JOISIE Journal Of Information System And Informatics Engineering
Vol. 5, No.1 Juni 2021, Hlm 1-8

p- ISSN: 2503-5304
e- ISSN: 2527-3116

SISTEM PENDETEKSIAN SERANGAN JARINGAN LOCAL AREA NETWORK (LAN) MENGGUNAKAN ALGORITMA NAIVE BAYES

Dwi Haryono [1)], Yulli Zulianda [2)], Wirta [3)], Lusiana [4)]
[1] Sistem Informasi, STMIK Amik Riau, Jl. Purwodadi Indah
[2] Teknik Informasi, STMIK Amik Riau, Jl. Purwodadi Indah
[3] Sistem Informasi, STMIK Amik Riau, Jl. Purwodadi Indah
[4] Teknik Informasi, STMIK Amik Riau, Jl. Purwodadi Indah
e-mail: [1] dwiharyono@stmik-amik-riau.ac.id, [2] YulliZulianda@stmik-amik-riau.ac.id, [3] wirtaagustin@stmik-amik-riau.ac.id, [4] Lusiana@stmik-amik-riau.ac.id

Abstract

Local Area Network (LAN) is a network that is used with a scale limited to the scope of space, buildings and a maximum distance of one kilometer working intranet. The interconnection of computer interfaces with one another in systems and applications makes it easier to help work but also has an impact on increasing types intrusion or attacks against LAN users. LANs are increasing exponentially increasing interruptions or attacks by crackers exploiting weaknesses in Internet protocols, operating systems and application software. attempts to identify an intruder who has entered the system without authorization by a cracker or a legitimate user but is abusing system resource privileges. So it is necessary to detect a LAN network attack. The method used is the Naive Bayes Algorithm. Its purpose is to help computer systems deal with network attacks and detect network attack intrusions.

Keywords: Naive Bayes, LAN, Cracker

Abstrak

Lokal Area Network (LAN) merupakan jaringan yang di gunakan dengan skala terbatas pada ruang lingkup ruang, gedung dan maksimal jarak satu kilometer bekerja secara intranet.terkoneksinya antarmuka komputer satu dengan yang lain secara sistem dan aplikasi memudahkan dalam membantu pekerjaan namun juga berdampak pada meningkatnya jenis gangguan atau serangan terhadap pengguna LAN. LAN yang meningkat secara eksponensial meningkatkan juga gangguan atau serangan yang dilakukan oleh cracker dalam mengeksploitasi kelemahan pada protokol internet, sistem operasi dan software aplikasi. usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi oleh cracker atau seorang user yang sah tetapi menyalahgunakan privilege sumberdaya sistem. Sehingga perlu dilakukan pendekteksian serangan jaringan LAN. Metode yang digunakan Algoritma Naive Bayes. Tujuan adalah membantu sistem komputer untuk menangani serangan jaringan dan mendeteksi gangguan serangan jaringan.

Kata Kunci : Naive Bayes, LAN, Cracker

1. PENDAHULUAN

Komunikasi berbasiskan teknologi jaringan komputer merupakan teknologi yang sudah banyak digunakan. (Informatika et al., 2014). Komunikasi pada jaringan komputer, menggunakan aturan komunikasi yang sesuai dikenal dengan nama network protocol. (Haryono et al., 2020). Penggunaan jaringan komputer yang meningkat secara eksponensial meningkatkan juga gangguan atau serangan yang dilakukan oleh cracker mengeksploitasi kelemahan pada protokol jaringan,(Rosid, 2020). sistem operasi dan software aplikasi. Gangguan atau serangan terhadap jaringan komputer khususnya internet mengalami peningkatan dari tahun ke tahun. (Susanti & Putri, 2020)

Kebutuhan akan jaringan khususnya internet merupakan suatu kebutuhan yang tidak akan bisa dilepaskan dari kegiatan sehari-hari baik dari kegiatan pendidikan hingga kegiatan diperusahaan baik instansi pemerintahan maupun swasta. (Nawawi et al., 2019). Dengan besarnya

kebutuhan data dan informasi yang dapat di akses secara *online* tentunya kebutuhan untuk menyediakan sistem keamaan jaringan juga sangat diperlukan, dan sebelum menyediakan sistem keamanan jaringan yang tepat tentunya diperlukan tindakan untuk mengindentifikasi gangguan atau serangan apa yang sedang terjadi dalam sebuah jaringan komputer, bagaimana mengatasinya, serta gejala yang ditimbulkan dari gangguan atau serangan tersebut. (Nawawi et al., 2019)

Ada banyak sekali gangguan atau serangan jaringan komputer, salah satu diantaranya adalah *Spoofing, DdoS, DNS Poisoning, Trojan House, Sniffer, SQL Injection, Cross Site Scripting, Phising, Malware, Worm*. (Adi, 2018). Tanpa izin bahkan pengambil alihan sistem kendali terhadap sebuah perangkat komputer. Jenis gangguan atau serangan juga dapat berkembang semakin luas seiring dengan perkembangan teknologi.(Mafakhir & Solichin, 2020)

Dari permasalahan tersebut maka perlunya sebuah sistem yang dapat mendeteksi gangguan atau serangan jaringan berdasarkan gejala yang ditimbulkan. (Manalu et al., 2017). Penerapan *Algoritma Naive Bayes* pada sistem pendeteksi gangguan atau serangan tersebut juga dapat membantu dalam pengambilan keputusan yang digunakan untuk menyediakan sistem keamanan yang sesuai.(Firdaus & Mukhlis, 2020) *Naive Bayes* merupakan *algoritma* yang menggunakan pendekatan statistik dalam mengambil keputusan sehingga dapat dikatakan naive bayes merupakan algoritma yang sangat sesuai jika diterapkan pada sistem pendeteksi gangguan atau serangan jaringan**.**(Ahmad & No, n.d.)

2. METODE PENELITIAN

Menurut (Setiawan, & Ratnasari, 2015) *Naive Bayes Classifier* merupakan pengklasifikasi probabilitas sederhana berdasarkan pada teorema Bayes. Teorema Bayes dikombinasikan dengan "*Naive*" yang berarti setiap atribut/variabel bersifat bebas (*independent*). *Naive Bayes Classifier* dapat dilatih dengan efisien dalam pembelajaran terawasi *(supervised learning)*. Keuntungan dari klasifikasi adalah bahwa ia hanya membutuhkan sejumlah kecil data pelatihan untuk memperkirakan parameter (sarana dan varians dari variabel) yang diperlukan untuk klasifikasi. Karena variabel independen diasumsikan, hanya variasi dari variabel untuk masing-masing kelas harus ditentukan, bukan seluruh matriks kovarians.

Dalam prosesnya, *Naive Bayes Classifier* mengasumsikan bahwa ada atau tidaknya suatu *fitur* pada suatu kelas tidak berhubungan dengan ada atau tidaknya *fitur* lain di kelas yang sama. Pada saat klasifikasi, pendekatan bayes akan menghasilkan label kategori yang paling tinggi probabilitasnya (V_{MAP}) dengan masukan atribut $a_1, a_2, a_3, \ldots, a_n$.

$$V_{MAP} = \text{argmax}_{vjev} P(V_j | a_1, a_2, a_3, \ldots, a_n)$$

Dimana :

V_{MAP} = Probabilitas tertinggi.

$a_1, a_2, a_3, \ldots, a_n$ = Atribut (Inputan)

Teorema Bayes Menyatakan :

$$P(B|A) = \frac{P(A|B)P(B)}{P(A)}$$

Dimana :

P(B|A) = Peluang B jika diketahui keadaan jenis penyakit mata A.

P(B|A) = Peluang *evidence* A jika diketahui hipotesis B.

P(B) = Probabilitas hipotesis B tanpa memandang evidence apapun.

P(A) = Peluang evidence penyakit mata A.

Menggunakan teorema Bayes ini, dapat ditulis sebagai berikut

$$V_{MAP} = \text{argmax}_{vjev} \frac{P(V_j | a_1, a_2, a_3, \ldots, a_n) p(V_j)}{P(V_j | a_1, a_2, a_3, \ldots, a_n)}$$

Dimana :

V_{MAP} = Probabilitas tertinggi.

$V(v_j)$ = Peluang jenis penyakit mata

$P(a_1,a_2,a_3,\ldots,a_n|v_j)$ = Peluang atribut-atribut (inputan) jika diketahui keadaan v_j

$P(a_1,a_2,a_3,\ldots,a_n)$ = Peluang atribut-atribut (inputan)

Karena nilai $P(a_1,a_2,a_3,\ldots,a_n)$ nilainya konstan untuk semua v_j sehingga persamaan ini dapat ditulis :

$$V_{MAP} = \text{argmax}_{vjev} P(V_j | a_1, a_2, a_3, \ldots, a_n) p(V_j)$$

Untuk menghitung $P(a_1,a_2,a_3,\ldots,a_n|v_j)$ semakin sulit karena jumlah gejala $P(a_1,a_2,a_3,\ldots,a_n|v_j)$ bisa jadi sangat besar. Hal ini disebabkan jumlah gejala tersebut sama dengan jumlah semua kombinasi gejala dikali dengan

jumlah kategori yang ada.

Perhitungan *Naive bayes classifier* adalah :

Menghitung P(ai|vj) dengan rumus :

$$P(a_i|v_j) = \frac{n_c + n.p}{n + m}$$

Dimana :

n_c = jumlah kelas pada data v = v_j dan a = a_i

p = 1/ banyaknya jenis kelas / penyakit

m = jumlah parameter / gejala

n = jumlah kelas pada data v = v_j / tiap kelas

Tahapan-tahapan *Algoritma Naive Bayes* sebagai berikut :

1. Menentukan nilai n_c untuk setiap *class*
2. Menghitung nilai P (a_i | v_j) dan menghitung nilai P (v_j)
3. Menghitung P(ai|vj) x P(vj) untuk tiap v
4. Menentukan hasil klasifikasi yaitu v yang memiliki hasil perkalian yang terbesar.

3. HASIL DAN PEMBAHASAN

Pada proses analisa *Algoritma Naive Bayes*penulis menggunakan *sample* data yang didapat dari bagian teknisi kampus STMIK Amik Riau dan quisoner yang disebarkan kepada mahasiswa, hal ini bertujuan untuk melakukan perbandingan antara sistem yang dibangun dengan proses perhitungan secara manual. Dimana dalam proses perhitungan manual ini penulis akan menggunakan sample data bentuk serangan jaringan dan identifikasi terhadap serangan jaringan yang pernah terjadi. Dimana untuk data serangan jaringan dapat dilihat pada tabel 1 berikut.

Tabel 1.Nama Serangan Jaringan Komputer

No	Kode	Nama Serangan
1	S100	Spoofing
2	S101	Ddos (Distributed Denial of Service)
3	S102	DNS Poisoning
4	S103	Trojan Horse
5	S104	Sniffer
6	S105	SQL Injection
7	S106	Cross Scripting
8	S107	Phising
9	S108	Malware
10	S109	Worm

Berikut data identifikasi terhadap serangan yang digunakan indikator dalam proses data dapat dilihat pada tabel 2 berikut :

Tabel 2. Bentuk Identifikasi Terhadap Serangan Jaringan

No	Kode	Bentuk Identifikasi Serangan
1	I100	Serangan teknis yang rumit yant terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yangbekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain.
2	I101	Mengambil nama DNS dari sistem lain dengan membahayakan domain name server suatu domain yang sah.
3	I102	Tindakan penyusupan dengan menggunakan identitas resmi secara ilegal.
4	I103	Akses ke situs web diarahkan melalui sebuah proxy server.
5	I104	Melibatkan sebuah server web yang dimiliki penyerang yang diletakkan pada internet antara pengguna dengan WWW.
6	I105	Seseorang menaruh link yang palsu (yang sudah di-hack) pada halaman web yang populer.
7	I106	Kita menggunakan search engine (mesin pencari, seperti Yahoo, Alta Vista, Goggle) untuk mendapatkan link dari topik yang ingin dicari. Tanpa kita ketahui, beberapa dari link ini telah diletakkan oleh hacker yang berpura-pura menjadi orang lain.
8	I107	Server penyerang memberikan versi halaman yang sudah ditulis-ulang kepada pengguna.
9	I108	Membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan.
10	I109	Server atau keseluruhan segmen jaringan menjadi “tidak berguna sama sekali” bagi client.
11	I110	Serangan di dilancarkan dengan menggunakan utility ping pada sebuah sistem operasi.
12	I111	Alamat IP penyerang biasanya telah disembunyikan atau spoofed sehingga alamat yang dicatat oleh target adalah alamat yang salah.
13	I112	Penerima akan bingung untuk menjawab permintaan koneksi TCP yang baru karena masih menunggu banyaknya balasan ACK dari pengirim yang tidak diketahui tersebut.

No	Kode	Bentuk Identifikasi Serangan
14	I113	Mengendalikan beberapa network lain untuk menyerang target.
15	I114	Sejumlah paket data yang besar dikirimkan begitu saja kepada korban.
16	I115	Melambatkan dan memadatkan trafik di jaringan.
17	I116	Mengacaukan DNS Server asli agar pengguna Internet terkelabui untuk mengakses web site palsu yang dibuat benar-benar menyerupai aslinya tersebut.
18	I117	Meng-install software secara otomatis.
19	I118	Terjadi pencurian data.
20	I119	Upload dan Download file secara otomatis.
21	I120	Terjadinya modifikasi file atau data.
22	I121	Membuang-buang space komputer.
23	I122	Terjadi suatu kegiatan penyadapan tanpa merubah data atau paket apapun di jaringan.
24	I123	Terjadi perubahan paket data dalam jaringan.
25	I124	Terjadinya pengambil alihan server.
26	I125	Terjadinya pencurian password komputer.
27	I126	Menghentikan layanan yang diberikan oleh server sehingga terjadi gangguan terhadap layanan atau jaringan komputer.
28	I127	Mencoba mendapatkan informasi seperti username, password, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik.
29	I128	Server akan mengalami down.
30	I129	Terjadinya pengrusakan file atau berkas.

Serangan jaringan Local Area Network (LAN) memiliki bentuk identifikasi masing-masing. Serangan dan bentuk identifikasinya ditunjukkan pada Tabel 3 berikut :

Tabel 3. Serangan dan bentuk identifikasinya

Jenis Serangan	Identifikasi Serangan no-
Spoofing	1,3,12,17
Ddos (Distributed Denial of Service)	9,10,13,15,29
DNS Poisoning	2,4,8
Trojan Horse	7,10,11,16,19,29,30
Sniffer	3,5,6,28
SQL Injection	19,22,26,29
Cross Scripting	1,8,17,20,24
Phising	6,7,14,18,20
Malware	16,21,23,25,27
Worm	9,12,18,22,24,28

Uji coba dilakukan dengan mendapatkan data berdasarkan bentuk dari identifikasi serangan jaringan 12 pengguna. Data bentuk identifikasi serangan jaringan dibandingkan dengan data bentuk identifikasi yang menyebabkan serangan jaringan tertentu.

Contoh perhitungan dengan menggunakan klasifikasi Naïve Bayes Classifier dapat diterapkan pada pengguna ke-1 mengalami bentuk identifikasi serangan nomor 18,22,24 dan 26.

Keterangan gejala :

1. Meng-install *software* secara otomatis.
2. Membuang-buang space komputer.
3. Terjadi perubahan paket data dalam jaringan.
4. Terjadinya pencurian *password* komputer.

Langkah-langkah perhitungan Naive Bayes Classifier sebagai berikut :

1. Menentukan nilai n_c untuk setiap class

Jenis Serangan ke-1 : Spoofing

n = 1
p = 1/10 = 0.1
m = 30
18. $n_c = 0$
22.$n_c = 0$
24.$n_c = 0$
26.$n_c = 0$

Jenis Seranganke-2 : Ddos (Distributed Denial of Service)

n = 1
p = 1/10 = 0.1
m = 30
18. $n_c = 0$
22.$n_c = 0$
24.$n_c = 0$
26.$n_c = 0$

Jenis Seranganke-3 : DNS Poisoning

n = 1
p = 1/10 = 0.1
m = 30
18. $n_c = 0$

22.n_c = 0
24.n_c = 0
26.n_c = 0

dan seterusnya hingga jenis serangan ke 10

2. **Menghitung nilai P (ai|vj) dan menghitung nilai P (vj)**

Jenis Seranganke-1. Spoofing

P(18|S) = 0 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(22|S) = 0 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(24|S) = 0 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(26|S) = 0 + 30 x0.1 / 1 + 30= 0,0967741935483871
P(S) = 1/10 = 0.1

Jenis Serangan ke-2. Ddos (Distributed Denial of Service)

P(18|DD) = 1 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(22|DD) = 0 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(24|DD) = 1 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(26|DD) = 0 + 30 x0.1 / 1 + 30= 0,0967741935483871
P(DD) = 1/10 = 0.1

Jenis Seranganke-3. DNS Poisoning

P(18|DP) = 0 + 30x 0.1 / 1 + 30=0,0967741935483871
P(22|DP) = 0 + 30 x 0.1 / 1 + 30= 0,0967741935483871
P(24|DP) = 0 + 30 x0.1 / 1 + 30= 0,0967741935483871
P(26|DP) = 0 + 30 x0.1 / 1 + 30= 0,0967741935483871
P(DP) = 1/10 = 0.1

dan seterusnya hingga jenis serangan ke 10

3. **Menghitung $P(a_i|v_j)$ x $P(v_j)$ untuk tiap v**

Jenis Seranganke-1, Spoofing

P(S) x [P(18|S) x P(22|S) x P(24|S) x P(26|S)]
= 0.1 x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871
= 8,80780524E-05

Jenis Seranganke-2, Ddos (Distributed Denial of Service)

P(DD) x [P(1|DD) x P(4|DD) x P(5|SO) x P(6|DD)]
= 0.1 x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871
= 8,80780524E-05

Jenis Seranganke-3, DNS Poisoning

P(DP) x [P(1|DP) x P(2|DP) x P(4|DP) x P(5|DP) x P(6|DP)]
= 0.1 x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871x 0,0967741935483871
= 8,80780524E-05

dan seterusnya hingga jenis serangan ke 10

4. **Menentukan hasil klasifikasi yaitu v yang memiliki hasil perkalian yang terbesar.**

Hasil v yang memiliki perkalian terbesar didapatkan pada Tabel 4 berikut :

Tabel 4. Perbandingan Nilai V Hasil Klasifikasi Sample

Penyakit	Nilai v
Spoofing	8,77078E-05
Ddos (Distributed Denial of Service)	8,77078E-05
DNS Poisoning	8,77078E-05
Trojan Horse	8,77078E-05
Sniffer	8,77078E-05
SQL Injection	0,000155925
Penyakit	**Nilai v**
Cross Scripting	0,000116944
Phising	0,000116944
Malware	8,77078E-05
Worm	**0,000207899**

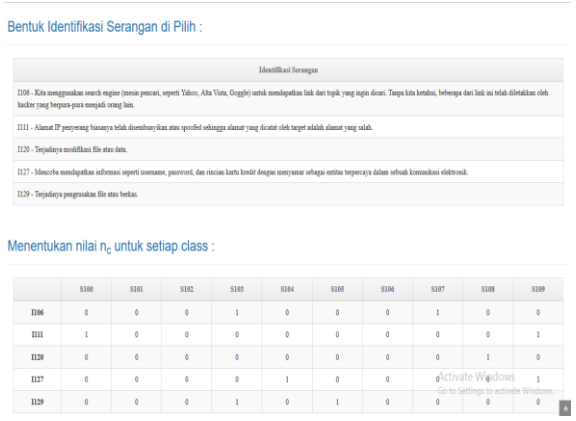
Karena nilai **0,000207899** paling besar, maka contoh kasus penggunake-1 diklasifikasikan sebagai jenis serangan **Worm**.

Tampilan Hasil Perhitungan Algoritma Naive Bayes merupakan halaman yang tampil saat pengguna meng-klik button proses pada Halaman Konsultasi Pakar.

Jenis Serangan Jaringan :

Jenis Serangan
S100 - Spoofing
S101 - Ddos (Distributed Denial of Service)
S102 - DNS Poisoning
S103 - Trojan Horse
S104 - Sniffer
S105 - SQL Injection
S106 - Cross Scripting
S107 - Phising
S108 - Malware
S109 - Worm

Gambar 2. Klasifikasi Jenis Serangan



Bentuk Identifikasi Serangan di Pilih :

Identifikasi Serangan

I106 - Kita menggunakan search engine (mesin pencari, seperti Yahoo, Alta Vista, Goggle) untuk mendapatkan link dari topik yang ingin dicari. Tanpa kita ketahui, beberapa dari link ini telah dieletakkan oleh hacker yang berpura-pura menjadi orang lain.

I111 - Alamat IP penyerang biasanya telah disembunyikan atau spoofed sehingga alamat yang dicatat oleh target adalah alamat yang salah.

I120 - Terjadinya modifikasi file atau data.

I127 - Mencoba mendapatkan informasi seperti username, password, dan rincian kartu kredit dengan menyamar sebagai entitas terpercaya dalam sebuah komunikasi elektronik.

I129 - Terjadinya penggunakan file atau berkas.

Menentukan nilai n_c untuk setiap class :

	S100	S101	S102	S103	S104	S105	S106	S107	S108	S109
I106	0	0	0	1	0	0	0	1	0	0
I111	1	0	0	0	0	0	0	0	0	1
I120	0	0	0	0	0	0	0	0	1	0
I127	0	0	0	0	1	0	0	0	0	1
I129	0	0	0	1	0	1	0	0	0	0

Gambar 3. Tampilan Hasil Perhitungan Algoritma Naive Bayes 1

Menghitung nilai P ($a_i|v_j$) dan menghitung nilai P (v_j) :

n =	1
m =	0.1
p =	10

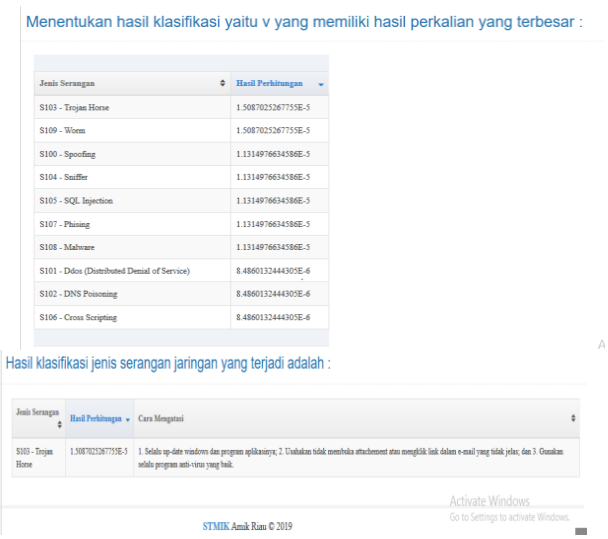
	S100	S101	S102	S103	S104	S105	S106	S107	S108	S109
I106	0.09677	0.09677	0.09677	0.12903	0.09677	0.09677	0.09677	0.12903	0.09677	0.09677
I111	0.12903	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.12903
I120	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.09677	0.12903	0.09677
I127	0.09677	0.09677	0.09677	0.09677	0.12903	0.09677	0.09677	0.09677	0.09677	0.12903
I129	0.09677	0.09677	0.09677	0.12903	0.09677	0.12903	0.09677	0.09677	0.09677	0.09677

Gambar 4. Penghitungan Hasil Algoritma Naive Bayes 2

Menghitung $P(a_i|v_j) \times P(v_j)$ untuk tiap v :

Jenis Serangan	Hasil Perhitungan
S100 - Spoofing	1.1314976634586E-5
S101 - Ddos (Distributed Denial of Service)	8.4860132444305E-6
S102 - DNS Poisoning	8.4860132444305E-6
S103 - Trojan Horse	1.5087025267755E-5
S104 - Sniffer	1.1314976634586E-5
S105 - SQL Injection	1.1314976634586E-5
S106 - Cross Scripting	8.4860132444305E-6
S107 - Phising	1.1314976634586E-5
S108 - Malware	1.1314976634586E-5
S109 - Worm	1.5087025267755E-5

Gambar 5. Penghitungan Hasil Algoritma Naive Bayes 3



Menentukan hasil klasifikasi yaitu v yang memiliki hasil perkalian yang terbesar :

Jenis Serangan	Hasil Perhitungan
S103 - Trojan Horse	1.5087025267755E-5
S109 - Worm	1.5087025267755E-5
S100 - Spoofing	1.1314976634586E-5
S104 - Sniffer	1.1314976634586E-5
S105 - SQL Injection	1.1314976634586E-5
S107 - Phising	1.1314976634586E-5
S108 - Malware	1.1314976634586E-5
S101 - Ddos (Distributed Denial of Service)	8.4860132444305E-6
S102 - DNS Poisoning	8.4860132444305E-6
S106 - Cross Scripting	8.4860132444305E-6

Hasil klasifikasi jenis serangan jaringan yang terjadi adalah :

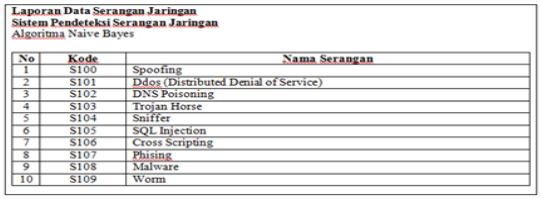
Jenis Serangan	Hasil Perhitungan	Cara Mengatasi
S103 - Trojan Horse	1.5087025267755E-5	1. Selalu up-date windows dan program aplikasinya; 2. Usahakan tidak membuka attachement atau mengklik link dalam e-mail yang tidak jelas; dan 3. Gunakan selalu program anti-virus yang baik.

STMIK Amik Riau © 2019

Gambar 6. Tampilan Hasil Perhitungan Algoritma Naive Bayes 2

3.1 Laporan Data Serangan Jaringan

Tampilan Laporan Data Serangan Jaringan merupakan laporan data seringan jaringan yang dapat dicetak berdasarkan inputan data serangan jaringan.



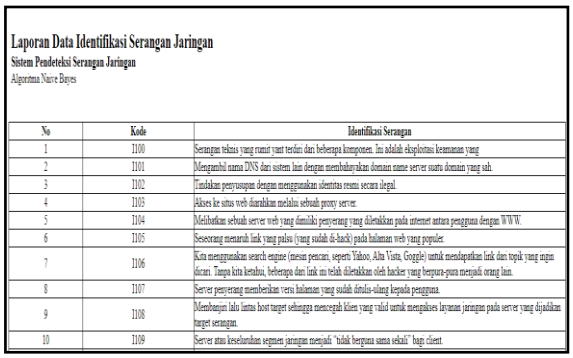
Laporan Data Serangan Jaringan
Sistem Pendeteksi Serangan Jaringan
Algoritma Naive Bayes

No	Kode	Nama Serangan
1	S100	Spoofing
2	S101	Ddos (Distributed Denial of Service)
3	S102	DNS Poisoning
4	S103	Trojan Horse
5	S104	Sniffer
6	S105	SQL Injection
7	S106	Cross Scripting
8	S107	Phising
9	S108	Malware
10	S109	Worm

Gambar 7. Tampilan Laporan Data Serangan Jaringan

3.2 Laporan Data Identifikasi Serangan Jaringan

Tampilan Laporan Data Identifikasi Serangan Jaringan merupakan laporan data identifikasi serangan jaringan yang dapat dicetak berdasarkan inputan data identifikasi serangan jaringan.



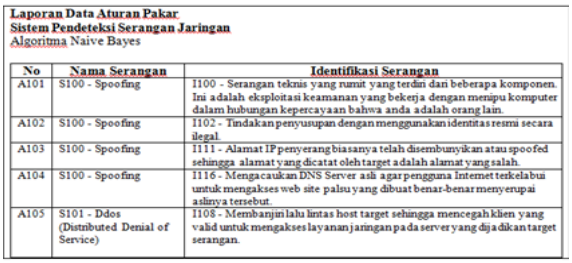
Laporan Data Identifikasi Serangan Jaringan
Sistem Pendeteksi Serangan Jaringan
Algoritma Naive Bayes

No	Kode	Identifikasi Serangan
1	I100	Serangan teknis yang rumit yant terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang
2	I101	Mengambil nama DNS dari sistem lain dengan membahayakan domain name server suatu domain yang sah.
3	I102	Tindakan penyusupan dengan menggunakan identitas resmi secara ilegal.
4	I103	Akses ke situs web diarahkan melalui sebuah proxy server.
5	I104	Melibatkan sebuah server web yang dimiliki penyerang yang diletakkan pada internet antara pengguna dengan WWW.
6	I105	Seseorang menarub link yang palsu (yang sudah di-hack) pada halaman web yang populer.
7	I106	Kita menggunakan search engine (mesin pencari, seperti Yahoo, Alta Vista, Goggle) untuk mendapatkan link dan topik yang ingin dicari. Tanpa kita ketahui, beberapa dari link ini telah diletakkan oleh hacker yang berpura-pura menjadi orang lain.
8	I107	Server penyerang memberikan versi halaman yang sudah ditulis-ulang kepada pengguna.
9	I108	Membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan.
10	I109	Server atau keseluruhan segmen jaringan menjadi "tidak berguna sama sekali" bagi client.

Gambar 8. Tampilan Laporan Data Identifikasi Serangan Jaringan

3.3 Laporan Data Aturan Pakar

Tampilan Laporan Data Aturan Pakar merupakan laporan data aturan pakar yang dapat dicetak berdasarkan inputan data aturan pakar.



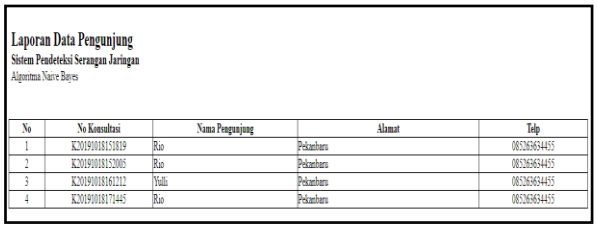
Laporan Data Aturan Pakar
Sistem Pendeteksi Serangan Jaringan
Algoritma Naive Bayes

No	Nama Serangan	Identifikasi Serangan
A101	S100 - Spoofing	I100 - Serangan teknis yang rumit yang terdiri dari beberapa komponen. Ini adalah eksploitasi keamanan yang bekerja dengan menipu komputer dalam hubungan kepercayaan bahwa anda adalah orang lain.
A102	S100 - Spoofing	I102 - Tindakan penyusupan dengan menggunakan identitas resmi secara ilegal.
A103	S100 - Spoofing	I111 - Alamat IP penyerang biasanya telah disembunyikan atau spoofed sehingga alamat yang dicatat oleh target adalah alamat yang salah.
A104	S100 - Spoofing	I116 - Mengacaukan DNS Server asli agar pengguna Internet terkelabui untuk mengakses web site palsu yang dibuat benar-benar menyerupai aslinya tersebut.
A105	S101 - Ddos (Distributed Denial of Service)	I108 - Membanjiri lalu lintas host target sehingga mencegah klien yang valid untuk mengakses layanan jaringan pada server yang dijadikan target serangan.

Gambar 9. Tampilan Data Aturan Pakar

3.4 Laporan Data Pengunjung

Tampilan Laporan Data Pengunjung Konsultasi merupakan laporan data pengunjung yang dapat dicetak berdasarkan inputan data pengunjung.



Laporan Data Pengunjung
Sistem Pendeteksi Serangan Jaringan
Algoritma Naive Bayes

No	No Konsultasi	Nama Pengunjung	Alamat	Telp
1	K20190108151019	Rio	Pekanbaru	085263634455
2	K20190108152005	Rio	Pekanbaru	085263634455
3	K20190108161222	Yulli	Pekanbaru	085263634455
4	K20190108171445	Rio	Pekanbaru	085263634455

Gambar 10. Tampilan Laporan Data Pengunjung

4. KESIMPULAN

Dari analisa dan pembahasan yang penulis lakukan pada bab-bab sebelumnya dapat diambil suatu kesimpulan yaitu:

1. Dari hasil perhitungan menggunakan algoritma Naive Bayes dapat ditentukan klasifikasi jenis serangan yang diambil dari perbandingan nilai v yaitu sebesar 0,000207899 dengan jenis serangan Worm.
2. Algoritma Naive Bayes dapat melakukan pendeteksian serangan jaringan LAN yang dapat membantu user untuk mengtahui jenis serangan dan cara mengatasinya.

4 UCAPAN TERIMAKASIH

Rangkaian menyelesaikan Penelitian ini peneliti mengucapkan terima kasih kepada STMIK Amik Riau dalam pemberi hibah.

5 DAFTAR PUSTAKA

Adi, S. (2018). Implementasi Algoritma Naive Bayes Classifier Untuk Klasifikasi Penerima Beasiswa PPA Di Universitas Amikom Yogyakarta. *Jurnal Mantik Penusa*, *22*(1), 11–16. http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/342

Ahmad, J., & No, Y. (n.d.). Metode Fuzzy Multiple Attribute Decision Making (Fmadm). *Jurnal Ilmiah MATRIK*, *03*, 45–58. http://www.ojs.stmikpringsewu.ac.id/index.php/JurnalTam/article/view/55

Firdaus, F., & Mukhlis, A. (2020). Implementasi Algoritma Naive Bayes Pada Data Set Kualitatif Prediksi Kebangkrutan. *JURIKOM (Jurnal Riset Komputer)*, *7*(1), 15. https://doi.org/10.30865/jurikom.v7i1.1757

Haryono, D., Herwin, H., & Nasution, T. (2020).

Implementasi Link Aggregation Control Protocol Untuk Meningkatkan Throughput Bandwidth Pada Up-Link Line. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *4*(1), 49. https://doi.org/10.35145/joisie.v4i1.633

Informatika, T., Malikussaleh, U., & Utara, A. (2014). Penerapan Algoritma Naive Bayes Untuk Mengklasifikasi Data Nasabah Asuransi. *Jurnal Informatika Ahmad Dahlan*, *8*(1), 102632. https://doi.org/10.26555/jifo.v8i1.a2086

Mafakhir, A. Z., & Solichin, A. (2020). Penerapan Metode Naïve Bayes Classifier Untuk Penjurusan Siswa Pada Madrasah Aliyah Al-Falah Jakarta. *Fountain of Informatics Journal*, *5*(1), 21. https://doi.org/10.21111/fij.v5i1.4007

Manalu, E., Sianturi, F. A., & Manalu, M. R. (2017). Penerapan Algoritma Naive Bayes Untuk Memprediksi Jumlah Produksi Barang Berdasarkan Data Persediaan dan Jumlah Pemesanan Pada CV. Papadan Mama Pastries. *Jurnal Mantik Penusa*, *1*(2), 16–21. https://ezp.lib.unimelb.edu.au/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=ffh&AN=2008-10-Aa4022&site=eds-live&scope=site

Nawawi, H. M., Purnama, J. J., & Hikmah, A. B. (2019). Komparasi Algoritma Neural Network Dan Naïve Bayes Untuk Memprediksi Penyakit Jantung. *Jurnal Pilar Nusa Mandiri*, *15*(2), 189–194. https://doi.org/10.33480/pilar.v15i2.669

Rosid, M. A. (2020). Classification of Student Complaints with the Naive Bayes and Literature Methods. *JOINCS (Journal of Informatics, Network, and Computer Science)*, *3*, 1–7. https://doi.org/10.21070/joincs.v3i0.711

Susanti, W., & Putri, R. N. (2020). Penerapan Cloud Computing Sebagai Media Pembelajaran Berbasis Online Masa Pandemi Covid-19. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, *4*(1), 56. https://doi.org/10.35145/joisie.v4i1.663