelitian serta sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

pada bab ini berisi dasar teori dari *Intrusion Prevention System, Snort, SQL Injection, Bayesian Network,* berdasarkan research atau penelitian yang dikerjakan.

BAB III. METODOLOGI PENELITIAN

Bab ini menjelaskan secara sistematis, bagaimana proses penelitian dilakukan, penjelasan pada bab ini meliputi tahapan perancangan sistem dan proses metode penelitian

BAB IV. HASIL DAN ANALISA

Pada bab ini menjelaskan hasil dari pengujian yang telah dilakukan serta menganalisa hasil tersebut pada tiap data yang diperoleh dari hasil pengujian yang dilakukan.

BAB V. KESIMPULAN

Pada bab terakhir ini berisi kesimpulan yang berisi tentang penelitian yang telah dilakukan, serta menjawab tujuan yang diinginkan pada BAB I (Pendahuluan).

Daftar Pustaka

[1]. Adesty, I., Prabowo, W. A., Sidiq, M. F., Adesty, I., Prabowo, W. A., & Sidiq, M. F. (2020). Implementation of Intrusion Prevention System (IPS) as a Security from DDoS (Distributed Denial of Service) Attacks Penerapan Intrusion Prevention System (IPS) Suricata Sebagai Pengamanan Dari Serangan Distributed Denial of Service.

[2]. Alfiansyah, B., & Risqiwati, D. (2018). NOTIFIKASI ALERT INTRUSION DETECTION SYSTEM, 121–127.

[3]. Batista, L. O., Silva, G. A. De, Araújo, V. S., Jonathan, V., Araújo, S., Rezende, T. S., … Souza, D. C. (2018). Fuzzy neural networks to create an expert system for detecting attacks by SQL Injection . Key words :, 8–21. https://doi.org/10.5769/J201801001.

[4]. Birkinshaw, C., & Rouka. (2019). Implementing an Intrusion Detection and Prevention System Using Software-Defined Networking : Defending Against Port-Scanning and Denial-of-Service Attacks, (February).

[5]. Budiman, A. (2016). DETEKSI SERANGAN PADA JARINGAN KOMPUTER DENGAN WIRESHARK MENGGUNAKAN METODE ANOMALLY-BASED IDS, 214–222.

[6]. Deni, D. (2018). Deteksi Serangan SQL Injection Dengan Metode Bayesian Network.

[7]. Elanda, A., & Tjahjadi, D. (2018). Analisis Manajemen Resiko Sistem Keamanan Ids (Intrusion Detection System) Dengan Framework Nist (National Institute Of Standards And Technology) Sp 800-30 . (Studi Kasus : Disinfolahtaau Mabes Tni Au), *12*(1), 1–13.

[8]. Hanafi, F. I. (2017). RANCANG BANGUN PROTOTYPE KEAMANAN JARINGAN KOMPUTER DENGAN METODE IPS (INTRUSION

PREVENTION SYSTEM).

[9]. Hidayat, A. (2019). Deteksi serangan buffer overflow dengan metode string matching.

[10]. M. R. Zalbina. (2016). Sistem Deteksi HTTP menggunakan HTTP Inspect Preprocessor dan Rule Options, 1–70.

[11]. Nugroho, M. A., & Suwastika, N. A. (2018). Perancangan Intrusion Prevention System pada Jaringan Software Defined Networks, *02*(01), 1–16.

[12]. Oke, A. (2018). Two Layers Trust-Based Intrusion Prevention System for Wireless Sensor Networks, *1*, 23–29.

[13]. Puspasari, D., & Suhartono, H. (2018). Wireless Intrusion Detection System Pada STMIK Bina Insani, *2*(2), 199–208.

[14]. Setiawan, N. (2017). Open System Interconnection Layer (OSI Layer) Open System Interconnection Layer Disusun oleh : Nugroho Setiawan For Educational Purpose, (October 2016).

[15]. Suwanto, R., Ruslianto, I., & Diponegoro, M. (2019). IMPLEMENTASI INTRUSION PREVENTION SYSTEM (IPS) MENGGUNAKAN SNORT DAN IPTABLE PADA MONITORING JARINGAN LOKAL BERBASIS WEBSITE, *07*(1).