

**SISTEM PENCEGAHAN RANSOMWARE
WANNACRY MENGGUNAKAN METODE STRING
MATCHING**



Oleh :

**Muhammad Ikhsan
NIM : 09011381621102**

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021**

**SISTEM PENCEGAHAN RANSOMWARE
WANNACRY MENGGUNAKAN METODE STRING
MATCHING**

SKRIPSI

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



Oleh :

**Muhammad Ikhsan
09011381621102**

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2021**

LEMBAR PENGESAHAN
SISTEM PENCEGAHAN RANSOMWARE WANNACRY MENGGUNAKAN
METODE STRING MATCHING

SKRIPSI

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

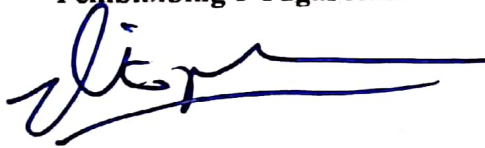
Oleh :

MUHAMMAD IKHSAN

09011381621102

Palembang, Juli 2021

Pembimbing I Tugas Akhir



Deris Setiawan, 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 : Selasa

Tanggal : 5 Juli 2021.

Tim Penguji :

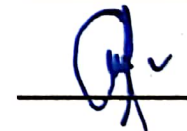
1. Ketua : Sarmayanta Sembiring, S.SI., M.T.

2. Sekretaris : Iman Saladin B. Azhar. S.Kom., M.MSI.

3. Pembimbing I : Deris Stiawan, M.T., Ph.D.

4. Pembimbing II : Ahmad Heryanto, M.T.

5. Anggota I : Ahmad Zarkasi, S.T., M.T.



Mengetahui,
Ketua Jurusan Sistem Komputer



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

NIP. 196612032006041001

HALAMAN PERNYATAAN

Yang bertanda tangan dibawah ini :

Nama : Muhammad Ikhsan
NIM : 09011381621102
Program Studi : Sistem komputer Unggulan
Judul : Sistem Pencegahan Ransomware Menggunakan Metode String Matching

Hasil Pengecekan *Software iThenticate / Trunitin* : 1 %

Menyatakan bahwa laporan tugas akhir saya merupakan hasil karya sendiri dan bukan hasil penjiplakan / plagiat dari penelitian orang lain. Apabila ditemukan unsur penjiplakan / plagiat dalam laporan tugas akhir ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian pernyataan ini saya buat dalam keadaan sadar dan tidak dipaksakan



Palembang, April 2021



Yang menyatakan,

Muhammad Ikhsan

KATA PENGANTAR

Assalamu'alaikum Warahmatullah Wabarakatuh

Puji dan syukur penulis panjatkan atas kehadiran Allah Subhanahu Wata'ala yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan Tugas Akhir ini dengan judul **“Sistem Pencegahan Ransomware Menggunakan Metode String Matching”**. Shalawat serta salam tak lupa kita curahkan kepada junjungan kita Nabi Muhammad SAW beserta keluarga, sahabat dan para pengikutnya yang insyaallah istiqomah hingga akhir zaman.

Selesainya penyusunan Tugas Akhir ini tidak terlepas dari peran serta semua pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan ucapan terima kasih yang sebesar – besarnya kepada :

1. Allah Subhanahu Wata'ala yang telah memberikan berkah serta nikmat kesehatan dan kesempatan kepada penulis dalam menyusun skripsi ini.
2. Kedua orang tua saya, yaitu Alm. Ayahanda Saya H. Suparyana, S. Pd. I dan Ibu saya Hj. Jumiyati. Yang telah memberikan semangat dan doa terbaik, untuk mengerjakan skripsi ini.
3. Kedua Kakak laki – laki dan Kakak perempuan dan seluruh keponakan saya. Yang telah memberikan dukungan serta semangat yang kuat, dalam menjalani masa perkuliahan ini.
4. Bapak Dr. Ir. H. Sukemi, M.T., selaku Ketua Jurusan di Sistem Komputer Universitas Sriwijaya.
5. Bapak Deris Setiawan, M.T., Ph.D., selaku Pembimbing I Skripsi atau Tugas Akhir.
6. Bapak Ahmad Heryanto, S.Kom., M.T., selaku Pembimbing II Skripsi atau Tugas Akhir.
7. Bapak Sutarno, S.T., M.T., selaku Pembimbing Akademik.
8. Bapak Sarmayanta Sembiring, S.Si., M.T., sebagai Ketua Sidang.
9. Bapak Ahmad Zarkasih, S.T., M.T., sebagai Penguji Sidang.
10. Bapak Ahmad Fali Oklilas , S.T., M.T., selaku Kepala Laboratorium Elektronika Dasar, yang telah meminjamkan fasilitas lab.

11. Teman – Teman saya Cahyadi, Ilham, Atha, Renal, Alep, Arep, Yogik, Hapis, Does, Andik, Hamzah, Febby, Rofi, Resky, Amrina, Yusril, Udin, dan teman – teman penghuni Lab Eldas.
12. Sri Retno Rahayu, yang telah memberikan *mood booster* dan semangat dalam mengerjakan skripsi, pengurusan berkas dan revisian.
13. Admin Jurusan Sistem Komputer Mbak Renny dan Mbak Sari, dalam membantu pengurusan berkas.
14. Satpam Fasilkom Kak Angga, Kak Herman dan Kak Hery, dalam memberikan izin menginap di Lab.
15. Untuk semua pihak yang terlibat dalam membantu pembuatan skripsi ini. Yang tidak bisa disebutkan satu persatu.

Wassalamu’alaikum Warahmatullahi Wabarakatuh.

Palembang, Juli 2021

Penulis

Muhammad Ikhsan

NIM. 09011381621102

Ransomware Wannacry Prevention System with String Matching

Muhammad Ikhsan (09011381621102)

Department of Computer Engineering, Faculty of Computer Science

Sriwijaya University

Email : muhammadikhsantkj1@gmail.com

Abstract

Wannacry ransomware is a specific type of malware that threatens access to victims unless their data has been redeemed or paid for. Usually, ransomware encrypts the content on the victim's hard drive making it inaccessible to the victim. After making a payment or ransom, a decryption key will be given to the victim. In this research, a snort detection system is used and the prevention system is opsense. For string matching, the pattern obtained from the snort detection system will be used and the packets will be filtered with the searched keywords. The success rate for the snort detection system is 66%, while the success rate for the prevention system is 61%. And the detection system of the string matching level of confusion matrix is 85% of the unvarra dataset, while the confusion matrix of the attack trial dataset is 95%.

Key Word : Ransomware, Wannacry, String Mathing, Suricatta

Sistem Pencegahan Ransomware Menggunakan Metode String Matching

Muhammad Ikhsan (09011381621102)

Jurusan Sistem Komputer, Fakultas Ilmu Komputer
Universitas Sriwijaya

Email : muhammadikhsantkj1@gmail.com

ABSTRAK

Ransomware wannacry adalah jenis malware tertentu yang mengancam akses ke korban kecuali datanya telah ditebuskan atau dibayarkan. Biasanya, *ransomware* mengenkripsi konten yang ada pada *hard drive* korban sehingga membuatnya tidak dapat diakses oleh korban. Setelah melakukan pembayaran atau tebusan, *key* dekripsi akan diberikan kepada korban. Dalam penelitian ini digunakanlah sebuah sistem deteksi *snort* dan sistem pencegahannya adalah *opnsense*. Untuk *string matching* akan memanfaatkan pola yang didapatkan dari sistem deteksi *snort* dan akan disaring paket – paket tersebut dengan kata kunci yang dicari. Untuk tingkat keberhasilan pada sistem deteksi *snort* adalah 66%, sementara tingkat keberhasilan dari sistem prevensi adalah 61%. Dan sistem deteksi dari *string matching* tingkat *confussion matrix* adalah 85% dari dataset unvarra, sementara *confussion matrix* dari dataset percobaan serangan adalah 95%.

Kata kunci : *Ransomware, Wannacry, String Mathing, Suricatta*

DAFTAR ISI

	Halaman
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xv
BAB I. PENDAHULUAN	1
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	3
1.7. Sistematika Penulisan	4
BAB II. TINJAUAN PUSTAKA	6
2.1. Penelitian Sebelumnya atau Terdahulu	6
2.2. Definisi Intrusion Prevention System (IPS)	6
2.3. Beberapa Kategori Sistem Pencegahan atau IPS berdasarkan Penyebarannya	7
2.3.1. Sistem Pencegahan Berbasis <i>Host</i> (HIPS)	8
2.3.2. Sistem Pencegahan Berbasis Jaringan (NIPS)	9
2.3.3. Sistem Pencegahan Anomali Pada Jaringan Nirkabel	11
2.3.4. <i>Network Behavior Analysis</i> (NBA)	12
2.4. Kategorisasi Sistem Pencegahan Anomali Berdasarkan Cara Deteksi ...	13
2.4.1. <i>Signature Based</i>	13
2.4.2. <i>Based Anomaly</i>	14
2.5. Sistem Deteksi Anomali (IDS)	14
2.6. Akurasi Hasil Dari Deteksi Snort <i>Intrusion Detection System</i>	14
2.7. <i>Malware</i>	15
2.6.1. Taksonomi <i>Malware</i>	15

2.6.2.	Jenis – Jenis <i>Malware</i> Menurut Perilakunya	16
2.8.	<i>Ransomware</i>	18
2.7.1.	<i>Crypto Ransomware</i>	26
2.7.2.	Jenis <i>Crypto Ransomware</i>	26
2.7.3.	<i>Locky (Ransom.Locky)</i>	28
2.9.	<i>WannaCry</i>	28
2.8.1.	<i>EternalBlue</i>	29
2.8.2.	<i>Doublepulsar</i>	29
2.10.	<i>String matching</i>	30
2.11.	Fitur Ekstraksi	31
2.12.	<i>Snort</i>	31
2.11.1.	<i>Sniffer-Mode</i>	32
2.11.2.	<i>Packet-Logger-Mode</i>	32
2.13.	<i>Instrusion Detection Mode</i>	32
2.14.	<i>Instrusion Prevention Mode</i>	33
2.15.	Cara kerja <i>Snort</i>	33
2.16.	<i>OPNsense</i>	34
2.17.	Suricata	34
2.18.	Cara Kerja Suricata	35
BAB III. METODOLOGI PENELITIAN		36
3.1.	Pendahuluan	36
3.2.	Kerangka kerja	36
3.3.	Perancangan Sistem	38
3.3.1.	<i>Dataset Ransomware Wannacry</i>	38
3.3.2.	Kebutuhan <i>Hardware</i> atau Perangkat Keras	39
3.3.3.	Kebutuhan <i>Software</i> atau Perangkat Lunak	39
3.3.4.	Skenario pada <i>dataset unvarra</i>	40
3.3.5.	Skenario pada percobaan sendiri	41
3.4.	<i>Snort</i> sebagai IDS	41
3.5.	Deteksi <i>Ransomware WannaCry</i> Menggunakan <i>Snort</i>	42
3.6.	Mengunduh <i>Ransomware Wannacry</i> pada <i>theZoo</i>	43
3.7.	Mencari Celah Pada Komputer Target	44

3.8.	Mencari Pola Serangan dari <i>Ransomware WannaCry</i>	46
3.9.	Mendeteksi Serangan <i>Wannacry</i> Menggunakan Metode String Matching	49
3.10.	<i>Opsense</i> sebagai IPS	52
3.11.	Mencegah Serangan <i>Ransomware Wannacry</i> Menggunakan <i>Opsense</i> yang Terintegrasi Dengan <i>Services Suricata</i>	53
BAB IV. HASIL DAN ANALISA		55
4.1.	Pembahasan	55
4.2.	Data Hasil Ekstraksi	55
4.3.	Analisa Dataset	56
4.4.	Data Hasil Ekstraksi	57
4.5.	Pengenalan Pola Serangan pada <i>Ransomware Wannacry</i>	58
4.6.	Pola serangan <i>ransomware wannacry</i>	58
4.7.	Pengujian mode IDS (<i>Instrusion Detection System</i>) pada <i>Snort</i>	59
4.8.	Pengujian mode IPS (<i>Instrusion Prevention System</i>) <i>opsense</i>	60
4.9.	Pencocokan pola pada <i>payload</i> serangan <i>ransomware wannacry</i> menggunakan <i>String Matching</i>	63
4.10.	Tingkat Keberhasilan Yang Didapatkan pada Sistem Deteksi <i>Snort</i> ...	64
4.11.	Tingkat Keberhasilan Pencegahan pada Sistem <i>Opsense</i> Yang Terintegrasi Dengan <i>Suricata</i>	64
4.12.	Perhitungan Confussion Matrix pada String-Matching	67
4.13.	Varian <i>ip address</i> berbeda pada skenario serangan percobaan sendiri	65
BAB V. KESIMPULAN DAN SARAN		67
5.1.	Kesimpulan (Sementara)	67
5.2.	Saran	67
DAFTAR PUSTAKA		68

DAFTAR GAMBAR

	Halaman
Gambar 1.1 Kerangka alur metodologi penelitian	4
Gambar 2.1 Model Sistem Pencegahan atau IPS	7
Gambar 2.2 Model Jaringan HIPS	9
Gambar 2.3 Model dari mode <i>in line</i> pada Sistem Pencegahan Berbasis Jaringan	10
Gambar 2.4 Model Pada Mode Pasif di <i>network</i> Sistem Pencegahan Berbasis Jaringan	11
Gambar 2.5 Model sistem pencegahan pada <i>wireless</i>	12
Gambar 2.6 Arsitektur Jaringan <i>Network Behavior Analysis</i>	13
Gambar 2.7 Pengelompokan <i>Malicious software</i>	16
Gambar 2.8 Skenario <i>symmetrical cryptosystem ransomware</i>	27
Gambar 2.9 Skenario <i>asymmetrical cryptosystem ransomware</i>	28
Gambar 2.10 Pesan yang ditampilkan oleh WannaCry2	29
Gambar 2.11 Skenario <i>EternalBlue</i>	30
Gambar 2.12 Gambaran cara kerja pada algoritma <i>string matching</i>	30
Gambar 2.13 Cara kerja <i>snort</i>	33
Gambar 2.14 Cara kerja <i>Suricata</i>	35
Gambar 3.1 Kerangka Kerja Penelitian	37
Gambar 3.2 Skenario pada <i>dataset unvarra</i>	40
Gambar 3.3 Skenario pada pengambilan <i>dataset</i>	41
Gambar 3.4 Konfigurasi tambahan pada <i>port</i> di <i>snort.conf</i>	42
Gambar 3.5 <i>Rule</i> untuk mendeteksi <i>wannacry</i> pada <i>snort</i>	43

Gambar 3.6 Memberikan akses pada direktori <i>thezoo</i>	43
Gambar 3.7 Menjalankan <i>tools thezoo</i>	43
Gambar 3.8 Isi dari seluruh <i>library thezoo</i>	44
Gambar 3.9 Daftar urutan <i>ransomware wannacry</i>	44
Gambar 3.10 Mendapatkan atau mengunduh <i>ransomware wannacry</i> pada <i>thezoo</i>	44
Gambar 3.11 Pencarian kerentanan menggunakan <i>eternalblue doublepulsar</i> .	45
Gambar 3.12 Mengatur letak direktori dari <i>eternalblue</i> dan <i>doublepulsar</i>	45
Gambar 3.13 Mengatur tipe <i>payload</i> yang akan digunakan	45
Gambar 3.14 Mengatur tipe arsitektur yang digunakan	45
Gambar 3.15 Menyelipkan <i>payload</i> pada proses yang berjalan	45
Gambar 3.16 Menentukan <i>ip address</i> korban	45
Gambar 3.17 Menentukan <i>ip address</i> target	46
Gambar 3.18 Nomor urut target	46
Gambar 3.19 <i>Dataset wireshark</i> yang berisi <i>wannacry</i>	47
Gambar 3.20 <i>Command</i> untuk <i>snort</i>	47
Gambar 3.21 Fungsi <i>command snort</i>	47
Gambar 3.22 <i>Alert</i> yang didapat pada <i>snort</i>	47
Gambar 3.23 <i>Dataset wireshark</i> yang telah diekstraksi	48
Gambar 3.24 Hasil <i>alert</i> divalidasi dengan <i>dataset</i> dan <i>pcap</i>	48
Gambar 3.25 <i>Pseudocode</i> program <i>string matching</i>	49
Gambar 3.26 Hasil dari program pencarian <i>string matching</i>	50
Gambar 3.27 Pemberian akses eksekusi pada program	50
Gambar 3.28 <i>Source Code</i> dari program <i>string matching</i>	51

Gambar 3.29 Validasi antara <i>raw data (pcap)</i> dan <i>log</i> hasil dari <i>string matching</i>	52
Gambar 3.30 Suricata firmware pada opnsense	53
Gambar 3.31 Konfigurasi pada opnsense	54
Gambar 3.32 Rules wannacry pada suricata	54
Gambar 4.1 Data Hasil Ekstraksi Sebelum dikenali pola serangan	55
Gambar 4.2 Data Hasil Ekstraksi Setelah dikenali pola serangan	56
Gambar 4.3 Validasi dataset <i>unvarra</i> hasil ekstraksi berdasarkan <i>raw data</i> , <i>csv</i> dan <i>alert</i>	57
Gambar 4.4 Gambar diatas menggunakan perbandingan <i>csv</i> dan <i>alert snort</i> ..	58
Gambar 4.5 Data Hasil <i>Feature Extraction Dataset Serangan</i>	59
Gambar 4.6 Kecocokan antara <i>rules</i> dan <i>alert</i>	60
Gambar 4.7 Log pada Suricata	61
Gambar 4.8 Log detail pada Suricata	61
Gambar 4.9 Validasi alerts dan rules	62
Gambar 4.10 Pencarian Pola menggunakan String Matching	63

DAFTAR TABEL

	Halaman
Tabel 2.1 Jenis – jenis parameter pada <i>Confussion Matrix</i>	14
Tabel 2.2 List dari <i>ransomware famillies</i> berdasarkan fitur, metode pembayaran, tipe enkripsi dan jenis <i>platform-</i> nya	19
Tabel 3.1 Daftar Ransomware yang terdapat di <i>dataset</i>	28
Tabel 3.2 Tabel Spesifikasi <i>Hardware</i> atau Perangkat Keras	29
Tabel 3.3 Informasi dari kebutuhan <i>Software</i> atau Perangkat Lunak	30
Tabel 4.1 Detail Jumlah Paket Berdasarkan Tipe Protokol	39
Tabel 4.2 Hasil Pengujian <i>Snort IDS</i>	42

BAB I. PENDAHULUAN

1.1. LATAR BELAKANG

Wannacry ransomware terdapat banyak sebutan sebagai contohnya (*Wanna decrypt0r*, *WannaCry*, *WannaCrypt0r*, *Wcry*) telah menjadi perhatian semenjak penyerangan pada beberapa negara pada tanggal 12 Mei 2017 [1]. Semenjak banyaknya laporan dengan total 300.000 sistem di 150 negara telah mengalami banyaknya kerugian dari beberapa *vendors*, serangan *wannacry* tidak hanya telah menginfeksi dalam skala kecil, tetapi juga termasuk Pemerintahan, Bidang Kesehatan, Telekomunikasi dan Produksi Gas / Minyak.

Ransomware dibuat untuk memblokir akses korban terhadap data mereka dan memeras korban dengan harus melakukan pembayaran uang atau sebagai tebusan untuk membuka akses kembali data atau *file* korban. *Ransomware* hadir dalam berbagai bentuk, misalnya mengunci layar pada sebuah perangkat atau perangkat lunak yang berbasis kriptografi yang mengenkripsi *file* target atau korban dengan algoritma kriptografi canggih. Namun sistem yang sudah ada mencoba mengatasi anomali ransomware tersebut dengan melakukan secara reaktif, yaitu dengan mengambil dan menyediakan sebuah sampel. Dari data yang telah teridentifikasi [2].

Sistem pencegahan anomali atau gangguan pada sebuah jaringan atau (IPS), suatu sistem pencegahan maupun deteksi yang acapkali digunakan pada sebuah jaringan atau *network* yang terhubung pada komputer secara lokal maupun non lokal. Pada sebuah mode pencegahan atau *intrusion* atau (IPS) menerapkan sebuah aturan maupun *rule* yang digunakan untuk anomali atau sebuah serangan yang dapat masuk melalui sebuah jaringan secara sah ataupun tidak sah, dengan mencocokkan antara aturan atau *rule* yang diatur berdasarkan *sid* atau *signature id*. Untuk cara kerja sistem pencegahan ini sendiri adalah dengan cara melakukan akses blok atau membuang berdasarkan paket yang telah dikenali oleh sistem tersebut. Pada sistem ini dapat melakukan aksi atau tindakan selayaknya sebuah dinding api atau *firewall* [3].

Tujuan para pelaku yang berperan sebagai penyerang mirip pelaku kejahatan di dunia nyata, hanya untuk mengambil keuntungan yang. Dengan

demikian banyak cara yang dilakukan oleh seorang penyerang, salah satunya adalah dengan pendekatan yang menghasilkan sebuah keuntungan. *Attacker* atau penyerang menjual *tools*, yang digunakan untuk eksploitasi dan menginfeksi korban dengan cara *drive – by – download*, mereka beroperasi secara *exploit-as-a-service* yaitu membangun dan menyewakan *botnet*. Bahkan menawarkan sebuah jasa pembuatan bot dan menjual bot atau sebuah virus disusun bagaikan buku dalam rak [2].

Dalam menggunakan sebuah metode *string matching* diperlukannya sebuah data yang diambil pada *traffic*, yang salah satu komputer tersebut telah diserang oleh *ransomware wannacry*. Pengambilan data tersebut dibutuhkan sebuah *intrusion prevention system (IPS)* adalah suatu bentuk keamanan jaringan yang berfungsi untuk mendeteksi dan mencegah ancaman yang datang pada sebuah jaringan. *Intrusion prevention system (IPS)* akan secara terus-menerus memonitor jaringan ada, mencari kemungkinan insiden berbahaya dan menangkap informasi tentangnya. IPS melaporkan peristiwa ini kepada administrator sistem dan mengambil tindakan pencegahan, seperti menutup titik akses dan mengonfigurasi *firewall* untuk mencegah serangan di masa depan [4].

Pada tugas akhir ini akan membahas bagaimana *string matching* digunakan dalam melakukan identifikasi serangan *ransomware wannacry* pada sebuah jaringan, dengan memanfaatkan sebuah *log* yang didapatkan dari *SNORT* dan *log* itulah yang akan di olah *string matching*.

1.2. TUJUAN

Berikut beberapa tujuan yang dapat dicapai dipembuatan tugas akhir ini adalah:

1. Mendeteksi *ransomware wannacry* menggunakan *SNORT*.
2. Melakukan *drop packet* untuk melakukan pecegahan pada serangan *ransomware*.

1.3. MANFAAT

Terdapat juga manfaat dari tugas akhir ini yang akan dilakukan, adalah :

1. Dapat memahami cara kerja dari *ransomware wannacry*.
2. Dapat melihat akurasi yang didapatkan dari *SNORT*.

1.4. RUMUSAN MASALAH

Berdasarkan latar belakang permasalahan utama yang akan di bahas didalam pembuatan tugas akhir ini adalah Bagaimana mencegah sebuah serangan *wannacry* pada komputer yang telah tertargetkan?

1.5. BATASAN MASALAH

Terdapat beberapa aspek pada batasan yaitu:

1. Dalam pengambilan data anomali *ransomware wannacry* harus dalam satu jaringan lokal.
2. Penyerangan bisa dilakukan bila *firewall* korban mati.
3. Tidak menggolongkan jenis selain dari serangan *ransomware wannacry*.

1.6. METODOLOGI PENELITIAN

Supaya tujuan pada penelitian ini dapat tercapai berikut tahap - tahapan yang harus dilewati yaitu :

1. Tahap pertama (Studi Pustaka / *Literature*)

Untuk Tahap awal ini dengan mencari sebuah agar sesuai maupun relevan. Kemudian, mencari data dari berbagai sumber, dan dapat dicari dalam sebuah journal, buku, artikel pada website berkaitan ataupun berhubungan dengan pada tugas akhir.

2. Tahap kedua (Perancangan Sistem)

Tahap kedua ini adalah untuk mencari cara untuk menerapkan sebuah metode dan membangun rancangan sistem pada penelitian ini. Dan mencari tahu apa saja yang akan digunakan dalam hal perangkat lunak maupun perangkat keras atau *hardware* agar dapat diterapkan pada *methode* atau metode pada penelitian ini.

3. Tahap Ketiga (Pengetesan)

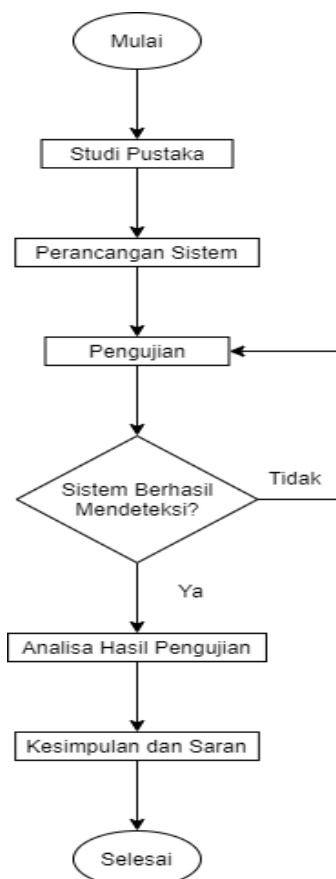
Tahap ketiga ini adalah tahap yang selanjutnya dari perancangan sistem, dimana akan dilakukan sebuah pengujian berdasarkan metode penelitian dan dilakukan sebuah perbandingan dengan riset sebelum untuk mendapatkan sebuah perolehan dengan konsep yang dirancang.

4. Tahap Keempat (Analisa)

Untuk tahap ini dilakukan sebuah pengalisan pada hasil maupun data yang dihasilkan melalui beberapa pengetsan melalui penerapan tertentu, guna menghasilkan hal yang rasional.

5. Tahap kelima (Kesimpulan dan Saran)

Untuk tahap ini dapat diambil ataupun ditarik sebuah kesimpulan dengan cara menganalisa beberapa studi *literature*, serta memberikan sebuah saran agar dapat dijakdikan oleh penulis penelitian selanjutnya.



Gambar 1.1 Kerangka alur metodologi penelitian

1.7. SISTEMATIKA PENULISAN

Dalam memberikan kemudahan di penulisan penelitian atau tugas akhir ini, maka diberikan beberapa susunan tugas akhir dan dapat memberikan penjelasan singkat pada masing – masing bab. Sebagai berikut :

BAB 1. PENDAHULUAN

Bab terdapat beberapa penjelasan secara analitis tentang informasi dari penelitian yang termasuk dalam latar belakang, tujuan, manfaat, rumusan dan batasan masalah.

BAB II. TINJAUAN PUSTAKA

Pada tahap ini berisi dasar – dasar teori atau tinjauan pustaka yang terdapat pada penelitian sebelumnya terkait dengan *Ransomware, IDS, string matching*.

BAB III. METODOLOGI PENELITIAN

Pada tahap ini menerangkan dengan *systematic*, bagaimana process penelitian dilakukan. Untuk menerangkan pada bab ini terdapat beberapa tahapan perancangan system dan pengimplementasian penelitian.

BAB IV. HASIL DAN ANALISA

Pada tahap ini akan menerangkan hasil dari pengetesan yang dilakukan dan memberikan analysis tiap pada data atau informasi yang didapat pada pengetesan.

BAB V. KESIMPULAN

Pada tahap ini memiliki berisi tentang ikhtisar pada tugas akhir ini, dan menjawab dari tujuan yang ingin dituju pada bab 1 pendahulaun

DAFTAR PUSTAKA

- [1] M. Akbanov, V. G. Vassilakis, and M. D. Logothetis, “WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms,” *J. Telecommun. Inf. Technol.*, 2019.
- [2] E. Kolodenker, W. Koch, G. Stringhini, and M. Egele, “Paybreak: Defense against cryptographic ransomware,” in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, 2017, pp. 599–611.
- [3] D. Stiawan, A. H. Abdullah, and M. Y. Idris, “The trends of intrusion prevention system network,” in *2010 2nd International Conference on Education Technology and Computer*, 2010, vol. 4, pp. V4--217.
- [4] E. Ukkonen, “Approximate string-matching with q-grams and maximal matches,” *Theor. Comput. Sci.*, vol. 92, no. 1, pp. 191–211, 1992, doi: 10.1016/0304-3975(92)90143-4.
- [5] Y. Chi, T. Jiang, X. Li, and C. Gao, “Design and implementation of cloud platform intrusion prevention system based on SDN,” in *2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA)*, 2017, pp. 847–852.
- [6] P. J. Taylor, T. Dargahi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, “A systematic literature review of blockchain cyber security,” *Digit. Commun. Networks*, vol. 6, no. 2, pp. 147–156, 2020.
- [7] D. Sequeira, “Intrusion Prevention Systems: Security’s Silver Bullet?,” pp. 36–41, 2003.
- [8] M. Syarif, “Implementasi Algoritma String Matching Dalam Pencarian Surat Dan Ayat Dalam Al-Quran Berbasis Web,” *Indones. J. Netw. Secur.*, vol. VI, no. 2, pp. 70–76, 2017, doi: 10.1096/fj.04-2774fje.
- [9] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention

systems (idps),” 2012.

- [10] 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,” in *2018 6th International Conference on Information and Communication Technology (ICoICT)*, 2018, pp. 299–304.
- [11] P. S. Kenkre, A. Pai, and L. Colaco, “Real time intrusion detection and prevention system,” in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, 2015, pp. 405–411.
- [12] A. S. Desai and D. P. Gaikwad, “Real time hybrid intrusion detection system using signature matching algorithm and fuzzy-GA,” in *2016 IEEE international conference on advances in electronics, communication and computer technology (ICAECCT)*, 2016, pp. 291–294.
- [13] R. Adenansi and L. A. Novarina, “Malware dynamic,” *JoEICT (Journal Educ. ICT)*, vol. 1, no. 1, 2017.
- [14] M. Sikorski and A. Honig, *Practical malware analysis: the hands-on guide to dissecting malicious software*. no starch press, 2012.
- [15] D. Patel, “Mining Ransomware Signatures from Network Traffic,” 2018.
- [16] S. Aurangzeb, M. Aleem, M. A. Iqbal, M. A. Islam, and others, “Ransomware: a survey and trends,” *J. Inf. Assur. Secur.*, vol. 6, no. 2, pp. 48–58, 2017.
- [17] A. O. Almashhadani, M. Kaiiali, S. Sezer, and P. O’Kane, “A multi-classifier network-based crypto ransomware detection system: a case study of Locky ransomware,” *Ieee Access*, vol. 7, pp. 47053–47067, 2019.
- [18] E. A. Winanto, A. Heryanto, and D. Stiawan, “Visualisasi Serangan Remote to Local (R2L) Dengan Clustering K-Means,” *Annu. Res. Semin.*, vol. 2, no. 1, pp. 359–362, 2016.

- [19] M. Bharati and S. Tamane, “Defending against bruteforc attack using open source—SNORT,” in *2017 International Conference on Inventive Computing and Informatics (ICICI)*, 2017, pp. 903–907.
- [20] G. D. Kurundkar, N. A. Naik, and S. D. Khamitkar, “Network intrusion detection using Snort,” *Int. J. Eng. Res. Appl.*, vol. 2, no. 2, pp. 1288–1296, 2012.
- [21] E. Stephani, F. Nova, and E. Asri, “Implementasi dan Analisa Keamanan Jaringan IDS (Intrusion Detection System) Menggunakan Suricata Pada Web Server,” *JITSI J. Ilm. Teknol. Sist. Inf.*, vol. 1, no. 2, pp. 67–74, 2020.
- [22] F. Ferdiansyah, “ANALISIS AKTIVITAS DAN POLA JARINGAN TERHADAP ETERNAL BLUE DAN WANNACRY RANSOMWARE,” *JUSIFO (Jurnal Sist. Informasi)*, vol. 2, no. 1, pp. 44–59, 2018.