# SISTEM PENCEGAHAN SERANGAN *REMOTE TO LOCAL (R2L)* DENGAN METODE *DECISION TREE*


**OLEH:**

**ARIA NASBI**

**09011181621011**

**JURUSAN SISTEM KOMPUTER**

**FAKULTAS ILMU KOMPUTER**

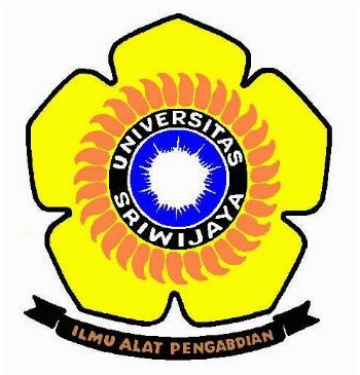
**UNIVERSITAS SRIWIJAYA**


**2020**

# SISTEM PENCEGAHAN SERANGAN *REMOTE TO LOCAL (R2L)* DENGAN METODE *DECISION TREE*

**TUGAS AKHIR**

**Diajukan Untuk Memenuhi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer**




**OLEH:**

**ARIA NASBI**
**09011181621011**

**JURUSAN SISTEM KOMPUTER**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS SRIWIJAYA**
**2020**

# LEMBAR PENGESAHAN

## SISTEM PENCEGAHAN SERANGAN *REMOTE TO LOCAL (R2L)* DENGAN METODE *DECISION TREE*

**TUGAS AKHIR**

**Diajukan Untuk Melengkapi Salah Satu Syarat**
**Memperoleh Gelar Sarjana Komputer**

**Oleh :**

**ARIA NASBI**
**09011181621011**

**Indralaya, November 2020**

**Pembimbing I Tugas Akhir**

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

**Pembimbing II Tugas Akhir**

**Ahmad Heryanto, S.Kom., M.T.**
**NIP.198701222015041002**

**Mengetahui,**
**Ketua Jurusan Sistem Komputer**

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

## HALAMAN PERSETUJUAN

Telah diuji dan lulus pada:

Hari : Jumat

Tanggal : 06 November 2020

Tim Penguji:

1. Ketua : Kemahyanto Exaudi Siahaan, S.Kom. M.T :.....
2. Sekretaris I : Deris Stiawan, M.T., Ph.D. :.....
3. Sekretaris II : Ahmad Heryanto, S.Kom., M.T. :.....
4. Anggota I : Ahmad Zarkasi, M.T. :.....
5. Anggota II : Aditya Putra Perdana P, M.T. :.....

**Mengetahui,**
**Ketua Jurusan Sistem Komputer**

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

## HALAMAN PERNYATAAN

Yang bertanda tangan di bawah ini:

Nama : Aria Nasbi

Nim : 09011181621011

Program Studi : Sistem Komputer

Judul skripsi : Sistem Pencegahan Serangan *Remote to Local* (R2L) dengan Metode *decision tree*

Hasil pengecekan software ithenticate / Turnitin : 7%

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri bukan hasil penjiplakan / *plagiat.* Apabila di temukan unsur penjiplakan / *plagiat* dalam laporan ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya.

Demikian pernyataan ini saya buat, dalam keadaan sadar dan tidak dipaksakan.


Indralaya, November 2020

Aria Nasbi

NIM.09011181621011

## HALAMAN PERSEMBAHAN

**“Setiap manusia akan ada masa kejayaannya masing-masing, tidak ada hak untuk kita dalam menilai serta dan menentukan hidup orang lain. Orang sombong tempat kembalinya di neraka (Q.S. Az- Zumar ayat 72). Kesombongan adalah tirai penghalang masuk Syurga (Q.S. al- ‘Araf ayat 13). Sesungguhnya orang-orang yang hidup dengan kesombongan itu tidak disukai-Nya (Q.S. an- Nahl ayat 22-23).”**

**“Indahnya Berbagi”**

**Skripsi ini terutama saya persembahakan untuk:**

1. Ayah dan emak saya yang tak pernah berhenti untuk berjuang dan berkorban demi berlangsungnya hidup saya, serta semangatnya dalam memberi dukungan untuk pendidikan anaknya.
2. Uwo dan udo, dalam diam juga melimpahkan kasih sayang yang tak terhingga. Dalam diam juga mendukung perjalanan hidup Aria Nasbi.
3. Dosen Pembing Tugas Akhir 1: Deris Stiawan, M.T, Ph.d. dan Pembimbing Tugas Akhir 2: Ahmad Heryanto, S.kom, M.T. yang telah bersusah payah membimbing saya mulai dari menentukan judul hingga menyelesaikan tugas akhir ini, demi mendapatkan gelas sarjana di Fakultas Ilmu Komputer.
4. Dosen Pembimbing Akademik, Ibu Sri Desy Siswanti, M.T yang telah meluangkan banyak waktu demi anak didiknya mulai dari saya masuk Jurusan Sistem Komputer hingga saya menyelasikan studi saya di Fakultas Ilmu Komputer, Universitas Sriwijaya.
5. Seluruh teman kampus terutama SKA 2016 dan teman kos Apartemen unsri Lt.3
6. Teman-temanku di luar lingkungan kampus, juga yang tak hentinya memberi *support*, menyemangati serta hal lainnya.

# KATA PENGANTAR

Puji syukur atas kehadirat Allah SWT, atas segala karunia dan rahmat-Nya sehingga penulis dapat menyelesaikan penulisan Proposal Tugas Akhir ini dengan judul "Sistem Pencegahan Serangan *Remote to Local (R2L)* Dengan Metode *Decision Tree*"

Penulisan Proposal Tugas Akhir ini dilakukan untuk melengkapi salah satu syarat memperoleh gelar Sarjana Komputer di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya. Sebagai sumber penulisan, penulis mengambil berdasarkan hasil penelitian, observasi dan beberapa sumber literatur yang mendukung dalam penulisan proposal ini.

Pada kesempatan ini juga, penulis menyampaikan ucapan terima kasih yang sebesar-besarnya kepada semua pihak yang telah membantu selama dalam proses penulisan Proposal Tugas Akhir ini.

Oleh karena itu, pada kesempatan ini penulis mengucapkan rasa syukur kepada Allah SWT. dan mengucapkan terima kasih kepada yang terhormat :

1. Orang tua serta keluarga penulis tercinta, yang telah memberikan doa dan restu, dukungan serta kepercayaan sehingga penulis masih melanjutkan pendidikan hingga sampai saat ini dan menjadi penyemangat penulis dalam menyelesaikan tugas akhir ini.
2. Bapak Jaidan Jauhari, S.Pd., M.T. selaku Dekan Fakultas Ilmu Komputer Universitas Sriwijaya.
3. Bapak Dr. H. Sukemi, M.T. selaku Ketua Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
4. Ibu Sri Desy Siswanti, S.T., M.T selaku dosen pembimbing akademik di jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya
5. Bapak Deris Stiawan, M.T., Ph. D selaku Dosen Pembimbing I Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.

6. Bapak Ahmad Heryanto, S. Kom., M.T. selaku Dosen Pembimbing II Tugas Akhir di Jurusan Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
7. Mbak Winda Kurnia Sari selaku admin Jurusan Sistem Komputer yang telah membantu mengurus seluruh berkas.
8. Seluruh dosen, staff, serta karyawan Fakultas Ilmu Komputer Universitas Sriwijaya.
9. Seluruh teman-teman seperjuangan angkatan 2016 Sistem Komputer Fakultas Ilmu Komputer Universitas Sriwijaya.
10. Almamater Universitas Sriwijaya.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan Proposal Tugas Akhir ini. Untuk itu, segala saran dan kritik yang membangun sangatlah penting bagi penulis, Akhir kata, semoga Proposal Tugas Akhir ini dapat bermanfaat dan berguna bagi para pembaca.

Palembang, November 2020
Penulis

Aria Nasbi
NIM. 09011181621011

# SISTEM PENCEGAHAN SERANGAN *REMOTE TO LOCAL* (R2L) DENGAN METODE *DECISION TREE*

**Aria Nasbi (09011181621011)**

Jurusan Sistem Komputer, Fakultas Ilmu Komputer, Universitas Sriwijaya

E-mail : nasbiaria17@gmail.com

## Abstrak

*Intrusion detection system* (IDS) yang merupakan suatu sistem untuk mendeteksi lalu lintas dalam sebuah jaringan, tetapi kelemahan dari IDS ini hanya bisa mendeteksi dan memberikan *alert* tanpa memberikan respon jika terdapat paket serangan. Adapun sistem yang mendeteksi dan memberikan respon terhadap lalu lintas jaringan ini di sebut *intrusion prevention system* (IPS) yaitu sistem yang mampu meberikan tindakan untuk *deny* atau *allow* pada suatu paket yang melintas pada lalu lintas jaringan tersebut. *Remote to Local* (R2L) merupakan suatu intrusi yang bertujuan untuk melakukan akses terhadap sistem yang menjadi target *attacker* tanpa memiliki hak akses terhadap sistem yang akan menjadi korban tersebut. *Decision tree* merupakan suatu metode yang memberikan tingkat akurasi yang lebih tinggi dari algoritma lainnya dalam mendeteksi serangan *DoS* dan *Probe*, hasil deteksi yang dievaluasi dengan menggunakan *confusion matrix* untuk mendapatkan hasil akurasi. Oleh karena itu, metode *decision tree* di gunakan pada penelitian ini, dan menghasilkan akurasi 94%.

**Kata kunci:** *intrusion detection system (IDS), Intrusion Prevention system (IPS), Decision Tree, Remote to Local (R2L)*

# *INTRUSION PREVENTION SYSTEM OF REMOTE TO LOCAL (R2L) ATTACK WITH DECISION TREE METHOD*

***Aria Nasbi (09011181621011)***

*Department of Computer Systems, Faculty of Computer Science, Sriwijaya University*

*E-mail: nasbiaria17@gmail.com*

***Abstract***

*Intrusion detection system (IDS) which is a system for detecting traffic in a network, but the weakness of this IDS can only detect and provide alerts without responding if there is an attack packet. The system that detects and responds to network traffic is called an intrusion prevention system (IPS), which is a system that is capable of giving actions to deny or allow a packet passing through the network traffic. Remote to Local (R2L) is an intrusion that aims to access the system that is the attacker's target without having access rights to the system that will become the victim. Decision tree is a method that provides a higher level of accuracy than other algorithms in detecting DoS and Probe attacks, the detection results are evaluated using confusion matrix to get accuracy results. Therefore, the decision tree method is used in this study, and produces an accuracy of 94%.*

***Keywords****: intrusion detection system (IDS), Intrusion Prevention system (IPS), Decision Tree, Remote to Local (R2L)*

## Daftar Isi

**Halaman**

**Halaman Judul** ..... **i**

**Halaman Pengesahan** ..... **ii**

**Halaman Persetujuan** ..... **iii**

**Halaman Pernyataan** ..... **iv**

**Halaman Persembahan** ..... **v**

**Kata Pengatar** ..... **vi**

**Abstrak** ..... **viii**

***Abstract*** ..... **ix**

**Daftar Isi** ..... **x**

**Daftar Gambar** ..... **xiii**

**Daftar Tabel** ..... **xiv**

**Daftar Rumus** ..... **xv**

**Bab I**

**Pendahuluan**

**1.1 Latar Belakang** ..... **1**

**1.2 Tujuan** ..... **2**

**1.3 Manfaat** ..... **2**

**1.4 Rumusan Masalah** ..... **3**

**1.5 Batasan Masalah** ..... **3**

**1.6 Metodologi Penelitian** ..... **3**

**1.7 Sistematika Penulisan** ..... **4**

**Bab II**

**Tinjauan Pustaka**

**2.1 Penelitian Terkait ..... 6**
**2.2 Diagram Penelitian ..... 6**
**2.3 Landasan Teori ..... 7**
**2.3.1 Definisi IDS *(Intrusion Detection System)* ..... 7**
**2.3.1.1 Klasifikasi IDS ..... 8**
**2.3.1.1.1 Sumber Data *(Data Resource)* ..... 8**
**2.3.1.1.2 Metode Deteksi IDS ..... 9**
**2.3.2 Definisi IPS *(Intrusion Prevention System)* ..... 9**
**2.3.2.1 Perbandingan IDS dan IPS ..... 10**
**2.3.2.2 Klasifikasi IPS ..... 11**
**2.3.3 *Remote to Local* (R2L) ..... 11**
**2.3.4 *SQL injection Attack* ..... 12**
**2.3.5 *Suricata Engine* ..... 12**
**2.3.6 Algoritma *Decision Tree* ..... 13**
**2.3.7 Dataset ..... 16**
**2.3.7.1 Evaluasi Hasil Sistem Deteksi ..... 16**

**Bab III**

**Metodologi Penelitian**

**3.1 Pendahuluan ..... 18**
**3.2 Kerangka Kerja Penelitian ..... 18**
**3.3 Data yang digunakan ..... 20**
**3.3.1 Dataset ..... 20**
**3.3.2 Data real-time ..... 20**
**3.4 Perancangan sistem ..... 20**
**3.4.1 kebutuhan perangkat lunak dan perangkat keras ..... 21**
**3.5 *Suricata engine* sebagai IDS *(Intrusion Detection System)* ..... 21**
**3.6 Data *Extraction* ..... 21**

**3.7 Deteksi dengan Metode *Decision Tree* Deteksi dengan Metode *Decision Tree* ..... 24**
**3.8 Mencari Pola Serangan *Remote to Local* (R2L) ..... 25**
**3.9 Pencegahan Serangan *Remote to Local* (R2L)..... 25**
**3.9.1 Skenario Percobaan ..... 25**
**3.9.2 Tahapan Pengujian IPS *system* ..... 26**

**Bab IV**
**Hasil Dan Analisa**
**4.1 Pendahuluan..... 28**
**4.2 Perbandingan Data ..... 28**
**4.2.1 Data Pcap *(Wireshark)* ..... 28**
**4.2.2 Data Hasil Ekstraksi ..... 29**
**4.2.3 Perbandingan Data Ekstraksi, Raw data dengan *Alert Snort* . 31**
**4.3 Koreksi Hasil Pengujian *Data Extraction*..... 33**
**4.4 Hasil Deteks Dengan Algoritma *Decision Tree* ..... 35**
**4.4.1 Hasil deteksi *Suricata engine* ..... 35**
**4.4.2 Data correction ..... 35**
**4.5. Hasil Data di Drop Dengan IPS *Engine* yang Telah Di Bangun ..... 38**
**4.5.1 *Rules* yang digunakan ..... 38**
**4.5.2 *Capture* Data *pcap* Serangan ..... 39**
**4.5.3 Performa Perbandingan Data Sistem IPS ..... 40**
**4.5.4 Hasil dan Validasi Data Serangan yang di *Drop* ..... 41**

**Bab V**
**Kesimpulan dan Saran**
**5.1 Kesimpulan ..... 44**
**5.2 Saran..... 45**

**Daftar Pustaka**

# DAFTAR GAMBAR

**Halaman**


**Gambar 2.1 Diagram konsep penelitian ..... 7**
**Gambar 2.2 Arsitektur dasar IDS ..... 8**
**Gambar 2.3 Topologi dan terminologi dalam implementasi IPS ..... 10**
**Gambar 2.4 Struktur dari algoritma *Decision Tree* ..... 13**
**Gambar 2.5 Topologi proses pengambilan dataset ..... 16**
**Gambar 3.1 Kerangka kerja penelitian ..... 19**
**Gambar 3.2 *Flowchart* Program *Feature Extraction* ..... 22**
**Gambar 3.3 *Flowchart Program Decision Tree* ..... 24**
**Gambar 4.1 Dataset berbentuk *Pcap (Wireshark)* ..... 29**
**Gambar 4.2 Hasil *feature extraction* ..... 30**
**Gambar 4.3 *Data clean* ..... 30**
**Gambar 4.4 Perbandingan antara *Raw Data, Alert,* Dan *Data Extraction* .. 32**
**Gambar 4.5 *Validasi antara Raw Data dengan Data Extraction* ..... 33**
**Gambar 4.6 *Confusion matrix* dari R2L *attack.* ..... 36**
**Gambar 4.7 Data *capture* proses simulasi paket *drop* ..... 40**
**Gambar 4.8 Validasi antara data pcap dan *Alert* IPS *engine* ..... 42**

# DAFTAR TABEL

**Halaman**


| | | |
|---|---|---|
| **Tabel 1** | **Perbandingan IDS dan IPS** | **10** |
| **Tabel 2** | **Tipe *Alert* pada *Confussion Matrix*** | **17** |
| **Tabel 3** | ***Confusion Matrix*** | **17** |
| **Tabel 4** | **Kebutuhan penelitian tugas akhir.** | **21** |
| **Tabel 5** | **Atribut *Data Extraction*** | **23** |
| **Table 6** | ***Payload* dari serangan R2L** | **34** |
| **Table 7** | **Hasil deteksi dataset dengan *Suricata engine*** | **35** |
| **Table 8** | **Pebandingan Data dalam Perancangan Sistem IPS** | **40** |

# DAFTAR RUMUS

**Halaman**


**Rumus 2.1 Menentukan entropi dalam Algoritma *Decision Tree* ..... 15**

**Rumus 2.2 Mencari gain dalam Algoritma *Decision Tree* ..... 15**

**Rumus 2.3 Untuk mencari akurasi ..... 17**

**Rumus 2.4 Untuk mencari *false positive rate* ..... 17**

**Rumus 2.5 Untuk mencari *true positive rate* ..... 17**

# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

*Intrusion Detection System* (IDS) merupakan *alarm* intrusi dalam keamanan jaringan. Dimana tidak memberi respon terhadap paket serangan yang terdeteksi tetapi hanya memberikan *alert [1]*. Yang selanjutnya akan di tindak lanjuti oleh *administrator* atau *incident handler*

Secara umum, menurut [2] berdasarkan metode deteksi terbagi menjadi dua kategori yaitu *signature based* dan *anomaly based*. *Signature based* yaitu metode yang melakukan pencocokan data dengan melihat *behavior* yang sudah di definisikan sebelumnya. Sedangkan *anomaly based* merupakan metode yang di ambil berdasarkan behaviour yang bebeda dengan *behavior* normal.

Dari kedua metode tersebut masih memliki kelemahan [3]. Untuk IDS yang berdasarkan teknik *signature based* tidak bisa mendeteksi tipe serangan baru yang tidak ada pada database serangan. Sedangkan IDS dengan metode *anomaly* sering menghasilkan *false alarm* yang besar walaupun mampu untuk mendeteksi serangan tipe yang baru.

Paket-paket yang telah terdeteksi akan di beri tindakan baik itu *allow* ataupun *deny*, maka sistem yang selanjutnya digunakan adalah *Intrusion prevention system* (IPS) [4]. IPS akan memberikan sistem keamanan yang lebih *advance* dari IDS, dimana IPS ini akan memberikan respon terhadap paket intrusi yang terdeteksi. IPS berjalan secara otomatis di belakang *firewall* untuk mendeteksi dan memblokir aktivitas yang berbahaya dalam jaringan[5].

*Remote to Local* (R2L) merupakan jenis intrusi yang melakukan akses pada mesin yang dituju secara ilegal [6], tanpa harus memliki *account* yang sah terhadap web server, aplikasi dan terhadap mesin yang di tuju lainnya [7]. *Attacker* akan memanfaatkan kerentanan dari mesin yang di tuju dan mengeskploitasinya sehingga *attacker* tersebut mendapat hak akses.

Dengan menggunakan perhitungan statistika dan algoritma yang matematis *machine learning* dapat di gunakan untuk mengetahui informasi yang tersembunyi ataupun data yang mencurigakan[8]. Dalam percobaan [9] membandingkan beberapa algoritma *mechine learning* diantaranya *Decision Tree, Ripper Rule, Back Propagation Neural Network , Radial Basis Function Neural Network, Bayesian Network* dan *Naïve Bayesian*. Hasil dari percobaan tersebut menunjukkan *Decision Tree* memberikan tingkat akurasi yang lebih tinggi dari algoritma lainnya dalam mendeteksi serangan *DoS* dan *Probe.*

Dalam penelitian sebelumnya[3] bagaimana memvisualisasikan serangan *Remote to Local* dengan menggunakan algoritma clustering k-mean untuk mendeteksi dan/atau mengelompokkan serangan R2L. Dari beberapa ulasan di atas, maka penelitian ini akan melakukan deteksi dan pencegahan terhadap serangan *Remote to Local* (R2L) dengan menggunakan algoritma *Decision Tree.*

## 1.2 Tujuan

Penelitian ini fokus pada serangan *Remote to Local* dengan menggunakan algortima *decision tree* untuk memblokir paket serangan yang terdeteksi. Adapun tujuan yang ingin dicapai dari penelitian tugas akhir ini antara lain adalah:

1. Membedakan antara paket normal dan paket serangan sehingga dapat mendeteksi dan mencegah serangan *Remote to Local* (R2L).
2. Menerapkan algoritma *decision tree* untuk mendeteksi dan melakukan pemblokiran terhadap paket serangan *Remote to Local*.
3. Menghitung akurasi deteksi serangan *Remote to Local* dengan algoritma *decision tree*
4. Melakukan *drop* terhadap paket yang terdeteksi sebagai serangan *Remote to Local* (R2L)

## 1.3 Manfaat

Adapun manfaat yang di dapat dari penelitian tugas akhir ini adalah:

1. Dapat membedakan paket serangan dan paket normal.
2. Dapat memberikan kemudahan dalam mendeteksi paket serangan *remote to local.*

3. Dapat memberikan keamanan pada server dari serangan *remote to local*, karena jika terdapat paket serangan *remote to local* maka paket serangan tersebut akan otomatis di *block.*
4. Sistem ini akan berjalan secara real-time.

## 1.4 Rumusan Masalah

Ada beberapa masalah yang akan di bahas dari penelitian ini yaitu:

1. Bagaimana mengekstrak dataset, kemudian mencari pola dari serangan *remote to local* tersebut?
2. Bagaimana setelah paket tersebut terdeteksi, kemudian melakukan *block* terhadap paket serangan tersebut?
3. Bagaimana melakukan semuanya tersebut secara real-time?

## 1.5 Batasan Masalah

Dari latar belakang dan rumusan masalah yang telah ada, maka di bawah ini merupakan batasan masalah yang akan di lakukan pada penelitian tugas akhir ini:

1. Menggunakan dataset yang telah di *capture* dengan menggunakan *wireshark.*
2. Mengklasifikasikan serangan *Remote to Local* (R2L) menggunakan algoritma *decision tree.*
3. Serangan yang di deteksi dan di *drop* hanya serangan SQL *injection*
4. Penelitian ini hanya sebatas mendeteksi dan mem-*block,* tidak di visualkan.

## 1.6 Metodologi Penelitian

Agar tujuan penelitian tugas akhir ini dapat tercapai berikut ini adalah tahapan penelitian:

1. Tahap Pertama (Studi Pustaka/ Literatur)

Dengan memepelajari literatur akan lebih memudahkan dalam menjalankan penelitian ini, banyak jenis literatur yang dapat dijadikan sebagai referensi seprti artikel, journal, paper dan lainnya.

2. Tahap Kedua (Perancangan Sistem)

Pada tahapan ini merupakan tahapan mengenai bagaimana membangun dan menerapkan metode pada sistem tugas akhir. Selain itu, apa saja yang digunakan pada penelitian seperti hardware maupun software, kemudaian bagaiman proses konfigurasi atau pun menulis code untuk penerapan metode pada tugas akhir.

3. Tahap Ketiga (Pengujian)

Tahap ini merupakan tahan pengujian berdasarkan metodologi penelitian dan penelitian sebelumnya sehingga didapatkan data hasil uji yang sesuai dan tepat dengan algoritma.

4. Tahap Keempat (Analisa)

Pada tahap ini adalah menganalisa proses dari berjalannya penelitian tugas akhir ini, dimana dengan metodologi yang telah di lakukan dan analisa terhadap hasil yang telah di dapat dari penelitian tugas akhir ini.

5. Tahap Kelima (Kesimpulan dan Saran)

Dari beberapa tahap yang telah dilalui maka dari proses dan hasil penelitian ini di dapatkan kesimpulan, dan akan ada beberapa saran untuk para peneliti berikutnya

## 1.7 Sistematika Penelitian

Pada penyusunan tugas akhir ini dibuat sistematika penulisan untuk mempermudah dan memperjelas konten dari tiap bab, yaitu:

**BAB I. PENDAHULUAN**

Bab pertama dalam laporan ini akan berisi beberapa bagian yang menggambarkan sebelum penelitian, yang akan di dapat dari penelitian dengan beberapa batasan dalam masalah pada penelitian ini dan tidak lupa juga menambahkan beberapa aturan dalam penulisan laporan ini.

**BAB II. TINJAUAN PUSTAKA**

Tinjauan Pustaka yang merupaka bagian bab ke dua pada laporan ini yang akan berisi tentang dasar-dasar teori terkait penelitian ini, baik itu metode yang digunakan, dasar-dasar teori yang membangun lainnya seperti tentang IDS, IPS, R2L dan yang terkait lainnya.

**BAB III. METODOLOGI PENELITIAN**

Pada bagian bab ke tiga yang berisikan metode penelitian, yang akan menjelaskan tentan metode yang akan di gunakan dan perancangan sistem lainnya.

**BAB IV. PENGUJIAN DAN ANALISISA**

Setelah mendapatkan hasil dari penelitian ini, semua akan di cantumkan pada bab ini, yaitu bab empat yang berisi tentang hasil dan analisanya.

**BAB V. KESIMPULAN dan SARAN**

Untuk meyimpulkan dari penelitian ini akan terdapat pada bagian bab ke lima, serta akan ada beberapa saran untuk yang akan melakukan penelitian selanjutnya.

# DAFTAR PUSTAKA


[1] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, no. 1, 2019.

[2] T. Akhir and A. Hidayat, "Deteksi serangan buffer overflow dengan metode string matching," 2019.

[3] E. A. Winanto, A. Heryanto, and D. Stiawan, "Visualisasi Serangan Remote to Local ( R2L ) Dengan Clustering K-Means," *Annu. Res. Semin. 2016*, vol. 2, no. 1, pp. 359–362, 2016.

[4] F. Hock and P. Kortiš, "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks," in *2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, 2015, pp. 1–4.

[5] R. F. Pratama, N. A. Suwastika, and M. A. Nugroho, "Design and implementation adaptive Intrusion Prevention System (IPS) for attack prevention in software-defined network (SDN) architecture," *2018 6th Int. Conf. Inf. Commun. Technol. ICoICT 2018*, vol. 0, no. c, pp. 299–304, 2018.

[6] P. Sornsuwit and S. Jaiyen, "Intrusion detection model based on ensemble learning for U2R and R2L attacks," in *2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 2015, pp. 354–359.

[7] D. Sklavounos, A. Edoh, and M. Plytas, "A Statistical Approach Based on EWMA and CUSUM Control Charts for R2L Intrusion Detection," in *2017 Cybersecurity and Cyberforensics Conference (CCC)*, 2017, pp. 25–30.

[8] H. Nihri, E. S. Pramukantoro, and P. H. Trisnawan, "Pengembangan IDS Berbasis J48 Untuk Mendeteksi Serangan DoS Pada Perangkat Middleware

IoT," *J. Pengemb. Teknol. Inf. dan Ilmu Komput. Univ. Brawijaya*, vol. 2, no. 12, 2018.

[9] P. Sangkatsanee, N. Wattanapongsakorn, and C. Charnsripinyo, "Practical real-time intrusion detection using machine learning approaches," *Comput. Commun.*, vol. 34, no. 18, pp. 2227–2235, 2011.

[10] Y. Chi, T. Jiang, X. Li, and C. Gao, "Design and implementation of cloud platform intrusion prevention system based on SDN," *2017 IEEE 2nd Int. Conf. Big Data Anal. ICBDA 2017*, pp. 847–852, 2017.

[11] A. Özgür and H. Erdem, "A review of KDD99 dataset usage in intrusion detection and machine learning between 2010 and 2015," *PeerJ*, vol. 4, pp. 0–21, 2016.

[12] R. Z. A. Mohd, M. F. Zuhairi, A. Z. A. Shadil, and H. Dao, "Anomaly-based NIDS: A review of machine learning methods on malware detection," in *2016 International Conference on Information and Communication Technology (ICICTM)*, 2016, pp. 266–270.

[13] A. Jamdagni, "Payload-based Anomaly Detection in HTTP Traffic," no. November, p. 190, 2012.

[14] "Mengenal Intrusion Prevention System (IPS) | Netsec Indonesia." [Online]. Available: https://netsec.id/intrusion-prevention-system/. [Accessed: 01-Feb-2020].

[15] J. Gondohanindijo, "IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan/Intrusi," *Maj. Ilm. Inform.*, vol. 03, no. 03, pp. 38–59, 2012.

[16] N. Dulanović, D. Hinić, and D. Simić, "An intrusion prevention system as a proactive security mechanism in network infrastructure," *Yugosl. J. Oper. Res.*, vol. 18, no. 1, pp. 109–122, 2008.

[17] T. I. Kuntoro Priyambodo, Uzayisenga Venant, Devi Valentino Waas, "A Comprehensive Review of e-Government Security," *Asian Journal of Information Technology*, vol. 16, no. 2. pp. 282–286, 2017.

[18] I. Ahmad, A. B. Abdullah, and A. S. Alghamdi, “Remote to Local attack detection using supervised neural network,” in *2010 International Conference for Internet Technology and Secured Transactions*, 2010, pp. 1–6.

[19] “Characteristics of an SQL injection attack.” [Online]. Available: https://www.ibm.com/support/knowledgecenter/en/SSMPHH_10.6.0/com.ibm.guardium.doc/monitor/threat_diags_character_SQL.html. [Accessed: 11-Aug-2020].

[20] “Suricata | Open Source IDS / IPS / NSM engine.” [Online]. Available: https://suricata-ids.org/. [Accessed: 11-Aug-2020].

[21] L. Mehra, M. K. Gupta, and H. S. Gill, “An effectual & secure approach for the detection and efficient searching of Network Intrusion Detection System (NIDS),” *IEEE Int. Conf. Comput. Commun. Control. IC4 2015*, pp. 4–8, 2016.

[22] S.-Y. Wu and E. Yen, “Data mining-based intrusion detectors,” *Expert Syst. Appl.*, vol. 36, no. 3, Part 1, pp. 5605–5612, 2009.