Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware

Agus Riki Gunawan[1],Nyoman Putra Sastra[2], Dewa Made Wiharta[3]

Submission: 25-01-2021, Accepted: 25-02-2021

Abstract** - Computer networks connected to the internet provide a lot of convenience to access information from around the world. However, the connection between the network and the Internet actually increases the likelihood of system interference. Therefore we need a system that can be used as a layer of security on the web server data. The use of the Snort and honeypot systems is intended as a network monitoring system and to prevent attacks on the Udayana University network. To obtain accurate data as basic data to characterize the attacker's activity, literature research, observation and problem analysis are used. The Snort system and the Honeypot system are layered security systems that monitor the internal network 24 hours a day, therefore if there is any suspicious incoming data, the system will automatically provide information about attacks in the form of malware or hackers. The Snort system can detect 250,519 amounts of network data with 22 attributes and 212 types of network traffic. Snort system data is grouped based on working hours and outside working hours. The Honeypot system can block up to 248,574 attacks and 10 types of attacks, each of which has an attacker's IP address. Therefore, it can be concluded that the use of the snort and honeypot systems in this research application is very accurate and can be used as detection and prevention of attacks on the Udayana University network.

Keyword : snort, honeypot, detection, prevention, network, traffic

Abstrak** - Jaringan komputer yang terkoneksi dengan internet memberikan banyak kemudahan untuk mengakses informasi dari seluruh dunia. Namun, koneksi antara jaringan dan Internet justru meningkatkan kemungkinan gangguan sistem. Oleh karena itu diperlukan suatu sistem yang dapat digunakan sebagai pengamanan berlapis pada data web server. Penggunaan sistem Snort dan honeypot dimaksudkan sebagai sistem monitoring jaringan dan untuk mencegah serangan terhadap jaringan Universitas Udayana. Untuk mendapatkan data yang akurat sebagai data dasar untuk mengkarakterisasi aktivitas penyerang digunakan metode penelitian kepustakaan, observasi dan analisis masalah. Sistem Snort dan sistem Honeypot merupakan sistem keamanan berlapis yang akan memantau jaringan internal selama 24 jam sehari, oleh karena itu jika ada data masuk yang mencurigakan, sistem secara otomatis akan memberikan informasi mengenai serangan berupa malware atau peretas. Sistem Snort dapat mendeteksi 250.519 jumlah data jaringan dengan 22 atribut dan 212 jenis trafik jaringan. Data sistem snort dikelompokkan berdasarkan jam kerja dan diluar jam kerja. Sistem Honeypot dapat memblokir hingga 248.574 serangan dan 10 jenis serangan, yang masing-masing memiliki alamat IP penyerang. Oleh karena itu, dapat disimpulkan bahwa penggunaan sistem snort dan honeypot pada aplikasi penelitian ini sangat akurat dan dapat digunakan sebagai pendeteksi dan pencegahan serangan pada jaringan Universitas Udayana.

Kata kunci : snort, honeypot, mendeteksi, mencegah, jaringan, trafik

I. PENDAHULUAN

Jaringan komputer yang terkoneksi dengan internet memberikan banyak kemudahan untuk mengakses informasi dari seluruh dunia. Namun, koneksi antara jaringan dan Internet justru meningkatkan kemungkinan gangguan sistem. Komputer menjadi mudah diakses, dan ada risiko infiltrasi oleh orang yang ingin mengakses komputer. Akibatnya, sistem komputer terancam atau diserang. Hal ini sangat berbahaya bagi sistem komputer perusahaan yang berisi data rahasia dan hanya dapat diakses oleh orang tertentu.

Antisipasi perlu dilakukan terhadap bahaya virus atau *malware* yang dapat menyebabkan kerusakan pada komputer, server, atau jaringan komputer. Internet digunakan sebagai media penyebaran dimana behavior sangat mempengaruhi hal tersebut [1]. Indonesia sendiri menjadi salah satu negara di Asia Pasific dengan jumlah serangan *malware* tertinggi [2]

Tujuan dari penelitian ini yaitu menggunakan sistem *snort* dan *honeypot* untuk memonitoring terjadinya serangan tehadap *malware* dan attacker yang masuk pada jaringan kampus Universitas Udayana. Data port scanning oleh system *snort* dan *honeypot* terkumpul selama 1 bulan mulai bulan Februari 2020 – Maret 2020 menggunakan *Snort IDS* dan *Honeypot*. Dapat menjelaskan proses dan langkah-langkah pembangunan sistem *Honeypot* yang mirip dengan sistem produksi sebenarnya dan menggunakan log sebagai mekanisme pemantauan pada sistem *Honeypot* [3].

IDS berfungsi sebagai sistem keamanan jaringan dan komputer. IDS hanya cocok digunakan sebagai sistem keamanan. Namun, ini tidak dapat digun akan sebagai satu-satunya sistem untuk melindungi keamanan jaringan [4]

Honeypot adalah metode untuk membuat sistem palsu atau layanan palsu. Layanan dapat digunakan untuk memikat target yang buruk atau menolak pengguna yang dapat merusak sistem atau layanan [5]

Malware adalah software yang secara khusus dirancang untuk melakukan aktivitas berbahaya atau software perusak

[1] *Mahasiswa, Program Studi Magister Teknik Elektro, Fakultas Teknik, Universitas Udayana, Jalan gunung agung, Denpasar. Bali, 80118 INDONESIA (tlp: 087863031389; e-mail: agusriki3440@gmal.com)*
[2 3] *Dosen, Program Studi Magister Teknik Elektro, Fakultas Teknik, Universitas Udayana, Jln. Jalan Kampus Bukit Jimbaran 80361 INDONESIA (telp: 0361-703315; fax: 0361-4321; e-mail: putra.sastra@unud.ac.id, wiharta@unud.ac.id)*

P-ISSN: 1693-2951, e-ISSN : 2503-2372

lainnya (seperti Trojan horse, virus, spyware, dan exploit) [6]. *Malware* adalah perangkat lunak atau perangkat lunak yang dirancang untuk menyusup atau merusak sistem computer [7]. *Malware* termasuk virus, worm, trojan horse, sebagian besar rootkit, spyware, ransomware, dll. [8]

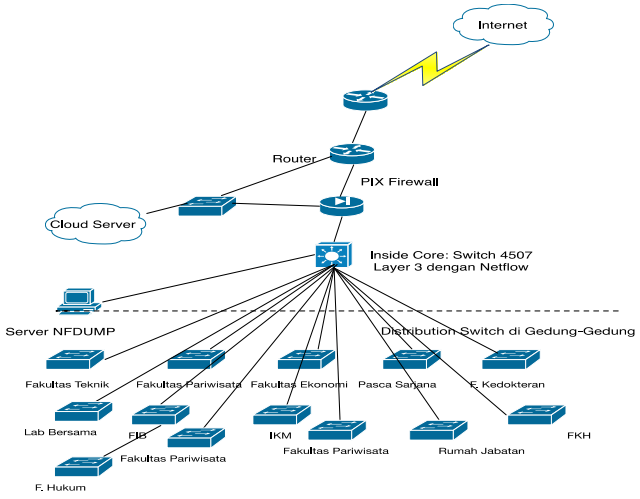
Ekstraksi data log secara visual dapat menampilkan pola distribusi serangan port scanning, sehingga mencerminkan perilaku penyerang di jaringan kampus Universitas Udayana. Melalui visualisasi ini, dapat membantu administrator jaringan mengambil tindakan preventif untuk melindungi jaringan yang mereka kelola. [9]

Penelitian yang dilakukan ini mengacu pada penelitian terdahulu yang dilakukan oleh 'Muh Masruri Mustofa dengan judul " Penerapan Sistem Keamanan Honeypot dan Snort IDS pada jaringan Nirkabel". Pada penelitian beliau menerapkan jaringan point to point yang tidak pada jaringan asli untuk menguji sistem tersebut. Hasil dari penelitian beliau adalah sistem Honeypot dapat merekam dan mengelabui penyerang dengan server palsu dalam bentuk file log, dan pada sistem Snort dapat memberikan rekaman trafik yang janggal keserver dalam bentuk file log atau alert.

II. KAJIAN PUSTAKA

A. *GDLN Universitas Udayana*

Lokasi Kampus Universitas Udayana terbagi menjadi 3 lokasi yaitu Kampus Universitas Udayana Bukit Jimbaran (Kampus Bukit), Kampus Univesitas Udayana Jalan PB. Sudirman (Kampus Sudirman) dan Kampus Universitas Udayana Jalan Pulau Nias (Kampus Nias). Konfigurasi akses pengguna Internet dipusatkan pada 2 tempat, yaitu Network Operation Center (NOC) di gedung Global Development Learning Network (GDLN) dan NOC Kampus Bukit Jimbaran (PUSKOM). Infrastruktur jaringan Universitas Udayana ditunjukkan pada Gambar 1.



Gambar 1: Infrastruktur Jaringan Kampus Sudirman Universitas Udayana.

Dapat dijelaskan bahwa router utama (main router) pada jaringan Kampus Sudirman terhubung dengan server cloud Universitas Udayana. Dari router BGP NOC yang ada di GDLN terhubung dengan perangkat cisco berupa router dan akan diteruskan ke router cisco yang lainnya sampai akhirnya akan didistribusikan ke masing-masing jaringan Universitas Udayana. Dari router GDLN akan terhubung dengan switch yang terdapat di masing-masing fakultas yang ada di Kampus Sudirman menggunakan media transmisi fiber optic, switch-switch terhubung ke jaringan LAN pada PC, jaringan Hot spot, dan jaringan VoIP.

B. *SNORT IDS (Intrusion Detection System)*

Snort merupakan sistem pencegahan dan deteksi intrusi jaringan bersifat open source dengan berbasis aturan (rule-driven) yang digunakan untuk memantau lalu lintas jaringan secara pasif dan memberikan peringatan atau alertketika ancaman terdeteksi [10]. *Snort* merupakan salah satu alat pada IDS dengan komunitas open source, sehingga *Snort* merupakan alat yang disukai untuk melindungi keamanan jaringan komputer [11]. Deteksi intrusi adalah proses memantau kejadian yang terjadi di sistem komputer atau jaringan dan menganalisis kemungkinan kejadian. Ada beberapa alasan untuk kejadian tersebut, seperti *malware* (seperti worm dan spyware) dan penyerang[12]. IDS digunakan untuk mendeteksi aktivitas yang mencurigakan dalam suatu sistem atau jaringan. [13].

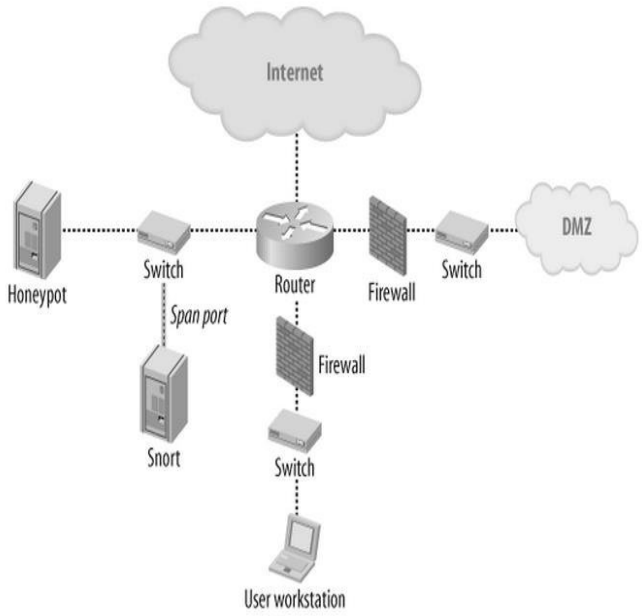
Snort bekerja mirip dengan TcpDump, tetapi berfokus pada sniffing paket yang aman. Fitur utama yang membedakan *Snort* dari TcpDump adalah pemeriksaan muatan. *Snort* menganalisis kumpulan aturan muatan yang disediakan. [14]

C. *Honeypot*

Honeypot adalah sistem atau komputer yang sengaja "dikorbankan" untuk menjadi sasaran serangan hacker [15]. Sistem dapat memberikan layanan untuk setiap serangan yang ditembus peretas ke dalam server. Metode ini dirancang untuk memungkinkan administrator server yang akan diserang untuk mengetahui teknik infiltrasi yang dilakukan oleh hacker, dan diharapkan dapat melindungi server yang sebenarnya.[16] *Honeypot* adalah sumber daya komputasi yang dibuat untuk menyerang, mengambil alih, mengakses, dan digunakan dengan berbagai cara yang tidak sah [17]. *Honeypot* adalah sumber daya keamanan yang dirancang untuk menyelidiki, menyerang, atau menghancurkan [18]

Honeypot dapat didefinisikan sebagai sumber daya sistem informasi yang dapat digunakan untuk mendeteksi kasus penggunaan sumber daya yang tidak sah atau tidak sah secara hukum [19]

Pada gambar 2. merupakan topologi penempatan *snort* dan *honeypot* pada suatu jaringan, dimana instalasi *snort* dan *honeypot* berada pada switch yang tersambung dengan router server. Pengguna jaringan akan masuk melalui router dan dilanjutkan ke switch yang sudah terinstall *snort* dan *honeypot*. Sehingga *snort* dan *honeypot* dapat medeteksi adanya pengguna yang mencurigakan atau tidak.

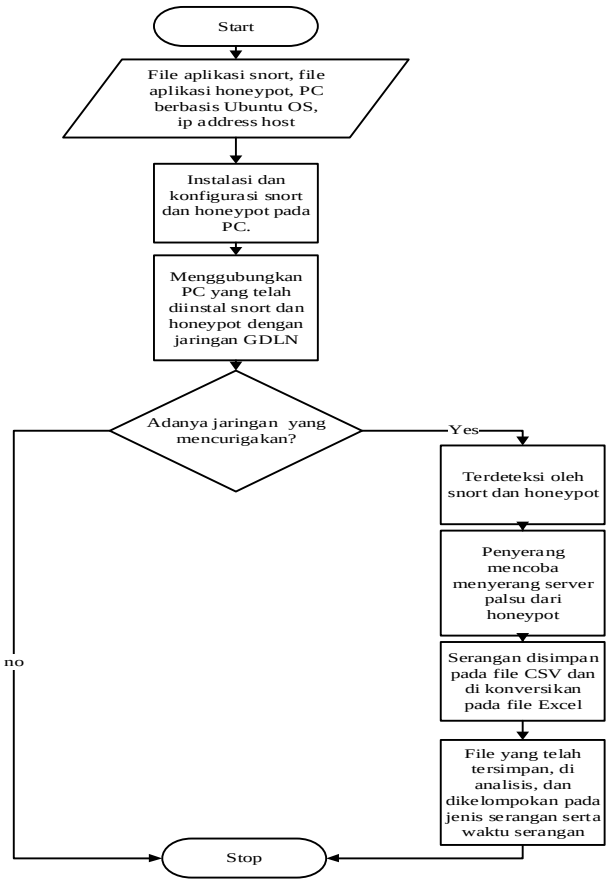


Gambar 2: Topologi Penempatan *Snort* dan *Honeypot* [20]

Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah pengumpulan data, studi pustaka, metode observasi serta analisis masalah. Pengumpulan data di mulai pada bulan februari 2020 - maret 2020 menggunakan aplikasi *snort* dan *honeypot* di install pada computer yang tersambung dengan jaringan kampus Universitas Udayana Sudirman, sehingga jalur internet akan melewati computer yang telah diinstall aplikasi *snort* dan *honeypot*. Setelah pengumpulan data, dilakukan studi pustaka agar mendapatkan konsep teoritis tentang masalah yang akan diteliti, dan pencarian sumber data di internet dan perpustakaan. Setelah melakukan studi pustaka, selanjutnya di lakukan observasi untuk pengamatan secara langsung pada objek yang diteliti meliputi instalasi, konfigurasi, tool yang dipakai dan pengujian koneksi terhadap internet. Selanjutnya di lakukan analisis permasalahan yang terjadi selama pengambilan data, dan memilah data penyerang sesuai jenis serangan.

Pada gambar 3. dapat dilihat cara kerja dari Snort dan Honeypot/ Honeyd saat melakukan pendeteksian. Mulai dari menjalankan Snort dan melakukan pendeteksian sampai dengan Snort selesai dijalankan ataupun dihentikan melakukan monitoring/ pendeteksian. Sehingga jika terdapat penyusupan pada jaringan internal, peran dari Honeypot adalah mengelabui peyerang seolah-olah terdapat server yang dapat di masukin dengan mudah.

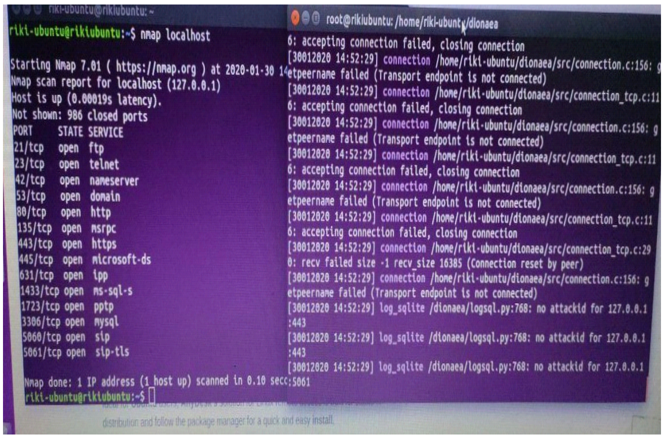


Gambar 3: Flowchart Implementasi *Snort* dan *Honeypot*.

III. HASIL DAN PEMBAHASAN

Penelitian ini menggunakan PC sebagai tempat instalasi sistem dengan operating sistem Ubuntu 16.04, ram 4GB, dan kapasitas harddisk 500GB. Instalasi snort membutuhkan 42,3 MB dengan format file penyimpanan adalah alert.csv, dan pada honeypot membutuhkan 32.7 MB dengan format dionaea.csv. PC yang telah terinstall snort dan honeypot di hubungkan pada server dengan IP 103.29.196.157, yang dimana jaringan akan melewati sistem snort dan honeypot sebelum masuk kedalam server.

Pada pengujian *Snort* IDS dan *Honeypot* menggunakan Nenmap dengan mencoba scaning port pada local host. Terdapat lokal host dengan port yang berbeda, dimana beberapa port dalam lokal host tersebut di buat oleh *honeypot* bertujuan untuk mengelabui penyerang. Sehingga disaat yang bersamaan *snort* mengcapture jaringan yang masuk pada server.



Gambar 4: Scaning Port Local Host

Pada gambar datas di tunjukan port yang telah di buat oleh *Honeypot* dan port yang memang dimiliki oleh server sendiri, sehingga penyerang tidak akan mengetahui port mana yang dimiliki oleh server aslinya.

D. Snort

Data yang digunakan pada penelitian ini adalah data alert.csv hasil dari Snort yang dipasang pada PC berbasis ubuntu 16.04 yang terpasang pada jaringan Kampus Sudirman Universitas Udayana sejak Februari 2020 hingga awal Maret 2020. Snort diaktifkan dengan command prompt syntax (*/usr/local/bin/snort -c /usr/local/etc/snort.conf*) pada Ubuntu 16.04, terhubung pada jaringan lokal kampus dengan IP 103.29.196.157. Jumlah data tersimpan selama periode tersebut adalah 250.519 data dengan 22 atribut yang disediakan Snort secara default. Data kemudian diekstraksi untuk mendapatkan data unique berdasarkan sig_gen, sig_id, sig_rev, msg, proto, src, dst,dan dstport.

TABEL I
DATASHEET AWAL BAGIAN 1

Timestamp	Sig_generator	Sig_id	Sig_rev	Message	Protocol	Src
1	2	3	4	5	6	7
02/04-11:14:05.473546	1	10000001	1	ICMP test detected	ICMP	129.232.219.209
02/04-11:14:12.221462	1	2001219	19	ET SCAN Potential SSH Scan	TCP	103.219.106.203
02/04-11:14:20.830806	1	2403480	55043	ET CINS Active Threat Intelligence Poor Reputation IP TCP group 91	TCP	89.248.174.193
02/04-11:15:13.396054	1	2402000	5441	ET DROP Dshield Block Listed Source group 1	TCP	185.175.93.14
02/04-11:15:59.200706	1	10000001	1	ICMP test detected	ICMP	54.249.13.241
02/04-11:16:00.795962	1	10000001	1	ICMP test detected	ICMP	3.112.7.249
02/04-11:16:10.375658	1	2001219	19	ET SCAN Potential SSH Scan	TCP	103.219.106.203

TABEL II
DATASHEET AWAL BAGIAN 1

Srcport	Dst	Dstport	Ethsrc
8	9	10	11
103.29.196.157	C4:64:13:29:1F:01	78:E3:B5:AB:16:B4	0x3C
51195	103.29.196.157	22	C4:64:13:29:1F:01
58079	103.29.196.157	10000	C4:64:13:29:1F:01
51324	103.29.196.157	49628	C4:64:13:29:1F:01
103.29.196.157	C4:64:13:29:1F:01	78:E3:B5:AB:16:B4	0x62
103.29.196.157	C4:64:13:29:1F:01	78:E3:B5:AB:16:B4	0x62
54423	103.29.196.157	22	C4:64:13:29:1F:01

TABEL III
DATASHEET AWAL BAGIAN 3

Ethsrc	Ethlen	Tcpflags	Tcpseq	Tcpack	Tcpln	Tcpwindow	Ttl	Tos	Id	Dgmlen
12	13	14	15	16	17	18	19	20	21	22
248	64	14577	34	348116	8	0	14577	0		
78:E3:B5:AB:16:B4	0x4A	******S*	0x558CE910	0x0	0x39308	52	80	23406	60	61440
78:E3:B5:AB:16:B4	0x3C	******S*	0x82318608	0x0	0xFFFF	248	64	54321	40	40960
78:E3:B5:AB:16:B4	0x3C	******S*	0x59D53A12	0x0	0x400	247	64	23539	40	40960
249	64	0	84	86016	8	0	4	14717		
28	64	0	84	86016	8	0	22	22658		
78:E3:B5:AB:16:B4	0x4A	******S*	0xBCF21709	0x0	0x39308	52	80	13175	60	61440
78:E3:B5:AB:16:B4	0x3C	******S*	0xEAD37D25	0x0	0xFFFF	248	64	54321	40	40960
248	64	54321	40	409600	8	0	44086	0		

Pada Tabel I, Tabel II, dan Tabel III. menunjukkan data alert yang digunakan dalam aturan ancaman yang muncul dalam *snort* bersifat dinamis dan sering diperbarui. Ancaman "*ET DROP Dshield Block Listed Source group 1*" adalah salah satu ancaman utama yang diperbarui secara berkala dan merupakan daftar alamat IP yang buruk. Alamat IP ini dapat ditandai buruk dari berbagai sumber.

E. Visualisasi

Visualisasi data log dilakukan berdasarkan jenis layanan dan alert rate. Alert rate merupakan frekuensi munculnya alert setiap layanan pada data log IDS *Snort.* Adapun jenis layanan dan frekuensinya ditunjukkan pada diagram pie dibawah.

TABEL IV
VISUALISASI DATA LAYANAN

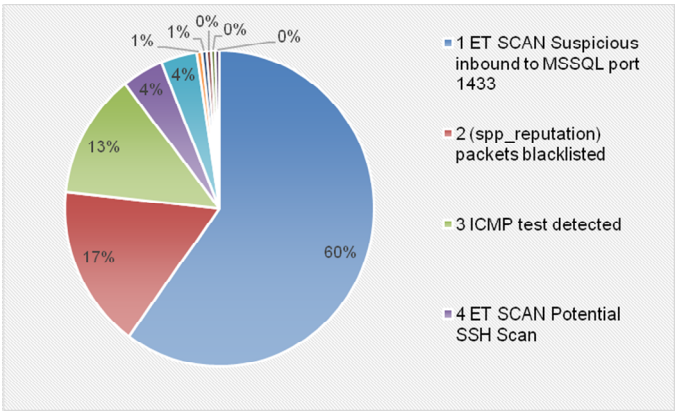
No	Jenis Layanan	Frekuensi Layanan	Persentase Layanan (%)
1	ET SCAN Suspicious inbound to MSSQL port 1433	125749	50%
2	(spp_reputation) packets blacklisted	50988	20%
3	ICMP test detected	31030	12%
4	ET DROP Dshield Block Listed Source group 1	10458	4%
5	ET SCAN Potential SSH Scan	9676	4%
…	…	…	…
208	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 29	1	0%
209	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 3	1	0%
210	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 46	1	0%
211	ET TOR Known Tor Relay/Router (Not Exit) Node TCP Traffic group 63	1	0%
212	MALWARE-CNC Win.Trojan.ZeroAccess inbound connection	1	0%

Terlihat pada Tabel IV. bahwa *Snort* IDS berhasil mendeteksi dan mencatat 212 jenis layanan berbeda. Layanan dengan alert rate tertinggi adalah *ET SCAN Suspicious inbound to MSSQL port 1433* memiliki persentase 50% merupakan system mencurigakan yang masuk melalui port 1433 menggunakan *MSSQL*, pada jenis layanan (spp_reputation) *packets blacklisted* memiliki persentase 20% merupakan paket yang dianggap mencurigakan yang masuk melalui jaringan lokal, pada jenis layanan *ICMP test detected* memiliki persentase 12% untuk mengirim berbagai jenis pesan tingkat rendah tentang kelainan yang terdeteksi selama koneksi jaringan, pada jenis layanan *ET DROP Dshield Block Listed Source group 1* memiliki persentase 4%, pada jenis layanan *ET SCAN Potential SSH Scan* memiliki persentase 4% dan 9 jenis layanan memiliki 1% nilai dari 9 jenis layanan terbanyak. Sedangkan jenis layanan dari nomor 10 hingga 212 memiliki rate dibawah 400 dan memiliki frequensi dibawah 0.001 yang merupakan jenis layanan tidak berbahaya bagi sistem. Sehingga *system SNORT IDS* sudah dapat mendeteksi berbagai jenis layanan pada jaringan dari layanan berbahaya hingga tidak berbahaya.

F. Layanan pada jam kerja dan tidak kerja

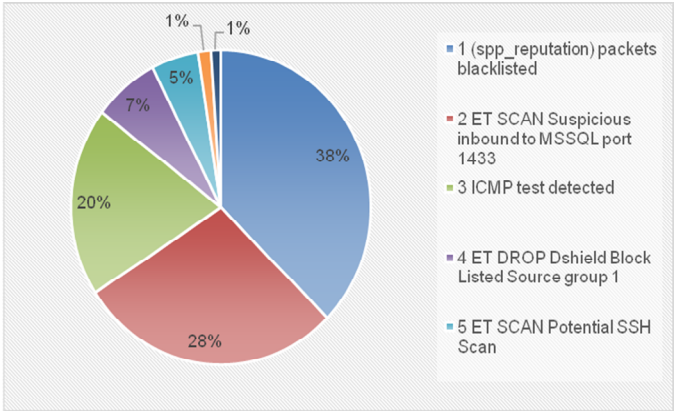
Layanan ini merupakan data penyerangan pada jam kerja dan jam tidak kerja, rentang waktu pada jam kerja adalah jam 8.00 pagi hingga jam 17.00 sore, dan pada jam tidak kerja adalah jam 17.00 sore hingga jam 8.00 pada tanggal 4 februari hingga 4 maret 2020.

P-ISSN: 1693-2951, e-ISSN : 2503-2372



Gambar 5. Grafik layanan pada jam kerja

Pada gambar 5 layanan pada jam kerja dengan jenis layanan *ET SCAN Suspicious inbound to MSSQL port 1433* memiliki persentase 60%, pada jenis layanan *(spp_reputation) packets blacklisted* memiliki persentase sebesar 17% ini merupakan ip yang dianggap berbahaya, pada layanan *ICMP test detected* memiliki persentase sebesar 13% yang merupakan ping dari client menuju server. Pada jam kerja, lalulintas jaringan lebih banyak pada ping dari *MSSQL port 1433.*



Gambar 6. Grafik Layanan Jam Tidak Kerja

Pada gambar 6, pada jam tidak kerja dengan jenis layanan *(spp_reputation) packets blacklisted* memiliki persentase 38%, Jenis layanan *ET SCAN Suspicious inbound to MSSQL port 1433* memiliki persentase 28%, *ICMP test detected* memiliki persentase 20%, dan *"ET DROP Dshield Block Listed Source group 1*" memiliki persentase 7%.

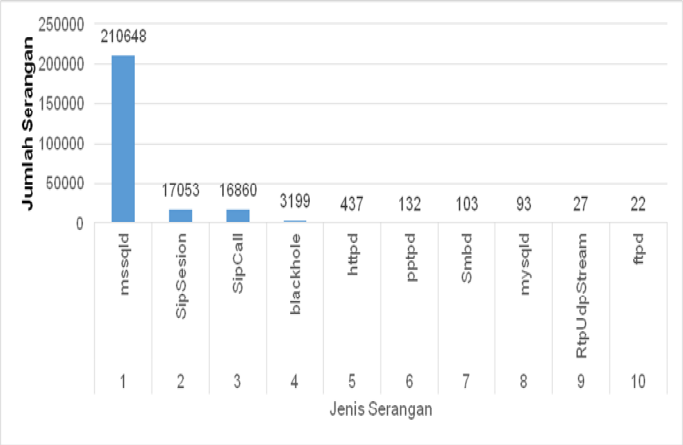
G. Honeypot

Pada system *honeypot* data yang digunakan dalam penelitian ini merupakan data serangan yang disimpan oleh sistem *honeypot* yang telah dipasang pada Server jaringan gedung GDLN Kampus Sudirman Universitas Udayana sejak Februari 2020 hingga awal Maret 2020. Log file yang dihasilkan sistem *honeypot* kemudian dirubah kedalam bentuk CSV file dengan jumlah data yang diperoleh selama periode tersebut mencapai 248.574 data serangan dengan 11 atribut. Adapun data serangan yang telah diperoleh dapat dilihat pada Tabel V.

TABEL V
DATA SHEET AWAL

connection	connection_type	connection_transport	connection_protocol	connection_timestamp	connection_root	connection_parent	local_host	local_port	remote_host	remote_port
1	2	3	4	5	6	7	8	9	10	11
503	accept	tcp	mssqld	1.57E+09	503		103.29.196.157	1433	103.29.249.70	59537
504	accept	tcp	mssqld	1.57E+09	504		103.29.196.157	1433	103.29.249.70	59609
505	accept	tcp	mssqld	1.57E+09	505		103.29.196.157	1433	103.29.249.70	59648
506	accept	tcp	mssqld	1.57E+09	506		103.29.196.157	1433	103.29.249.70	59827
507	accept	tcp	mssqld	1.57E+09	507		103.29.196.157	1433	103.29.249.70	59871
508	accept	tcp	mssqld	1.57E+09	508		103.29.196.157	1433	103.29.249.70	60017
509	accept	tcp	mssqld	1.57E+09	509		103.29.196.157	1433	103.29.249.70	60112
510	accept	tcp	mssqld	1.57E+09	510		103.29.196.157	1433	103.29.249.70	60231
511	accept	tcp	mssqld	1.57E+09	511		103.29.196.157	1433	103.29.249.70	60358
512	accept	tcp	mssqld	1.57E+09	512		103.29.196.157	1433	103.29.249.70	60383
513	accept	tcp	mssqld	1.57E+09	513		103.29.196.157	1433	103.29.249.70	60402
514	accept	tcp	mssqld	1.57E+09	514		103.29.196.157	1433	103.29.249.70	60424

Data yang digunakan pada penelitian ini adalah data *dionaea.csv* hasil dari honeypot yang dipasang pada PC berbasis ubuntu 16.04 yang terpasang pada jaringan Kampus Sudirman Universitas Udayana sejak Februari 2020 hingga awal Maret 2020. Honeypot diaktifkan dengan command prompt syntax *(/opt/dionaea/bin/dionaea -c /opt/dionaea/etc/dionaea/dionaea.cfg*) pada Ubuntu 16.04, terhubung pada jaringan lokal Universitas Udayana dengan IP 103.29.196.157. Honeypot yang telah aktif akan memberikan beberapa port palsu untuk mengelabui dan dikorbankan kepada penyerang, dengan maksud server asli akan tetap aman. Adapun visualisasi data serangan terhadap jenis layanan dengan frekuensi serangannya dapat dilihat pada gambar 7.



Gambar 7. Visualisasi frekuensi serangan terhadap jenis layanan.

Pada gambar 7 menunjukan besarnya serangan terhadap jenis layanan dengan 248.574 jumlah serangan pada bulan februari hingga maret.

Jenis serangan *mssqld* dengan jumlah serangan sebanyak 210.648 yang merupakan metode serangan yang akan membuat aplikasi menunjukan error ketika mengakses database. Pada error ini si penyerang akan mempelajari informasi sistem seperti Database, Versi Database, Sistem Operasi, dan lain sebagainya.

Pada jenis serangan *SIPSession (Session Initiation Protocol)* memiliki jumlah serangan sebanyak 17053 yang merupakan protokol yang digunakan untuk membuat, kelola dan akhiri sesi di jaringan berbasis IP. Sesi jaringan berbasis IP dapat berupa telepon sederhana atau bisa menjadi sesi konferensi (seperti aplikasi zoom dan unud conference).

Pada jenis serangan *SipCall* memiliki jumlah serangan sebanyak 16860 yang merupakan Serangan yang dilakukan oleh penyerang menggunakan serangan SIPcall yang secara bersamaan dalam jumlah banyak, dimana SIP adalah VoIP untuk *honeypot*.

Pada jenis serangan *Blackhole* memiliki jumlah serangan sebanyak 3199 yang merupakan sejenis serangan *Denial of Service (DoS)* pada *Honeypot*, dimana data berbahaya menyatakan kepada sumber bahwa data tersebut memiliki rute terbaik untuk mencapai tujuan.

Sedangkan pada jenis serangan *Httpd* memiliki jumlah serangan sebanyak 437 dibuat untuk mensimulasikan layanan di server asli, sehingga penyerang akan menganggap sudah dapat masuk kedalam server aslinya. Sehingga dapat disimpulkan bahwa 5 jenis serangan diatas merupakan serangan berbahaya bagi data serta sistem.

TABEL IV
INFORMASI PENYERANG

Jenis Serangan	Ip Address	Perusahaan/ Komunitas	Negara
Mssqld	103.29.249.70	18A/19,DODDANEKUNDI (gbbn.co.in)	Mormugao, Goa, India
	103.29.117.167	AS131442 Digital Network Associates Pvt Ltd	Pālghar, Maharashtra, India
SipSession	103.48.25.59	NetSat Private Limited (netsat.net.pk)	Karachi, Sindh, Pakistan
	103.29.220.132	Touch Net India Pvt. Ltd. (touchnetindia.net)	Najafgarh, Delhi, India
	103.122.66.107	PT. Jinom Network Indonesia	Kebomas, East Java, Indonesia
	37.49.230.60	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	77.247.109.61	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	77.247.109.59	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	13.77.161.15	Microsoft Corporation (microsoft.com)	Quincy, Washington, United States
	172.15.0.1	AT&T Corp. (att.com)	Lausanne, Vaud, Switzerland
SipCall	37.49.230.60	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	77.247.109.61	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	77.247.109.59	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
	13.77.161.15	Microsoft Corporation (microsoft.com)	Quincy, Washington, United States
	77.247.108.16	ABC Consultancy (abcconsultancygroup.com)	Amsterdam, North Holland, Netherlands
Blackhole	184.69.150.210	Shaw Communications Inc. (shaw.ca)	Vancouver, British Columbia, Canada
	94.43.254.154	SILKNET BROADBAND (silknet.com)	Tbilisi, T'bilisi, Georgia
	178.245.151.35	TURKCELL INTERNET (turkcell.com.tr)	İzmir, İzmir, Turkey
	202.82.16.126	LKWFSL Lau Wong Fat Sec School (pccw.com)	Hong Kong, Central and Western, Hong Kong
	218.164.52.118	Chunghwa Telecom Co.,Ltd.nNo.21-3, Sec. 1, Xinyi Rd., Taipei 10048, Taiwan, R.O.C.nTaipei Taiwan (cht.com.tw)	Kaohsiung, Takao, Taiwan
Httpd	218.25.89.94	China Unicom Liaoning province network (chinaunicom.cn)	Shenyang, Liaoning, China
	103.9.124.70	PT Global Teknologi Teraindo (globalmta.biz.id)	Jakarta, Jakarta, Indonesia
	157.230.216.203	DigitalOcean, LLC (digitalocean.com)	North Bergen, New Jersey, United States
	104.248.255.89	DigitalOcean, LLC (digitalocean.com)	Frankfurt am Main, Hesse, Germany
	156.96.155.240	NEWTREND (fastlink.net)	Philadelphia, Pennsylvania, United States

System *Honeypot* mendeteksi IP address pada setiap jenis serangan, pada setiap jenis serangan terdapat 5 IP address tertinggi. Pada IP address setiap jenis serangan ditemukan bahwa IP address tersebut dari luar jaringan lokal Universitas udayana. Terdapat 4 IP address dengan organisasi dan negara yang sama, yaitu IP address 37.49.230.60, 77.247.109.61, 77.247.109.59, 77.247.108.16 merupakan penyerang dari organisasi *ABC Consultancy (abcconsultancygroup.com)* di Negara Amsterdam dengan jumlah serangan sebanyak 32.768 serangan.

IV. KESIMPULAN

Berdasarkan penelitian yang telah di lakukan tentang "Penerapan Keamanan Jaringan Menggunakan Sistem Snort dan Honeypot Sebagai Pendeteksi dan Pencegah Malware" dapat simpulkan bahwa Sistem Snort dapat mendeteksi 250.519 data dengan 22 atribut layanan dan dibagi berdasarkan jam kerja dan jam tidak kerja.

Honeypot dalam penelitian ini dapat mencegah 248.574 data serangan dengan 11 atribut, yang setiap atributnya dapat mendeteksi IP penyerang dan tanggal penyerangan.

System snort dan honeypot dapat dijalankan pada background server agar tidak membebani kinerja dan performa dari server jaringan. Dengan penerapan system snort dan honeypot dapat memberikan keamanan berlapis selama 24 jam secara otomatis dan dapat dipantau secara berkala, sehingga dapat diaplikasikan pada jaringan yang lebih besar.

Sehingga penerapan system snort dan honeypot sangat tepat dengan fungsi dari system snort sebagai monitoring jaringan server dan honeypot sebagai pencegahan serangan pada jaringan Universitas Udayana.

V. SARAN

1. Agar pemanfaatan sistem lebih bisa mencakup keseluruhan jaringan dilakukan monitoring tidak hanya pada server, tetapi pada router juga. Sehingga data yang di dapatkan lebih bervariasi dari penelitian ini.
2. Diterapkan sistem notifikasi ancaman dan serangan dari sistem snort dan honeypot melalui social media agar administrator dapat mengetahui dan melakukan tindakan secara cepat. Penerapan sistem notifikasi dapat berupa Web BASE, Whatsapp, Telegram, Email, atau Tweeter.

VI. DAFTAR PUSTAKA

[1] Black,Scott. 2013. "*Malware, Spyware, Adware, And Viruses"*. USA:Clark College

[2] Mawudor, Bright G. 2015. *Continuous Monitoring Methods as a Mechanism for Detection and Mitigation of Growing Threats in Banking Security Systems"* Korea:https://www.researchgate.net/publication/307801986

[3] Julianto, Sulistiono. 2006. *Honeypot sebagai alat bantu pendeteksi serangan pada sistem pengolahan keamanan jaringan*. Depok:Universitas Gunadarma.

[4] Arief, Rudiyanto M. 2005. "*Penggunaan sistem IDS untuk pengamanan jaringan dan computer"*. Yogyakarta: STMIK Amikom.

[5] Nugroho, Ardianto Setyo. 2013. *Analisis Dan Implementasi Honeypot Menggunakan Honeyd Sebagai Alat Bantu Pengumpulan Informasi Aktivitas Serangan Pada Jaringan.Institut Sains & Teknologi*. Yogyakarta: AKPRIND.

[6] Kramer, S., & Bradfield, J. C. 2010. *A general definition of malware. Journal in Computer Virology*, 6(2), 105–114. http://doi.org/10.1007/s11416-009- 0137-1

[7] Cahyanto, Triawan A. 2017. *Analisis dan Deteksi Malware Menggunakan Metode Malware Analisis Dinamis dan Malware Analisis Statis*. Jember:JUSTINDO.

[8] M. Kalash, M. Rochan, N. Mohammed, N. D. B. Bruce, Y. Wang, and F. Iqbal. 2018. *Malware Classification with Deep Convolutional Neural Networks,"* 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur., pp. 1–5, 2018.

[9] Raditya A.H. 2015. *Implementasi Honeypot Untuk Mengungkap Pola Port Scanning Attack Dalam jaringan*. Yogyakarta. Univesitas Gajah Mada

[10] Shinta Dewi I.A. 2020. *Analisis Data Log IDS Snort dengan Algoritma Clustering Fuzzy C-Means.* Bali:Universitas Negeri Udayana.

[11] P. L. Restanti. 2014. *Analisis Kolaborasi IDS Snort dan Honeypot*. Semarang:Universitas Dian Nuswantoro

[12] Scarfone, Karen,Peter Mell. 2007. *Guide to Intrusion Detection and Prevention Systems (IDPS)*.US:NIST

[13] Jutono Gondohanindijo. 2011. *Sistem Untuk Mendeteksi Adanya Penyusup (IDS Intrusion Detection System)*.Semarang:Majalah Ilmiah Informatika.

[14] E.K.Dewi. 2016. *Model rancangan Keamanan Jaringan Dengan Menggunakan Proses Forensik*. Kediri:Jurnal Maklumatika.vol.2, p.34.

[15] Mustofa, Muh M. 2013. *Peneapan Sistem Keamanan Honeypot dan IDS Pada Jaringan Nirkabel (Hotspot)*. Yogyakarta.Jurnal Sarjana Teknik Informatika

[16] Akhriana A. 2019. "*Web App Pendeteksi Jenis Serangan Jaringan Komputer dengan Memanfaatkan Snort Dan Log Honeypot"*. Makasar:STMIK

[17] Spitzner, Lance. 2002. *Honeypots: Tracking Hackers*. Addison-Wesley Professional

[18] F. Utdirartatmo. 2005. *Trik Menjebak Hacker Dengan Honeypot*. Yogyakarta:Andi.

[19] Yulianto, Fazmah Arif. 2003. *Honeypot Sebagai Alat Bantu Pendeteksian Serangan pada Jaringan Komputer*. Indonesia : ITB

[20] Mustofa,M.M dan Aribowo,E. (2013). *Penerapan Sistem Keamanan Honeypot Dan IDS Pada Jaringan Nirkabel (Hotspot).*Yogyakarta:.Jurnal Sarjana Teknik Informatika