DETEKSI SERANGAN *PORT SCANNING* MENGGUNAKAN ALGORITMA *NAIVE BAYES*

Julius Chandra*[1], Hansen Hermanto[2], Abdul Rahman[3]
[1,2] STMIK GI MDP; Jl. Rajawali No.14, +62(711) 376400/376300
[3] Program Studi Teknik Informatika, STMIK GI MDP, Palembang
e-mail: *[1]hansenhermanto@mhs.mdp.ac.id, [2]juliuschandra190@mhs.mdp.ac.id,
[3]abdulrahman@mdp.ac.id

Abstrak

Serangan *Port Scanning* dapat menjadi masalah untuk kedepannya bagi jaringan jika tidak diatasi karena dapat merusak sistem dengan melakukan serangan lanjutan. *Port Scanning* memiliki dua tipe serangan yaitu *non stealth scan* dan *stealth scan, stealh scan* merupakan jenis *port scanning* yang lebih berbahaya dari pada *non stealth scan*. *Stealh scan* merupakan serangan yang dapat dianggap aktivitas normal bagi pendeteksi serangan, untuk itu dibutuhkan suatu teknik untuk mengenali ciri dari serangan *stealh scan*. Peneliti mengklasifikasi serangan *stealh scan* berdasarkan tiga jenis yaitu *FIN scan, NULL scan* dan *XMAS scan,* untuk mengenali ciri dari serangan tersebut dibutuhkan klasifikasi dari pola serangan dari tiga jenis tersebut. Peneliti menggunakan algoritma *naive bayes* untuk mengklasifikasikan ketiga jenis tersebut berdasarkan pola serangan. Pada paper ini peneliti akan membuat skenario sendiri untuk mengambil datasetnya dan setelah itu dataset akan diubah file nya melalui proses *featue extraction.* Tujuan dari *feature extraction* itu sendiri untuk mengubah file *.pcap* menjadi *.csv,* file *.csv* berguna untuk mempermudah peneliti mengenali pola dari serangan *stealh scan*. Pada penelitian ini setelah didapat pola serangan yang didapat dari informasi paket yang berasal dari *tcp header* dan *ip header*, pola tersebut peniliti amati dan dicari nilai probabilitasnya. Setelah didapat nilai probabilitasnya peneliti merancang sistem IDS menggunakan bahasa *python* dan mengimplementasikan algoritma *naive bayes*. Peneliti melakukan pengujian sistem IDS menggunakan *naïve* bayes sebanyak 10 kali. Hasil dari penelitian ini sendiri mendapatkan bahwa akurasi *naive bayes* sangat baik dalam deteksi dan pengklasifikasian berdasarkan jenis serangan dengan hasil untuk rata-rata akurasi *FIN scan* 99.04%, *NULL scan* 98.94%, *XMAS scan* 99.13% dan *all out attack* sebesar 99.10% .

Kata kunci— *Port Scanning,* IDS, Algoritma *Naive Bayes, FIN Scan, NULL Scan, XMAS Scan*

Abstract

Port Scanning attacks can become problems to the future for network if not resolved then it will damage the system with a follow-up attack. Port Scanning has two types of attacks i.e. non stealth scan and stealth scan. Stealth scan is an attack which can be considered normal activity for attack detection. Researchers classify stealth scan attacks based on three types that is FIN scan, NULL scan and XMAS scan, to recognize the characteristics of the attack is required classification of the attack pattern from the three types. Researches are using naive bayes algorithm to classify the three types based on the attack pattern. In this paper researchers will create their own scenario to take the dataset and after that the dataset will be modified its file through feature extraction process. The purpose of feature extraction itself to change file.pcap to .csv, file.csv is useful to simplify the researcher to recognize pattern from stealth scan attack. In this research after acquired the attack pattern which obtained from packet information originating from tcp header and ip header, the pattern the researcher observe dan find the probability value.

After obtained the probability value the researcher designing IDS system using phyton language and implement naive bayes algorithm. Researchers do IDS system testing using naive bayes as much as 10 times. Result of the research gets that accuracy of naive bayes is excellent in detection and classification based on attack type with results for average FIN scan accuracy 99.04%, NULL scan 98,94%,XMAS scan 99,13% and all out attack is 99.10%.

Keywords— *Port Scanning,* IDS, *Naive Bayes Algorithm, FIN Scan, NULL Scan, XMAS Scan*

1. PENDAHULUAN

Dalam perkembangan teknologi komputer, internet mendapatkan peranan besar dalam perkembangan tersebut. Internet digunakan oleh berbagai kalangan untuk menjalani ataupun mempermudah kegiatan yang dilakukannya, mulai dari rumah, kantor, sekolah sampai instansi-instansi pemerintahan memanfaatkan internet. Seiring perkembangan pengetahuan akan internet maka banyak terjadi serangan-serangan yang mengakibatkan kerugian bagi pengguna internet, oleh karena itu dibutuhkannyalah sebuah proteksi untuk mengamankan jaringan. Keamanan jaringan merupakan masalah krusial yang dihadapi pada era ini, di mana telah banyak kejahatan-kejahatan yang menyerang jaringan.

Serangan-serangan yang dilakukan biasanya untuk mendapatkan keuntungan dari merusak suatu sistem itu sendiri dengan tujuan untuk mendapatkan kepuasan ataupun uang. Salah satu jenis serangan yang dilakukan adalah *port scanning*, yang di mana *port scanning* adalah aktivitas untuk mengecek jalur data di jaringan tetapi bagi oknum yang ingin mendapatkan keuntungan tersendiri, teknik port scanning merupakan serangan yang mengecek *port* korban yang terbuka atau mencari celah dari *port* yang terbuka setelah itu penyerang dapat melakukan serangan lanjutan dari celah yang ditemukan tersebut. *Port scanning* memiliki bermacam teknik dalam penerapannya seperti *stealth scan*, *SOCKS port probe*, *bounce scan*, *TCP scanning* dan *UDP scanning*.

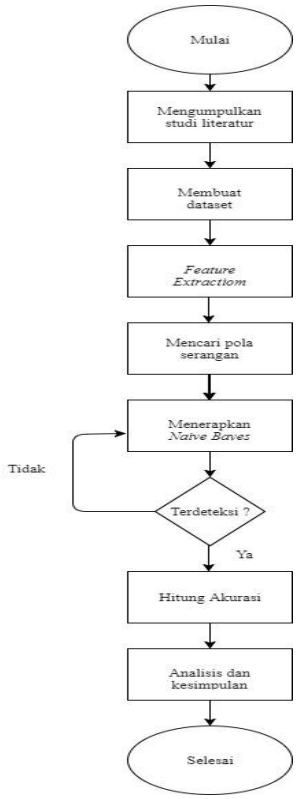
Teknik-teknik dalam *port scanning* tersebut memiliki berbagai macam jenis serangan contoh yang dapat di ambil adalah *stealth scan*, yang dimana *stealth scan* merupakan teknik menscan yang didesain untuk tidak terdeteksi oleh alat pendeteksi, teknik *stealth scan* mengirim paket-paket *TCP* ke host tujuan dengan flag yang tak terdeteksi, beberapa flag tersebut seperti *SYN*, *FIN* dan *NULL* [1]. Dalam pencegahannya dibutuhkan suatu aplikasi untuk mendeteksi serangan agar dapat dilakukannya sebuah pencegahan sebelum merusak sistem, untuk itu dibutuhkan *Intrusion Detection System* atau *IDS*.

IDS atau disebut juga *Intrusion Detection System* merupakan perangkat yang digunakan untuk mendeteksi serangan pada sebuah jaringan. Sebuah sistem serangan harus dapat mendeteksi berbagai macam tipe serangan dan harus tidak mengenali aktivitas yang legal sebagai serangan [6]. *IDS* akan menentukan serangan pada jaringan tersebut serangan atau bukan, jika serangan maka administrator dapat melakukan tindakan pada serangan tersebut. *IDS* dapat dibagi menjadi dua dalam hal pendekatan pendeteksiannya yaitu *signature based* dan *anomaly detection*. *Signature based* merupakan teknik yang menidentifikasi dan menyimpan pola yang telah dikenal dari serangan selanjutnya akan dicocokan antara pola dari serangan yang terjadi dan pola yang telah disimpan dan mengkategorikan sebagai serangan jika cocok sedangkan *anomaly detection* merupakan teknik deteksi yang dapat mengenali pola yang tidak diketahui tetapi dikarenakan semua anomali dapat dikatakan sebagai sebuah serangan maka banyak *false alarm* yang terjadi dikarenakan perilaku dari pola yang tidak biasa dalam paket data yang yang di tangkap [2]. Deteksi anomali mencoba untuk menentukan bahwa penyimpangan yang berasal dari pola normal dapat ditandai sebagai seragan [5].

Dalam hal mengurangi *false alarm* dibutuhkan suatu algoritma yang dapat mengklasifikasikan serangan yang lebih akurat, *naive Bayes* merupakan algoritma yang telah terbukti berhasil dalam melakukan *spam filter* [2]. *Naive bayes* adalah teknik prediksi berbasis *probabilistic* sederhana yang berdasar pada penerapan teorema *bayes* dengan asumsi ketidaktergantungan yang kuat [3]. *Naive bayes* sendiri sudah banyak digunakan untuk penelitian maupun menerapkannya disebuah aplikasi yang berfungsi untuk pengambil keputusan, dan pada penelitian ini penulis membuat sistem pendeteksi dengan jenis *IDS anomaly detection* yang dapat mendeteksi serangan *port scanning* dengan pola yang tidak biasa serta mengklasifikasikan serangan *port scanning* berdasarkan jenis dalam teknik *stealh scan*, yang dimana klasifikasi serangan *port scanning* pada penelitian ini mengggunakan dataset yang diciptakan sendiri oleh penulis, diciptakan sendiri dalam arti peneliti akan membuat skenario penyerangan sendiri menggunakan tool seperti *nmap* dan ditangkap menggunakan *wireshark*. *Naive bayes* selanjutnya akan diterapkan pada sistem deteksi yang akan di rancang peneliti dan mengamati hasil yang didapat. Alasan Peneliti menggunakan *naive bayes* sebagai algoritma yang diterapkan dalam *IDS* karena *naive bayes* terbukti berhasil melakukan *SPAM filters* yang dimana diharapkan dapat mengurangi *false alarm* dalam pendekatan *anomaly detection*.

2. METODE PENELITIAN

Pelaksanaan penelitian ini dilakukan secara bertahap berdasarkan diagram alir pada gambar 1.



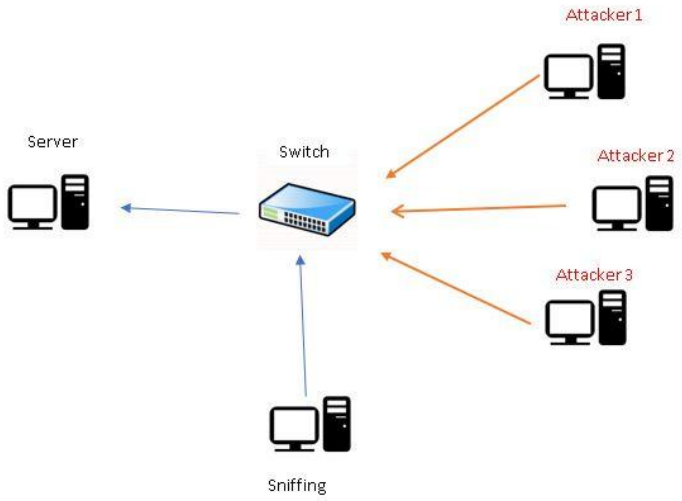
Gambar 0 Diagram Alir Metodologi Penelitian

2.1 Mengumpulkan Studi Literatur

Tahap awal penelitian ini adalah mengumpulkan studi literatur yang pokok bahasannya adalah deteksi serangan dan klasifikasi menggunakan metode *naive bayes*. Setelah peneliti mendapatkan beberapa studi literatur, peneliti merangkum hasil yang didapat dari studi literatur yang telah dikumpulkan, tujuan dari pengumpulan studi literatur adalah agar membantu peneliti mendapatkan referensi untuk penelitian ini.

2. 2 Membuat Dataset

Dataset yang digunakan pada penelitian ini adalah paket-paket dari tiga jenis serangan *stealth scan* dari *port scanning* yaitu *fin* scan, *null* scan dan *xmas* scan. Paket-paket tersebut sebelumnya ditangkap terlebih dahulu melalui proses *sniffing*, topologi untuk skenario pengumpulan dataset dapat dilihat pada gambar 2. Pengumpulan dataset dilakukan sebanyak tiga serangan, serangan pertama bertujuan untuk menangkap paket *FIN*, peneliti menggunakan aplikasi *nmap* untuk melakukan serangan, perintah yang digunakan untuk *FIN* adalah *nmap -sF -T4 -A -v IP target*, setelah itu dilakukan serangan ke dua untuk menangkap paket *NULL*, untuk *NULL* perintah yang digunakan *nmap -sN -T4 -A -v IP target* dan serangan ke tiga untuk menangkap paket *XMAS*, untuk *XMAS* perintahnya adalah *nmap sX -T4 -A -v IP target*. Peneliti melakukan serangan sambil mengakses web dengan tujuan agar *wireshark* menangkap paket normal juga, dengan begitu peneliti mendapatkan data pembanding paket normal dan paket serangan untuk dianalisis. Setiap serangan masing-masing dilakukan selama 10 menit, waktu ditetapkan dengan tujuan agar membatasi banyak paket yang ditangkap.



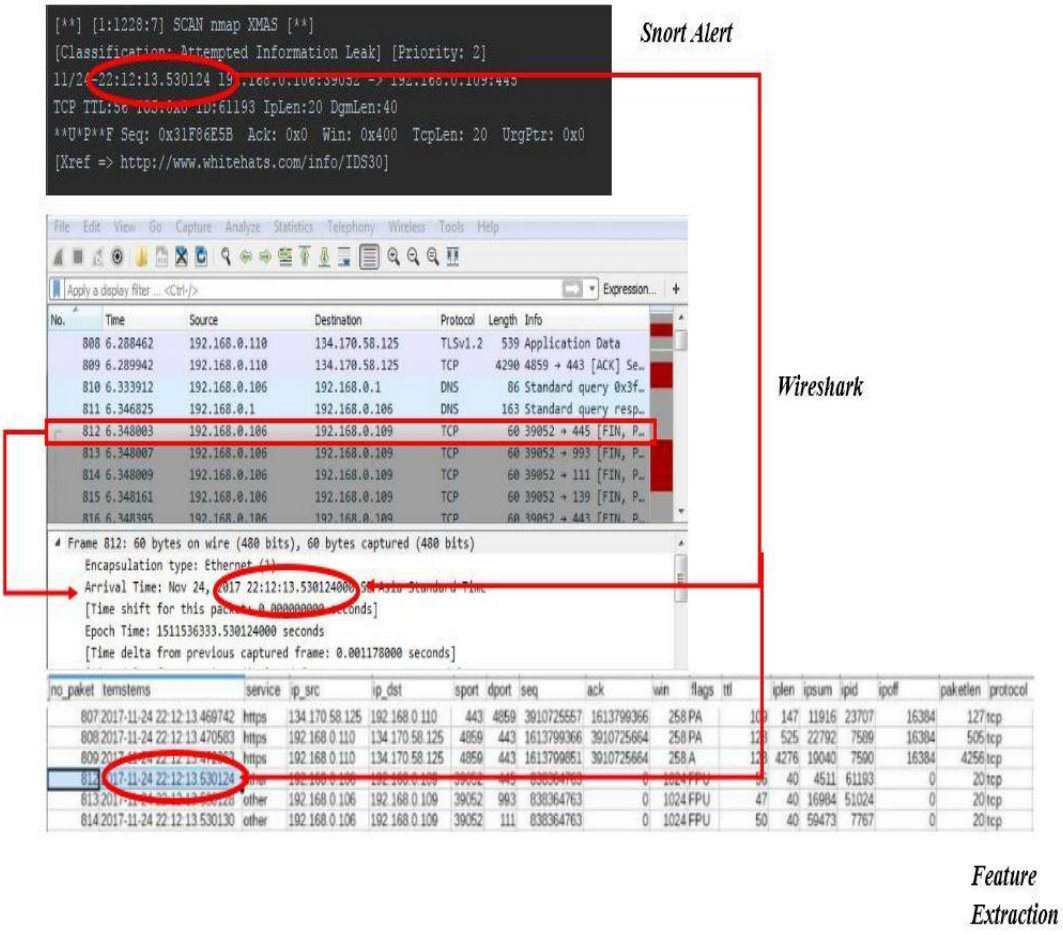
Gambar 2 Topologi Skenario Pengumpulan Dataset

2.3 *Feature Extraction*

Setelah peneliti mendapatkan dataset yang masih berupa *.pcap* dari tiga jenis serangan, peneliti melakukan *feature extraction* pada ketiga jenis serangan tersebut. Tujuan dari *feature extraction* itu sendiri berfungsi untuk mempermudah peneliti untuk menganalisa dan mengidentifikasi ciri pola serangan *port scanning* yang akan digunakan untuk menentukan probabilitas yang muncul pada setiap pola yang ada. *Feature extraction* itu sendiri hanya akan mengkonversi paket yang merupakan protocol TCP dan hasil dari *feature extraction* yang dilakukan oleh peneliti berupa file *.csv*

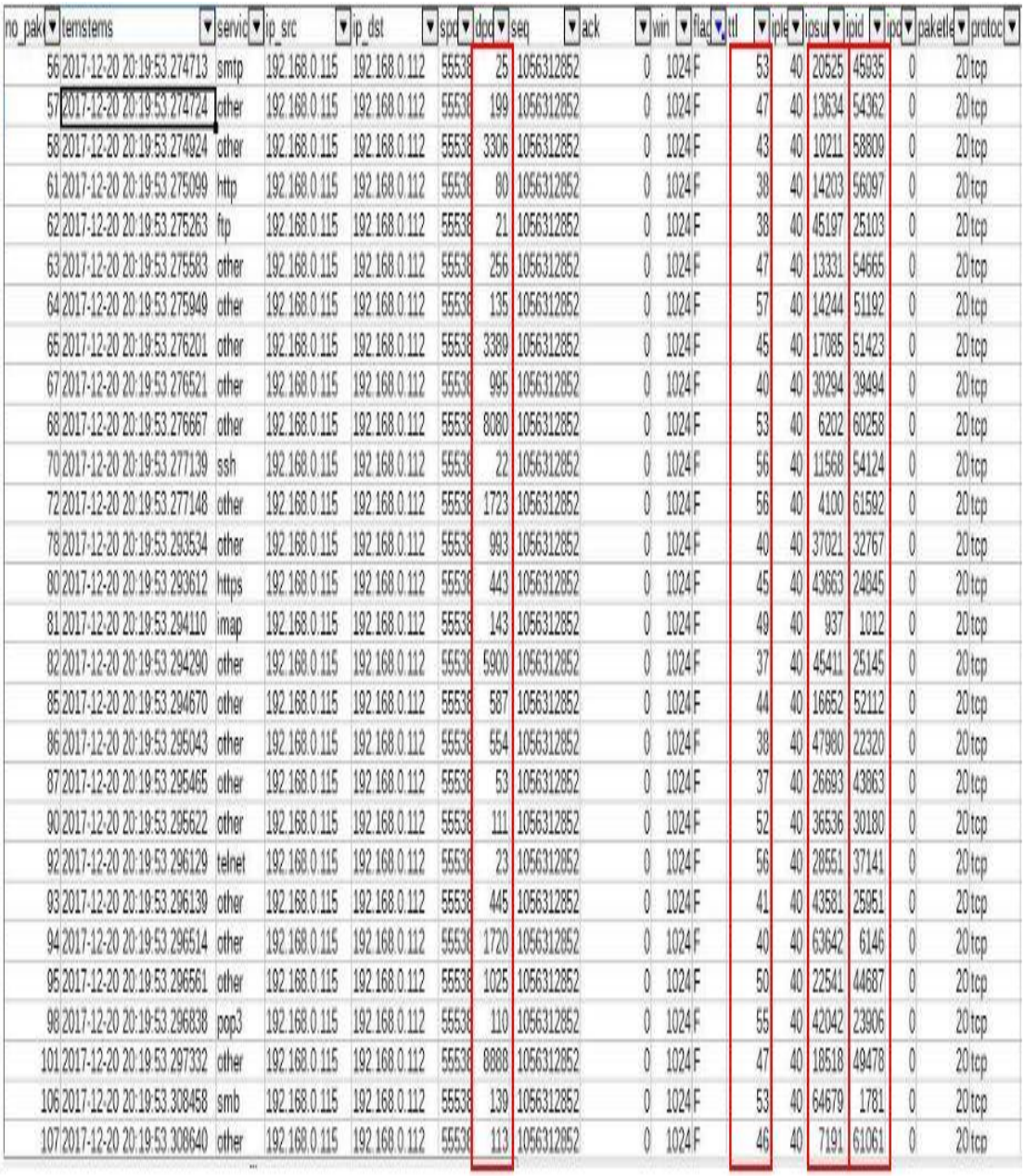
2.4 Mencari Pola Serangan

Setelah peneliti melakukan *feature extraction* pada paket *.pcap* yang didapat, file yang menjadi *.csv* tersebut peneliti lakukan analisis untuk dicari pola dari paket. Pertama-tama peneliti melakukan pencarian paket yang berupa serangan, dengan cara menvalidasi serangan dari *alert snort*, cara peneliti menvalidasi serangan adalah melihat waktu yang sama pada alert dan hasil *capture*, untuk lebih jelasnya dapat dilihat pada gambar 4.



Gambar 3 *Proses Validasi Serangan*

Pada gambar 3 dapat dilihat pada hasil deteksi *snort* waktu yang diambil adalah *22:12:13.530124* setelah itu peneliti mengamati pada file *.pcap* yang memiliki waktu yang sama dan mendapatkan paket dengan no 812 memiliki waktu yang sama dan terakhir pada hasil *feature extraction* sesuai no paket peneliti menemukan waktu yang sama, ini mengindikasikan serangan yang dideteksi dan yang di*capture* adalah sama sehingga membuktikan bahwa paket tersebut merupakan serangan. Semua paket berlaku cara ini untuk validasi serangan yang didapat oleh peneliti.



no_pak	temstems	servic	ip_src	ip_dst	spd	dpd	seq	ack	win	flag	ttl	iple	ipsu	ipid	ipd	paketle	protoc
56	2017-12-20 20:19:53.274713	smtp	192.168.0.115	192.168.0.112	55538	25	1056312852	0	1024	F	53	40	20525	45935	0	20	tcp
57	2017-12-20 20:19:53.274724	other	192.168.0.115	192.168.0.112	55538	199	1056312852	0	1024	F	47	40	13634	54362	0	20	tcp
58	2017-12-20 20:19:53.274924	other	192.168.0.115	192.168.0.112	55538	3306	1056312852	0	1024	F	43	40	10211	58809	0	20	tcp
61	2017-12-20 20:19:53.275099	http	192.168.0.115	192.168.0.112	55538	80	1056312852	0	1024	F	38	40	14203	56097	0	20	tcp
62	2017-12-20 20:19:53.275263	ftp	192.168.0.115	192.168.0.112	55538	21	1056312852	0	1024	F	38	40	45197	25103	0	20	tcp
63	2017-12-20 20:19:53.275583	other	192.168.0.115	192.168.0.112	55538	256	1056312852	0	1024	F	47	40	13331	54665	0	20	tcp
64	2017-12-20 20:19:53.275949	other	192.168.0.115	192.168.0.112	55538	135	1056312852	0	1024	F	57	40	14244	51192	0	20	tcp
65	2017-12-20 20:19:53.276201	other	192.168.0.115	192.168.0.112	55538	3389	1056312852	0	1024	F	45	40	17085	51423	0	20	tcp
67	2017-12-20 20:19:53.276521	other	192.168.0.115	192.168.0.112	55538	995	1056312852	0	1024	F	40	40	30294	39494	0	20	tcp
68	2017-12-20 20:19:53.276667	other	192.168.0.115	192.168.0.112	55538	8080	1056312852	0	1024	F	53	40	6202	60258	0	20	tcp
70	2017-12-20 20:19:53.277139	ssh	192.168.0.115	192.168.0.112	55538	22	1056312852	0	1024	F	56	40	11568	54124	0	20	tcp
72	2017-12-20 20:19:53.277148	other	192.168.0.115	192.168.0.112	55538	1723	1056312852	0	1024	F	56	40	4100	61592	0	20	tcp
78	2017-12-20 20:19:53.293534	other	192.168.0.115	192.168.0.112	55538	993	1056312852	0	1024	F	40	40	37021	32767	0	20	tcp
80	2017-12-20 20:19:53.293612	https	192.168.0.115	192.168.0.112	55538	443	1056312852	0	1024	F	45	40	43663	24845	0	20	tcp
81	2017-12-20 20:19:53.294110	imap	192.168.0.115	192.168.0.112	55538	143	1056312852	0	1024	F	49	40	937	1012	0	20	tcp
82	2017-12-20 20:19:53.294290	other	192.168.0.115	192.168.0.112	55538	5900	1056312852	0	1024	F	37	40	45411	25145	0	20	tcp
85	2017-12-20 20:19:53.294670	other	192.168.0.115	192.168.0.112	55538	587	1056312852	0	1024	F	44	40	16652	52112	0	20	tcp
86	2017-12-20 20:19:53.295043	other	192.168.0.115	192.168.0.112	55538	554	1056312852	0	1024	F	38	40	47980	22320	0	20	tcp
87	2017-12-20 20:19:53.295465	other	192.168.0.115	192.168.0.112	55538	53	1056312852	0	1024	F	37	40	26693	43863	0	20	tcp
90	2017-12-20 20:19:53.295622	other	192.168.0.115	192.168.0.112	55538	111	1056312852	0	1024	F	52	40	36536	30180	0	20	tcp
92	2017-12-20 20:19:53.296129	telnet	192.168.0.115	192.168.0.112	55538	23	1056312852	0	1024	F	56	40	28551	37141	0	20	tcp
93	2017-12-20 20:19:53.296139	other	192.168.0.115	192.168.0.112	55538	445	1056312852	0	1024	F	41	40	43581	25951	0	20	tcp
94	2017-12-20 20:19:53.296514	other	192.168.0.115	192.168.0.112	55538	1720	1056312852	0	1024	F	40	40	63642	6146	0	20	tcp
95	2017-12-20 20:19:53.296561	other	192.168.0.115	192.168.0.112	55538	1025	1056312852	0	1024	F	50	40	22541	44687	0	20	tcp
98	2017-12-20 20:19:53.296838	pop3	192.168.0.115	192.168.0.112	55538	110	1056312852	0	1024	F	55	40	42042	23806	0	20	tcp
101	2017-12-20 20:19:53.297332	other	192.168.0.115	192.168.0.112	55538	8888	1056312852	0	1024	F	47	40	18518	49478	0	20	tcp
106	2017-12-20 20:19:53.308458	smb	192.168.0.115	192.168.0.112	55538	139	1056312852	0	1024	F	53	40	64679	1781	0	20	tcp
107	2017-12-20 20:19:53.308640	other	192.168.0.115	192.168.0.112	55538	113	1056312852	0	1024	F	46	40	7191	61061	0	20	tcp

Gambar 4 Pola Serangan *FIN*

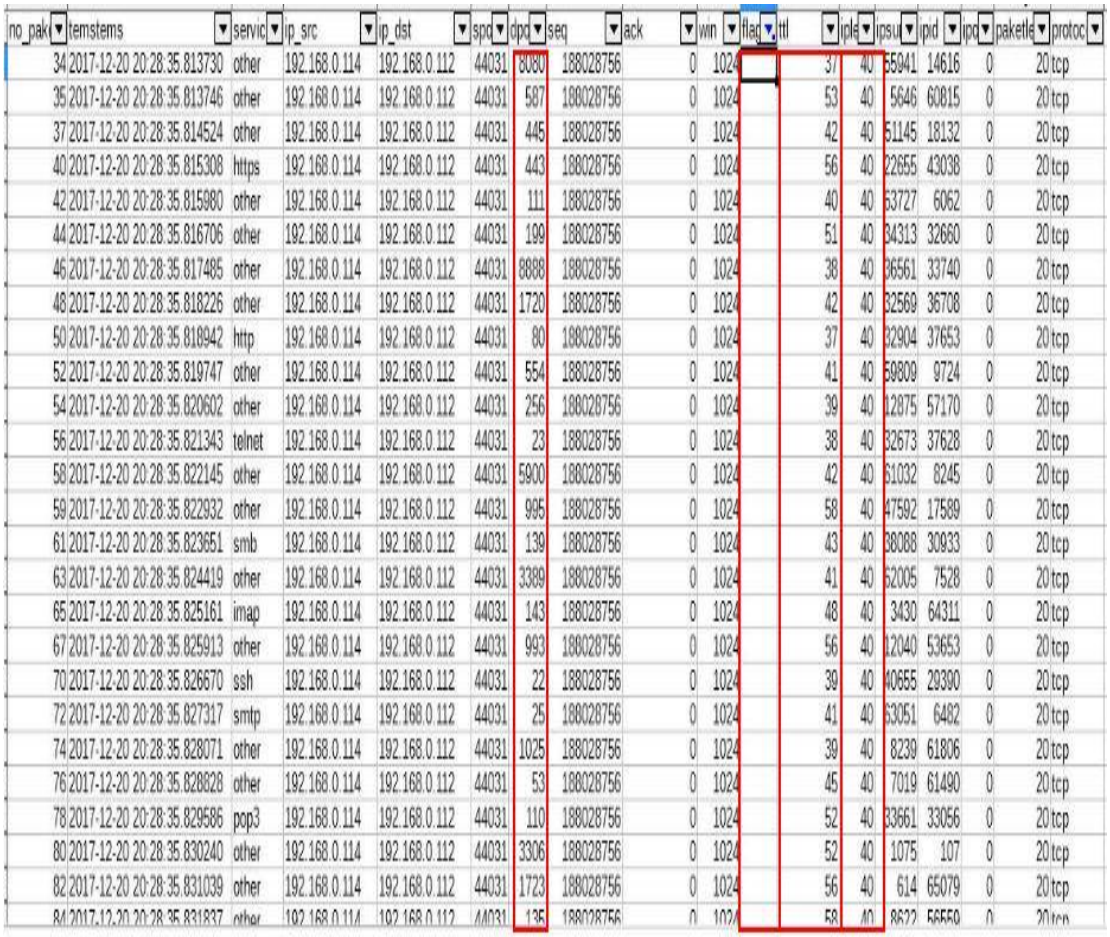
Pada Gambar 4 peneliti melakukan *filter* pada *flag F* dapat dilihat serangan *FIN* memiliki beberapa pola yang berbeda yang terletak pada *dport*, *TTL*, *ipsum* dan *ipid*, Peneliti mengamati pada *field dport*, *ipid* dan ipsum pola yang dimiliki adalah acak dan tidak memiliki kesamaan kecuali pada *field TTL* yang memilki nilai yang sama pada setiap serangannya dan memiliki rentang nilai. Setelah itu peneliti mengambil setiap rentang nilai dari *TTL* didapat. Setelah diamati peneliti mendapatkan rentang nilai *TTL* pada serangan *FIN* adalah 37-59 dan peneliti membagi tiga rentang nilai *TTL* yaitu 37-39, 40-49 dan 50-59 untuk meningkatkan ketelitian dalam peluang. Peneliti pada serangan *FIN* akan mengambil *window*, *flag*, *iplen* dan *TTL* sebagai pola yang menjadi dataset karena polanya sama setiap paket dan memiliki rentang nilai.

no_pak	temstems	servic	ip_src	ip_dst	spd	dpd	seq	ack	win	flag	ttl	iple	ipsu	ipid	ipoff	paketle	protoc
101	2017-12-20 20:38:15.011663	other	192.168.0.115	192.168.0.112	52594	111	3093078494	0	1024	FPU	39	40	32327	37717	0	20	tcp
102	2017-12-20 20:38:15.011670	other	192.168.0.115	192.168.0.112	52594	113	3093078494	0	1024	FPU	49	40	27558	39926	0	20	tcp
104	2017-12-20 20:38:15.011830	pop3	192.168.0.115	192.168.0.112	52594	110	3093078494	0	1024	FPU	41	40	43512	26020	0	20	tcp
105	2017-12-20 20:38:15.012177	other	192.168.0.115	192.168.0.112	52594	995	3093078494	0	1024	FPU	46	40	37218	31034	0	20	tcp
106	2017-12-20 20:38:15.012183	other	192.168.0.115	192.168.0.112	52594	199	3093078494	0	1024	FPU	50	40	40667	26561	0	20	tcp
107	2017-12-20 20:38:15.012289	other	192.168.0.115	192.168.0.112	52594	1025	3093078494	0	1024	FPU	43	40	35524	33496	0	20	tcp
108	2017-12-20 20:38:15.012413	other	192.168.0.115	192.168.0.112	52594	53	3093078494	0	1024	FPU	55	40	25032	40916	0	20	tcp
109	2017-12-20 20:38:15.012526	other	192.168.0.115	192.168.0.112	52594	5900	3093078494	0	1024	FPU	55	40	57484	8464	0	20	tcp
110	2017-12-20 20:38:15.012655	other	192.168.0.115	192.168.0.112	52594	554	3093078494	0	1024	FPU	37	40	32946	37610	0	20	tcp
113	2017-12-20 20:38:15.012809	telnet	192.168.0.115	192.168.0.112	52594	23	3093078494	0	1024	FPU	55	40	18407	47541	0	20	tcp
121	2017-12-20 20:38:15.014919	smtp	192.168.0.115	192.168.0.112	52594	25	3093078494	0	1024	FPU	52	40	62029	4687	0	20	tcp
122	2017-12-20 20:38:15.014926	https	192.168.0.115	192.168.0.112	52594	443	3093078494	0	1024	FPU	44	40	19135	49629	0	20	tcp
123	2017-12-20 20:38:15.014928	other	192.168.0.115	192.168.0.112	52594	993	3093078494	0	1024	FPU	59	40	52758	12166	0	20	tcp
124	2017-12-20 20:38:15.014929	other	192.168.0.115	192.168.0.112	52594	8080	3093078494	0	1024	FPU	59	40	1124	63800	0	20	tcp
125	2017-12-20 20:38:15.015062	other	192.168.0.115	192.168.0.112	52594	1720	3093078494	0	1024	FPU	42	40	35041	34235	0	20	tcp
127	2017-12-20 20:38:15.015065	http	192.168.0.115	192.168.0.112	52594	80	3093078494	0	1024	FPU	38	40	56636	13664	0	20	tcp
128	2017-12-20 20:38:15.015192	ftp	192.168.0.115	192.168.0.112	52594	21	3093078494	0	1024	FPU	57	40	5561	59875	0	20	tcp
130	2017-12-20 20:38:15.015572	other	192.168.0.115	192.168.0.112	52594	8888	3093078494	0	1024	FPU	57	40	49845	15591	0	20	tcp
131	2017-12-20 20:38:15.015578	other	192.168.0.115	192.168.0.112	52594	445	3093078494	0	1024	FPU	39	40	34137	35907	0	20	tcp
132	2017-12-20 20:38:15.015579	other	192.168.0.115	192.168.0.112	52594	587	3093078494	0	1024	FPU	42	40	40052	29224	0	20	tcp
133	2017-12-20 20:38:15.015587	imap	192.168.0.115	192.168.0.112	52594	143	3093078494	0	1024	FPU	59	40	22969	41955	0	20	tcp
134	2017-12-20 20:38:15.015717	other	192.168.0.115	192.168.0.112	52594	3306	3093078494	0	1024	FPU	45	40	49183	19325	0	20	tcp
135	2017-12-20 20:38:15.015719	other	192.168.0.115	192.168.0.112	52594	135	3093078494	0	1024	FPU	49	40	21502	45982	0	20	tcp
136	2017-12-20 20:38:15.015836	ssh	192.168.0.115	192.168.0.112	52594	22	3093078494	0	1024	FPU	38	40	35138	35162	0	20	tcp
137	2017-12-20 20:38:15.015840	other	192.168.0.115	192.168.0.112	52594	3389	3093078494	0	1024	FPU	52	40	63823	2893	0	20	tcp
138	2017-12-20 20:38:15.015964	other	192.168.0.115	192.168.0.112	52594	256	3093078494	0	1024	FPU	58	40	37531	27649	0	20	tcp
139	2017-12-20 20:38:15.015966	other	192.168.0.115	192.168.0.112	52594	1723	3093078494	0	1024	FPU	54	40	61011	5193	0	20	tcp
140	2017-12-20 20:38:15.016010	smb	192.168.0.115	192.168.0.112	52594	139	3093078494	0	1024	FPU	56	40	39648	26044	0	20	tcp

Gambar 5 Pola Serangan XMAS

Pada Gambar 5 peneliti melakukan *filter* pada *flag FPU* dapat dilihat sama seperti serangan *FIN* serangan *XMAS* memiliki beberapa pola yang berbeda yang terletak pada *dport, TTL, ipsum* dan *ipid*, Peneliti mengamati pada *field dport, ipid* dan ipsum pola yang dimiliki adalah acak dan tidak memiliki kesamaan kecuali pada *field TTL* yang memilki nilai yang sama pada setiap serangannya dan memiliki rentang nilai. Setelah itu peneliti mengambil setiap rentang nilai dari *TTL* didapat. Setelah diamati peneliti mendapatkan rentang nilai *TTL* pada serangan *XMAS* adalah 37-59 dan peneliti membagi tiga rentang nilai *TTL* yaitu 37-39, 40-49 dan 50-59 untuk meningkatkan ketelitian dalam peluang. Peneliti pada serangan *XMAS* akan *mengambil window, flag, iplen* dan *TTL* sebagai pola yang menjadi dataset karena polanya sama setiap paket dan memiliki rentang nilai.

Selanjutnya peneliti menganalisis pola dari serangan *NULL*, pada serangan *NULL* tidak dapat divalidasi melalui *snort* dikarenakan *snort* tidak dapat mendeteksi serangan *NULL*, untuk mengenali pola serangan *NULL* peneliti mengamati pola yang terdapat pada hasil ekstrak.



no_pak	temstems	servic	ip_src	ip_dst	spo	dpd	seq	ack	win	flag	ttl	iple	ipsu	ipid	ipd	paketle	protoc
34	2017-12-20 20:28:35.813730	other	192.168.0.114	192.168.0.112	44031	8080	188028756	0	1024		37	40	55941	14616	0	20	tcp
35	2017-12-20 20:28:35.813746	other	192.168.0.114	192.168.0.112	44031	587	188028756	0	1024		53	40	5646	60815	0	20	tcp
37	2017-12-20 20:28:35.814524	other	192.168.0.114	192.168.0.112	44031	445	188028756	0	1024		42	40	61145	18132	0	20	tcp
40	2017-12-20 20:28:35.815308	https	192.168.0.114	192.168.0.112	44031	443	188028756	0	1024		56	40	22655	43038	0	20	tcp
42	2017-12-20 20:28:35.815980	other	192.168.0.114	192.168.0.112	44031	111	188028756	0	1024		40	40	53727	6062	0	20	tcp
44	2017-12-20 20:28:35.816706	other	192.168.0.114	192.168.0.112	44031	199	188028756	0	1024		51	40	34313	32660	0	20	tcp
46	2017-12-20 20:28:35.817485	other	192.168.0.114	192.168.0.112	44031	8888	188028756	0	1024		38	40	36561	33740	0	20	tcp
48	2017-12-20 20:28:35.818226	other	192.168.0.114	192.168.0.112	44031	1720	188028756	0	1024		42	40	32569	36708	0	20	tcp
50	2017-12-20 20:28:35.818942	http	192.168.0.114	192.168.0.112	44031	80	188028756	0	1024		37	40	32904	37653	0	20	tcp
52	2017-12-20 20:28:35.819747	other	192.168.0.114	192.168.0.112	44031	554	188028756	0	1024		41	40	59809	9724	0	20	tcp
54	2017-12-20 20:28:35.820602	other	192.168.0.114	192.168.0.112	44031	256	188028756	0	1024		39	40	12875	57170	0	20	tcp
56	2017-12-20 20:28:35.821343	telnet	192.168.0.114	192.168.0.112	44031	23	188028756	0	1024		38	40	32673	37628	0	20	tcp
58	2017-12-20 20:28:35.822145	other	192.168.0.114	192.168.0.112	44031	5900	188028756	0	1024		42	40	61032	8245	0	20	tcp
59	2017-12-20 20:28:35.822932	other	192.168.0.114	192.168.0.112	44031	995	188028756	0	1024		58	40	47592	17589	0	20	tcp
61	2017-12-20 20:28:35.823651	smb	192.168.0.114	192.168.0.112	44031	139	188028756	0	1024		43	40	38088	30933	0	20	tcp
63	2017-12-20 20:28:35.824419	other	192.168.0.114	192.168.0.112	44031	3389	188028756	0	1024		41	40	62005	7528	0	20	tcp
65	2017-12-20 20:28:35.825161	imap	192.168.0.114	192.168.0.112	44031	143	188028756	0	1024		48	40	3430	64311	0	20	tcp
67	2017-12-20 20:28:35.825913	other	192.168.0.114	192.168.0.112	44031	993	188028756	0	1024		56	40	12040	53653	0	20	tcp
70	2017-12-20 20:28:35.826670	ssh	192.168.0.114	192.168.0.112	44031	22	188028756	0	1024		39	40	40655	29390	0	20	tcp
72	2017-12-20 20:28:35.827317	smtp	192.168.0.114	192.168.0.112	44031	25	188028756	0	1024		41	40	63051	6482	0	20	tcp
74	2017-12-20 20:28:35.828071	other	192.168.0.114	192.168.0.112	44031	1025	188028756	0	1024		39	40	8239	61806	0	20	tcp
76	2017-12-20 20:28:35.828828	other	192.168.0.114	192.168.0.112	44031	53	188028756	0	1024		45	40	7019	61490	0	20	tcp
78	2017-12-20 20:28:35.829586	pop3	192.168.0.114	192.168.0.112	44031	110	188028756	0	1024		52	40	33661	33056	0	20	tcp
80	2017-12-20 20:28:35.830240	other	192.168.0.114	192.168.0.112	44031	3306	188028756	0	1024		52	40	1075	107	0	20	tcp
82	2017-12-20 20:28:35.831039	other	192.168.0.114	192.168.0.112	44031	1723	188028756	0	1024		56	40	614	65079	0	20	tcp
84	2017-12-20 20:28:35.831837	other	192.168.0.114	192.168.0.112	44031	135	188028756	0	1024		58	40	8622	56559	0	20	tcp

Gambar 6 Pola Serangan *NULL*

Pada Gambar 6 peneliti melakukan *filter* pada *flag* kosong dapat dilihat sama seperti serangan *FIN* dan *XMAS* serangan *NULL* memiliki beberapa pola yang berbeda yang terletak pada *dport, TTL, ipsum* dan *ipid,* Peneliti mengamati pada *field dport, ipid* dan ipsum pola yang dimiliki adalah acak dan tidak memiliki kesamaan kecuali pada *field TTL* yang memilki nilai yang sama pada setiap serangannya dan memiliki rentang nilai. Setelah itu peneliti mengambil setiap rentang nilai dari *TTL* didapat. Setelah diamati peneliti mendapatkan rentang nilai *TTL* pada serangan *NULL* adalah 37-59 dan peneliti membagi tiga rentang nilai *TTL* yaitu 37-39, 40-49 dan 50-59 untuk meningkatkan ketelitian dalam peluang. Peneliti pada serangan *NULL* akan *mengambil window, flag, iplen* dan *TTL* sebagai pola yang menjadi dataset karena polanya sama setiap paket dan memiliki rentang nilai.

Setelah mengamati pola serangan, peneliti juga mengamati pola paket normal untuk dijadikan dataset sehingga dapat dicari juga peluang pada paket normal untuk klasifikasi *naive bayes*. Pada paket terapat *flag* didapat yaitu FA, S, R, FPA, PA, RA dan A. Sama dengan mencari pola serangan, untuk paket normal peneliti juga melakukan *filtering* dan mencari pola yang nilai nya sama pada setiap paket yang berjenis *flag* sama.

2.5 Menerapkan *Naive Bayes*

Gambar 7 Diagram Alir *Naive Bayes*

Pada gambar 7 merupakan diagram alir dari *naive bayes* yang dimulai dari membaca data training yang merupakan pola serangan dari *port scanning*. Hasil dari baca data pola serangan tersebut adalah peluang dari setiap pola yang telah dicari, peluang tersebut dibuatkan dalam bentuk tabel sesuai pola.

2.6 Hitung Akurasi

Setelah didapat hasil uji coba, peneliti menggunakan *confusion matrix* untuk menghitung akurasi dari deteksi *port scanning* menggunakan algoritma *naive bayes.* Untuk menghitung akurasi dipakai rumus $\frac{TP + TN}{TP + TN + FP + FN}$ [4].

Tabel 1 *Confusion Matrix*

Classification	*Predicted Class*		
Observed Class		*Class = Yes*	*Class = No*
	Class = Yes	A *True Positive (TP)*	B False Negative (FN)
	Class = No	C False Positive (FP)	D True Negative (TN)

2.7 Analisis dan Kesimpulan

Dari hasil penelitian tersebut, peneliti pun mempelajari kekurangan dan kelebihan dari algoritma *naive bayes* yang digunakan untuk mendeteksi serangan *port scanning*.

3. HASIL DAN PEMBAHASAN

Pengujian *Intrusion Detection System* menggunakan algoritma *Naive Bayes* dilakukan sebanyak 10 kali dan melakukan serangan *FIN Scan, NULL Scan, XMAS Scan* dan *All Out Attack* yang merupakan gabungan dari ketiga jenis serangan, pada paper ini hasil uji coba akan dirata-rata per jenis serangan.

3.1 Hasil Mencari Pola Serangan

Setelah mencari pola paket serangan dan paket normal, peneliti mengidentifikasi paket serangan dan normal berdasarkan *flag, iplen, window, TTL* dan jenis paket. Pada paket serangan terlihat jelas perbedaan terletak pada jenis *flag*, pada jenis paket *FIN flag* yang dibawa adalah *F*, pada jenis paket *NULL flag* yang dibawa adalah tidak ada atau *null*, sedangkan untuk paket jenis *XMAS flag* yang dibawa adalah FPU. Sebagai pembeda dari serangan peneliti juga menentukan pola paket normal, hasil identifikasi pola paket serangan dan normal dapat dilihat pada tabel 1.

Tabel 1 Pola Serangan dan Normal

No	*Flags*	*Iplen*	*Window(Byte)*	*TTL(ms)*	Jenis Paket
1	F	40	1024	37-39	Fin
2	F	40	1024	40-49	Fin
3	F	40	1024	50-59	Fin
4	-	40	1024	37-39	Null
5	-	40	1024	40-49	Null
6	-	40	1024	50-59	Null
7	FPU	40	1024	37-39	Xmas
8	FPU	40	1024	40-49	Xmas
9	FPU	40	1024	50-59	Xmas
10	RA	40	0	128	Normal
11	S	52	8192	128	Normal
12	S	52	64240-65535	128	Normal
13	S	60	29200-31337	48-64	Normal
14	SA	48-52	8192	108-110	Normal
15	SA	52	29200	48-57	Normal
16	SA	52	65535	128	Normal
17	SA	52	42780	46	Normal
18	FA	40	129	41-44	Normal
19	FA	40	254-259	41-44	Normal
20	FA	40	176-198	57	Normal
21	FA	40	946	58	Normal
22	FA	40	3456-6932	64	Normal
23	FA	52	2920	64	Normal
24	FA	40	259	111-112	Normal
25	FA	40	512	106	Normal
26	FA	40	62835-64763	128	Normal
27	FA	40	254-259	128	Normal
28	R	40	0	57-128	Normal
29	FPA	425-473	259	107-109	Normal
30	FPA	1837-1885	259	107-109	Normal
31	FPA	311	255	128	Normal
32	FPA	292	5896	50	Normal
33	FPA	177	257	128	Normal
34	FPA	2119-3579	3456	64	Normal

35	FPA	434-452	3992	64	Normal
36	F	40	1024	37-39	Normal
37	F	40	1024	40-49	Normal
38	F	40	1024	50-59	Normal
39	A	40-52	0-49	128	Normal
40	A	2948	65160	128	Normal
41	A	52	29200-65160	64	Normal
42	A	40	259	128	Normal
43	A	40	257-259	128	Normal
44	A	40	1024	128	Normal
45	PA	120-827	2920-3992	64	Normal
46	PA	113-3217	255-256	128	Normal
47	PA	191-1445	63865-64862	128	Normal

3.2 Hasil Perhitungan Akurasi dan Rata-Rata

Setelah didapat hasil dari 10 kali uji coba peneliti melakukan perhitungan akurasi per serangan, untuk lebih jelasnya dapat dilihat pada tabel 2.

Tabel 2 Hasil Keseluruhan Akurasi Tiap Serangan

	FIN Scan	*NULL Scan*	*XMAS Scan*	*All Out Attack*
Pengujian 1	98.82%	98.59%	98.70%	99.32%
Pengujian 2	98.81%	98.81%	99.93%	99.17%
Pengujian 3	99.12%	98.93%	98.92%	99.10%
Pengujian 4	99.33%	99.14%	98.64%	99.16%
Pengujian 5	99.51%	99.00%	98.98%	99.22%
Pengujian 6	98.95%	99.08%	99.96%	99.18%
Pengujian 7	98.79%	99.06%	99.07%	98.79%
Pengujian 8	99.10%	98.61%	99.09%	99.28%
Pengujian 9	99.12%	99.04%	99.05%	99.19%
Pengujian 10	98.89%	99.23%	98.98%	98.99%

Dari semua persentase tersebut dicarila rata-rata per serangan dari 10 kali uji coba tersebut.

Rata-rata akurasi *FIN* =

$$\frac{98.82\%+98.91\%+99.12\%+99.33\%+99.51\%+98.95\%+98.79\%+99.10\%+99.12\%+98.89\%}{10} = \mathbf{99.04\%}$$

Rata-rata akurasi NULL Scan =

$$\frac{98.59\%+98.81\%+98.93\%+99.14\%+99.00\%+99.08\%+99.06\%+98.61\%+99.04\%+99.23\%}{10} = \mathbf{98.94\%}$$

Rata-rata akurasi XMAS Scan =

$$\frac{98.70\%+99.93\%+98.92\%+98.64\%+98.98\%+99.96\%+99.07\%+99.09\%+99.05\%+98.98\%}{10} = \mathbf{99.13\%}$$

Rata-rata akurasi *All Out Attack* =

$$\frac{99.32\%+99.17\%+99.10\%+98.90\%+98.90\%+99.04\%+99.28\%+99.19\%+98.99\%+98.18\%}{10} = \mathbf{99.10\%}$$

4. KESIMPULAN

Sesuai rumusan masalah yang dibuat dari hasil pengamatan yang telah dilakukan peneliti menyimpulkan bahwa:

1. *Naive bayes* mengklasifikasikan jenis serangan berdasarkan pola serangan yang diamati, setelah itu pola tersebut dicari nilai probabilitasnya agar dapat dihitung oleh *naive bayes.*
2. Algoritma *naïve bayes* dapat diterapakan pada sistem deteksi serangan *port scanning.*
3. Akurasi peneliti menghitung akurasi klasifikasi menggunakan *confusion matrix* dengan rata-rata dari semua pengujian yang telah dilakukan dimana hasil akurasi nya adalah adalah *FIN* sebesar 99.04%, *NULL* sebesar 98.94%, *XMAS* sebesar 99.13% dan *all out attack* sebesar 99.10% yang dimana menurut hasil tersebut *naive bayes* tergolong sangat baik dalam hal ketepatan pengklasifikasian.

5. SARAN

Saran yang dapat direkomendasikan dalam penelitian selanjutnya adalah :

1. Algoritma *naive bayes* dapat digunakan untuk mengklasifikasi serangan yang berbeda.
2. Dalam hal mendeteksi serangan *port scanning* dan mengklasifikasi berdasarkan jenisnya, dapat digunakan algoritma yang berbeda atau dapat dilakukan perbandingan antara *naive bayes* dan algoritma lain.
3. Dapat ditambah jenis serangan *port scanning* yang lain untuk diklasifikasi *naive bayes.*

DAFTAR PUSTAKA

[1] Bhuyan, H. M, Bhattacharyya, D. K, Kalita. K, J.(2011). *Surveying Port Scans and Their Detection Metodologies.* The Computer Journal. Vol. 54 No. 10.

[2] Singh, R,R & Tomar D, S. (2015). *Network Forensics: Detection and Analysis of Stealth Port Scanning Attack*. P. 33-42. E-ISSN 2308-9830.

[3] Prasetyo, Eko. (2012). *Data Mining Konsen dan Aplikasi Menggunakan Matlab*. Yogyakarta: Andi

[4] Gorunescu, F. (2011). *Data Mining: Concept and Techniques.*

[5] Bai, Y dan Kobayashi, H. (2003). *Intrusion Detection System: Technology and Development.* AINA'03.

[6] Gujar, S. Shubhangi & Patil B. M. *Intrusion Detection Using Naive Bayes For Real Time Data*. Diakses 18 Agustus 2017. dari www.e-ijaet.org/media/33I20-IJAET0520947_v7_iss2_568-574.pdf.