Terakreditasi SINTA Peringkat 2
Surat Keputusan Dirjen Penguatan Riset dan Pengembangan Ristek Dikti No. 10/E/KPT/2019
masa berlaku mulai Vol. 1 No. 1 tahun 2017 s.d Vol. 5 No. 3 tahun 2021

Terbit online pada laman web jurnal: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 5 No. 1 (2021) 180 - 186 ISSN Media Elektronik: 2580-0760

Keamanan Jaringan dengan Cowrie Honeypot dan Snort Inline-Mode sebagai Intrusion Prevention System

Tati Ernawati[1], Fikri Faiz Fadhlur Rachmat[2]
[1,2]Program Studi Teknik Informatika, Politeknik TEDC Bandung
[1]tatiernawati@poltektedc.ac.id, [2]faizfikri88@gmail.com

Abstract

Computer network systems have been designing to share resources. Sharing resources process, data security, and confidentiality are main issues in anticipating misuse of the access to information by unauthorized parties. The solution to anticipating these problems is the availability of a security system capable of handling various intruders who threaten the system and protect network resources. This study builds and analyzes the performance of computer network security using cowrie honeypot and snort inline-mode as an Intrusion Prevention System (IPS). The development process goes through the stages of analysis, design, implementation, and monitoring. The content analysis method has been using to explore the problems and requirements of the system built. The security system was build by configuring the IP address and network system devices (server, remote admin, client attacker). The test has been carrying out on 3 test parameters (confidentiality, availability, and integrity), comparison testing method has been using to test the integrity parameters. The test results indicate that the system functionality test for user needs have fulfilled, the results of the confidentiality test (83.3%), availability (93.3%), and the integrity of the inline-mode snort show faster response time (0.069 seconds on average) and more CPU resource usage efficient (0.04% average) than the cowrie honeypot. IPS snort inline-mode overall integrity parameter testing is more recommended for used network security systems than cowrie honeypots.

Keywords: Cowrie Honeypot, Snort Inline-mode, Intrusion Prevention System, Network security

Abstrak

Sistem jaringan komputer dirancang dengan tujuan dapat berbagi sumberdaya untuk dipakai secara bersama. Pada proses berbagi sumberdaya, keamanan dan kerahasian data menjadi isu utama dalam mengantisipasi penyalahgunaan akses informasi oleh pihak yang tidak berwenang. Solusi untuk mengantisipasi permasalahan tersebut yaitu ketersediaan sistem kemananan yang mampu menangani berbagai penyusup yang mengancam sistem dan melindungi sumber daya jaringan. Penelitian ini membangun dan menganalisis kinerja keamanan jaringan komputer menggunakan cowrie honeypot dan snort inline-mode sebagai Intrusion Prevention System (IPS). Proses pembangunan melalui tahapan analisis, desain, implementasi dan monitoring. Metode analisis konten *(content analysis*) digunakan dalam menggali permasalahan dan kebutuhan sistem yang dibangun. Sistem keamanan dibangun dengan melakukan konfigurasi terhadap IP address dan perangkat sistem jaringan (server, remote admin, client attacker). Pengujian dilakukan pada 3 parameter uji (confidentialitas, availabilitas dan integritas), metode *comparison testing* digunakan untuk menguji parameter *integritas*. Hasil uji mengindikasikan uji fungsionalitas sistem terhadap kebutuhan pengguna adalah terpenuhi, hasil uji confidentialitas (83,3%), availabilitas (93.3%) dan integritas untuk snort inline-mode menunjukkan respon time lebih cepat (rata-rata 0.069 detik) dengan penggunaan resources CPU lebih efisien (rata-rata 0.04%) dibandingkan cowrie honeypot. Uji parameter integritas secara keseluruhan IPS snort inline-mode lebih direkomedandasikan untuk digunakan dalam sistem keamanan jaringan dibandingkan cowrie honeypot.

Kata kunci: Cowrie Honeypot, Snort Inline-mode, Intrusion Prevention System, Keamanan Jaringan

1. Pendahuluan

Perkembangan jaringan internet di Indonesia semakin meningkat. Pada tahun 2019 penggunaan jaringan internet mencapai 196,71 juta jiwa atau setara dengan 73,7% dari total jumlah penduduk di Indonesia 266,91 juta jiwa (naik 8,9% dibandingkan tahun 2018) [1]. Internet telah membantu manusia dalam bertukar informasi, tetapi tidak semua informasi bersifat terbuka dan dapat diakses secara bebas. Disisi lain, pengguna berusaha untuk mengakses informasi tersebut meskipun tidak memiliki akses sehingga diperlukan sistem

Diterima Redaksi: 11-01-2021 | Selesai Revisi: 26-02-2021 | Diterbitkan Online: 28-02-2021

keamanan jaringan untuk melindungi sumber daya jaringan (hak akses, data/informasi, perangkat lunak dan/atau perangkat keras) untuk mencegah penggunaan dari berbagai penyusup yang dapat mengancam sistem [2]. Sistem jaringan komputer dirancang dengan tujuan dapat berbagi sumberdaya untuk dipakai secara bersama. Pada proses berbagi sumberdaya, keamanan dan kerahasian data menjadi isu utama, sehingga apabila terjadi serangan *cyber* akan menyebabkan kerugian [3]. Hal penting yang perlu diperhatikan adalah *Confidentiality*, *Integrity* and *Availability* (CIA) yang merupakan standar untuk mengevaluasi dan menerapkan keamanan informasi [4].

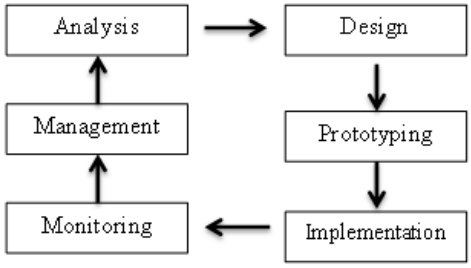
Upaya menghadapi permasalahan keamanan jaringan dapat dibantu dengan penerapan *firewall* namun kurang optimal dalam mendeteksi penyusupan. *Honeypot* dapat mendeteksi penyusupan dengan memanipulasi *port* yang dijadikan sebagai perangkap/umpan dalam jaringan untuk mengelabui *attacker*, mengumpulkan *log*/*malware* dan aktivitas *attacker* [5]. *Cowrie* adalah jenis *honeypot* meniru *Secure Shell* (SSH) pada *server*, memiliki kredensial *login* yang lemah dan mudah dibaca, sehingga *attacker* terperangkap pada zona dimana server tiruan dibuat. Tools *Intrusion Detection System* (IDS) lainnya untuk mendeteksi penyusupan adalah *snort*, mampu melakukan analisis lalu lintas waktu-nyata dan *logging* paket pada jaringan *Internet Protocol* (IP) [6]. *Snort* memiliki *inline-mode* sebagai *Intrusion Prevention System* (IPS) dalam melakukan pencegahan penyusupan, memblok semua akses pada jaringan yang dicurigai pada sebuah aktivitas jaringan. IPS berperan sebagai *firewall* dikombinasikan dengan IDS mendeteksi dengan cara mengijinkan atau blok paket secara mendetil [7].

Beberapa studi telah mengkaji terkait keamanan jaringan menggunakan IPS *cowrie honepot* dan *snort inline-mode*. [8] memodifikasi konfigurasi default variabel *cowrie* untuk meningkatkan kemampuan *cowrie*, hasil studi memberikan informasi terkait peningkatan kemampuan c*owrie*. Sementara itu [9] melakukan eksperimen menggunakan program *cowrie* untuk melindungi *port* SSH yang terbuka di *server* infrastruktur jaringan perbankan, hasil percobaan *cowrie* mampu mengidentifikasi tindakan penyerangan. [10] menganalisis aktivitas berbahaya (*malicious activity*) menggunakan *honeyport cowrie* (*linux host*), dionaea (*windows host*) dan *glastopf* (*web application*), hasilnya *honeypots* berhasil mendapatkan indikasi *malware* lebih banyak. [11] mengimplementasikan *snort-inline mode* sebagai IPS dengan notifikasi secara *realtime*, hasil eksperimen menunjukkan serangan dapat dideteksi, dilakukan pencegahan (*drop* akses ilegal). Kajian [12] melakukan komparasi *snort mode inline* dengan netfilter, hasil eksperimen menunjukan bahwa *snort* dapat mencegah serangan *pink attack* dengan sangat baik.

Tujuan studi ini adalah merancang dan mengimplementasikan sistem keamanan jaringan berdasarkan prinsip *confidentialitas, integritas, availabilitas system*. Tools yang digunakan adalah *cowrie honepot* dan *snort inline-mode* sebagai IPS. *Honeypo*t akan melakukan pengalihan akses dan *snort inline-mode* melakukan pemblokiran akses *attacker* yang mencoba masuk pada sistem. Hasil studi dapat dijadikan sebagai panduan/pedoman bagi pengguna yang memerlukan, terutama admin jaringan dalam merancang dan mengimpelentasikan sistem keamanan jaringan.

2. Metode Penelitian

Metodologi *Network Development Life Cycle* (NDLC) dalam [13] digunakan penulis dalam mengkaji, terdiri dari 6 (enam) tahapan yaitu *Analysis, Design, Simulation Prototype, Implementation, Monitoring*.



Gambar 1. Tahapan metodologi NDCL [13]

Tahap analisis, meliputi analisis permasalahan yang timbul, analisis kebutuhan sistem serta aplikasi pendukung yang lain. Permasalahan serta kebutuhan sistem (kebutuhan perangkat keras dan perangkat lunak untuk *server* serta *client*) diperoleh dengan metode analisis konten (*content analysis*) dari bermacam rujukan bersumber pada permasalahan yang diteliti.

Pada tahap desain akan dibuat topologi jaringan skala kecil antara *server* dan *attacker*, selanjutnya dilakukan simulasi kinerja awal pada jaringan dengan bantuan tools simulasi *packet tracer*. Hasil simulasi menjadi dasar dilakukan proses instalasi langsung pada server *Virtual Private Server* (VPS)

Tahap *implementation* difokuskan pada penginstalan sistem dan aplikasi pendukung serta konfigurasinya sesuai dengan kebutuhan. Penerapan IPS dikerjakan setelah instalasi *server cloud*, instalasi dan konfigurasi c*owrie honepo*t dan s*nort inline-mode* mencakup konfigurasi terhadap *IP address* dan perangkat sistem jaringan *(server, remote admin, client attacker).*

Tahapan monitoring, pelaksanaan monitoring dilakukan melalui pemantauan dan pengamatan selama percobaan/eksperimen pada kinerja IPS berdasarkan skenario pengujian. Parameter uji yang digunakan adalah confidentialitas, availibilitas dan integritas. Metode *comparison testing* digunakan dalam pengujian parameter integritas. Hasil tahapan ini dijadikan dasar

DOI: https://doi.org/10.29207/resti.v5i1.2825

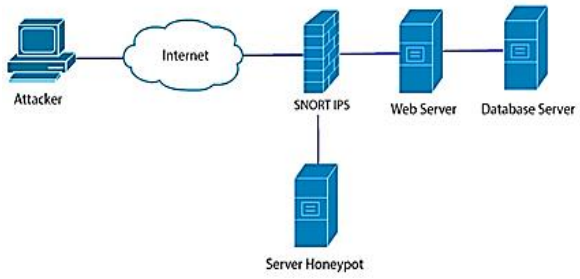
bagi penulis untuk menentukan IPS terbaik dalam membangun sistem keamanan jaringan komputer.

Tahap management tidak dilakukan karena terkait dengan kebijakan (*policy*) level management dan strategi bisnis.

3. Hasil dan Pembahasan

Hasil studi yang dicapai oleh penulis yaitu sistem keamanan jaringan menggunakan *cowrie honepot* dan *snort inline-mode* sebagai IPS.

3.1. Topologi Jaringan



Gambar 2. Topologi Jaringan yang akan dibangun

Gambar 2, s*erver* dibangun menggunakan layanan *cloud*, admin dapat mengakses *server* (*system cloud*) untuk keperluan administrasi jaringan. *Attacker* mengakses sistem melalui jaringan nirkabel. *Snort inline-mode* sebagai IPS akan berada pada posisi di depan server, server dibedakan menjadi 3 diantaranya *server honeypot* (*server* palsu), *web server* dan *database server*. Apabila *attacker* berusaha menyerang *server* utama, *honeypot* akan menyamar sebagai *server* utama yang bertugas untuk melayani kebutuhan *attacker*, sehingga *honeypot* dapat monitoring kegiatan yang dilakukan *attacker*.

3.2. Kebutuhan perangkat jaringan

Spesifikasi perangkat keras dibedakan peruntukannya untuk *server* dan *client*. Sementara untuk perangkat lunak yang digunakan terdiri dari *Linux Ubuntu 18.10, Cowrie Honeypot, Snort Inline-mode 2.9.7, Bitvise Client 7.45,Hydra dan Slowloris.*

3.3. Tahap Konfigurasi

Tahap konfigurasi IP *Address*, PC 1 (Admin) diberi alamat IP sesuai dengan yang diberikan oleh *provider*. *Server* memiliki IP *Address* 128.199.209.247 dengan Subnet mask 255.255.192.0 dan gateway 128.199.192.1. IP *Address* pada *attacker* tidak ditentukaan dikarenakan akan dilakukan beberapa percobaan dengan alamat IP yang berbeda (Tabel 1).

Tabel 1. IP Address Jaringan

Device	IP *Address*	*Subnet Mask*	*Default Gateway*
PC 1 (Admin)	-	-	-
PC 2 (*Server*)	128.199.209.247	255.255.192.0	128.199.192.1
PC 3 (*Attacker*)	-	-	-

Konfigurasi perangkat jaringan terdiri dari 3 (tiga) proses yaitu konfigurasi *server*, *remote admin* dan *client attacker*. Konfigurasi *server* mencakup proses registrasi yaitu menyewa *cloud* VPS *DigitalOcean* kemudian proses instalasi *cloud server Ubuntu*, c*owrie honeypo*t dan s*nort inline-mode*. Konfigurasi *remote admin* dilakukan untuk akses server dari jarak jauh menggunakan *bitvise client.* Konfigurasi *client attacker* menggunakan sistem operasi linux dan *tools hydra* sebagai penyerang pada *port* SSH, metode penyerangan yang digunakan yaitu *brute force attack*, sementara itu *slowloris* berperan sebagai penyerang pada sumber daya server/serangan *Distributed Denial of Services* (DDoS).

3.4. Tahap Pengujian

Skenario penyerangan yang akan dilakukan untuk menguji sistem keamanan jaringan yang dibangun, jenis serangan yang digunakan adalah *Brute Force Attack* dan *DDoS*. Pada penyerangan mengacu pada tujuan keamanan jaringan yang terdiri dari 3 skenario dimana serangan dilakukan oleh penguji bukan dari pihak luar (Tabel 2).

Tabel 2. Skenario Penyerangan

Jenis Skenario	Jenis Serangan	Keterangan
Skenario 1	*Brute Force Attack*	Untuk mengetahui tingkat *confidentialitas* atau kerahasiaan data pada sistem yang dibangun.sistem. Aplikasi serangan *brute force attack* menggunakan *hydra*
Skenario 2	DDoS	Untuk mengetahui tingkat *availibiltas* atau ketersediaan data pada sistem. Aplikasi serangan DDoS menggunakan slowloris.
Skenario 3	*Brute Force Attack* dan DDoS	Untuk mengetahui tingkat integritas sistem mengacu pada 3 parameter pengujian yaitu *response time*, *akurasi* dan penggunaan *resources*

Parameter uji keamanan sistem jaringan menggunakan 3 parameter CIA yaitu confidentialitas, availibilitas dan integritas [4].

Tabel 3. Parameter Uji

Parameter Uji	Keterangan
Confidentialitas	Menguji kemampuan sistem sesuai dengan kebutuhan yang diinginkan. Tingkat keberhasilan pada pengujian ini adalah apakah sistem mampu melakukan pengelabuan port, pemblokiran akses dan melayani ketersediaan data terhadap orang yang memiliki otentikasi atau hak akses.
Avalibilitas	Menguji IPS apakah sudah sesuai dengan kebutuhan yang diinginkan. Tingkat keberhasilan pada pengujian ini adalah memblokir paket-paket yang mencurigakan yang dirasa mengancam sistem
Integritas	3 (Tiga) kriteria yaitu *Response time* Waktu tanggap yang diberikan oleh interface ketika pengguna mengirim

DOI: https://doi.org/10.29207/resti.v5i1.2825

Parameter Uji	Keterangan
	permintaaan ke komputer. Parameter ini mengambil waktu yang dibutuhkan untuk mengetahui adanya serangan ke *server*
Akurasi pendeteksian dan pemblokiran	Pengujian ini untuk mengetahui persentase akurasi IPS dalam melakukan pemblokiran akses terhadap serangan. Data monitoring atau log yang dihasilkan dapat diolah berupa persentase tingkat akurasi dalam melakukan pendeteksian dan pemblokiran akses.
Penggunaan *resources*	Pengujian ini bertujuan untuk menghitung tingkat penggunaan sumber daya ketika *snort inline-mode* melakukan pendeteksian serta pemblokiran akses terhadap indikasi serangan yang terjadi

Tabel 4 menunjukkan hasil uji confidentialitas sistem keamanan *cowrie honeypo*t dan *snort inline-mode* terhadap 6 (Enam) *requirements* tingkat kerahasiaan data sebesar 83.3%. Secara keseluruhan hasil pengujian confidentialitas mengindikasikan bahwa sistem yang diimplementasikan telah berhasil menjaga kerahasiaan data terhadap jenis serangan *Brute Force*.

Tabel 4. Hasil Pengujian Terhadap Confidentialitas Sistem

	Tingkat kerahasiaan data	Hasil Uji
1.	Sistem mampu melakukan menyembunyikan *port ssh server asli*	Berhasil
2.	Sistem mampu memanipulasi *port ssh server* dengan *server* palsu	Berhasil
3.	Sistem mampu melayani permintaan atau aktivitas *attacker* pada *server* palsu	Tidak Berhasil
4.	Sistem memiliki kredensial *login* yang lemah, sehingga *attacker* dapat masuk pada *server* palsu dengan mudah	Berhasil
5.	Sistem mampu melakukan *monitoring traffic* atau lalu lintas jaringan terhadap *server*	Berhasil
6.	Sistem mampu memblokir akses terhadap *user* yang tidak memiliki otentikasi	Berhasil

Hasil pengujian terhadap *availability* sistem diperoleh dalam kurun waktu 5 (Lima) hari (W1 sampai dengan W5) dengan beberapa kali serangan. Perhitungan availabilitas sistem berdasarkan rumus Braastad dan Calzolari [14].

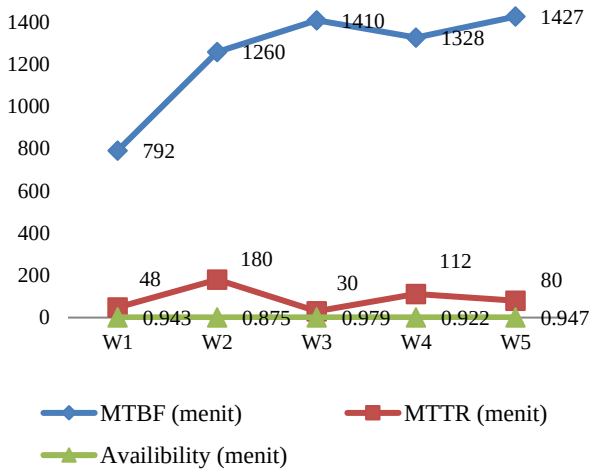
$$Availability = \frac{\text{MTBF}}{MTBF+MTTR} \quad (1)$$

Mean Time Between Faults (MTBF) adalah waktu rata-rata *uptime* sedangkan *Mean Time to Repair* (MTTR) adalah rata-rata waktu yang diperlukan untuk mengembalikan layanan .

Tabel 5 menunjukan data rata-rata tingkat availabilitas sistem yang disebabkan oleh kegagalan berupa *server down* dengan periode waktu W1 sampai W5. Nilai rata-rata availabilitas sistem 0.933 menit dengan waktu rata-rata *uptime* 1234.4 menit dan rata-rata waktu *repair* adalah 90 menit. Berdasarkan data hasil uji *Cowrie honeypot* dan *snort inline-mode* mengindikasikan bahwa kedua IPS belum dapat secara optimal membantu dalam menangani *server down* akibat serangan DDoS akan tetapi telah mampu meminimalisir serangan yang terjadi (93.3%).

Tabel 5. Hasil Pengujian *Availibility* Sistem

Waktu Downtime (Wn)	Penyebab Kegagalan	MTBF (menit)	MTTR (menit)	Availibility	
				menit	percentage
W1	Server Down	792	48	0.943	94.3 %
W2	Server Down	1260	180	0.875	87.5 %
W3	Server Down	1410	30	0.979	97.9 %
W4	Server Down	1328	112	0.922	92.2 %
W5	Server Down	1427	80	0.947	94.7 %
Nilai rata-rata		*1243.4*	*90*	*0.933*	*93.3 %*



Gambar 3. Grafik Hasil Pengujian Availabilitas Sistem

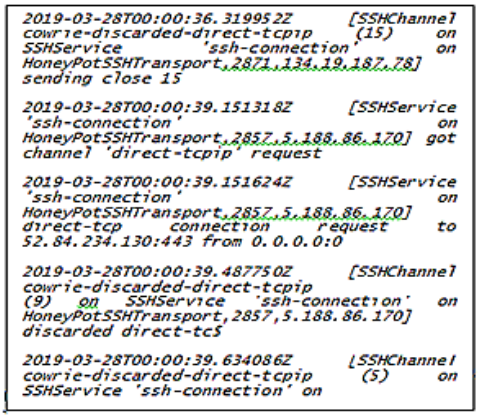
Gambar 3 memperlihatkan grafik availabilitas W1-W5 berdasarkan perhitungan nilai MTBF dan MTTR menggunakan satuan ukur menit. Berdasarkan grafik dapat dilihat bahwa nilai availabilitas terbaik yaitu 0.875 menit, dengan durasi waktu *uptime* selama 1260 menit dan waktu untuk mengembalikan layanan adalah 30 menit (W3).

Hasil pengujian integritas berdasarkan 3 (Tiga) parameter yaitu *response time*, akurasi dan penggunaan *resources*.

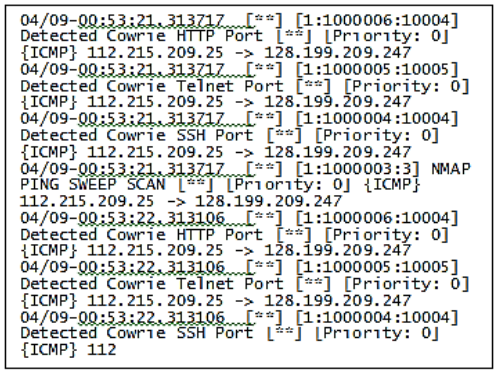
Pengujian parameter *response time* terhadap pendeteksian serangan dan pemblokiran untuk *cowrie honeypot* dan *snort inline-mode* telah dilakukan sebanyak 10 (Sepuluh) kali serangan. Gambar 4 merupakan hasil pengujian terhadap *cowrie honeypot* pada saat menerima serangan dari *attacker*. Serangan yang masuk dideteksi oleh *cowrie*.

Hasil pengujian pada *snort inline-mode* dilakukan serangan pada server dengan menggunakan *hydra* untuk melakukan *brute force attack* dan *slowloris* untuk melakukan DDoS (Gambar 5). Ketika serangan dilakukan, *snort* menghasilkan beberapa peringatan. *Snort inline-mode* dapat mendeteksi serangan terhadap port HTTP, Telnet dan SSH, protokol yang digunakan yaitu ICMP. Dalam peringatan ini IP Address sumber 112.215.209.25 dan IP tujuan 128.199.209.247.

DOI: https://doi.org/10.29207/resti.v5i1.2825



Gambar 4. Log Cowrie Honeypot

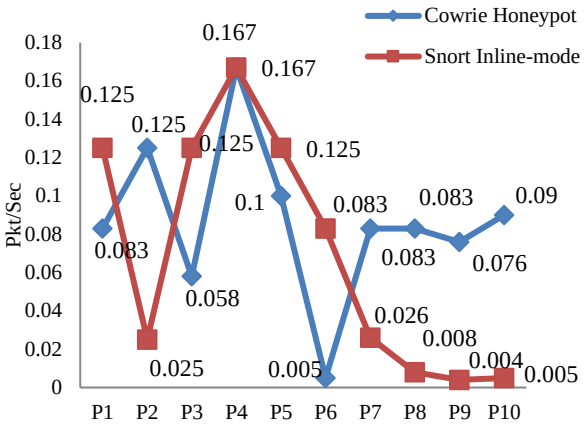


Gambar 5. Log Snort inline-mode

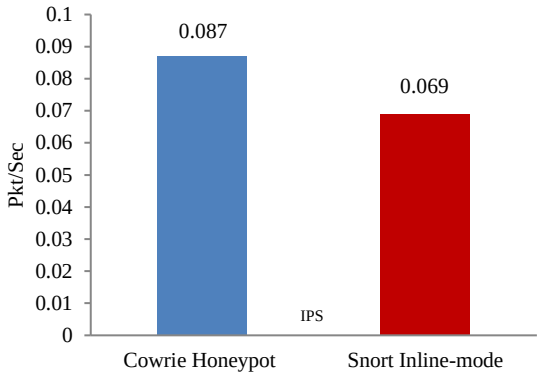
Tabel 6 merupakan hasil uji *respon time* untuk *Cowrie Honeyport* dan *Snort Inline-mode*. Pengujian ini bertujuan untuk memperoleh data IPS mana yang lebih baik dalam mendeteksi adanya aktivitas serangan ke server. Pengujian ini dilakukan sebanyak 10 (sepluh) kali dilakukan selama 2 menit, nilai *respon time* terkecil adalah nilai terbaik yang artinya tercepat dalam mendeteksi serangan. Hasil uji menunjukkan *Snort Inline-mode* memiliki rata-rata *respon time* lebih cepat yaitu 0.069 Pkt/sec dalam mendeteksi serangan terhadap server, sementara *Cowrie Honeyport* dapat merespon serangan dengan rata-rata 0.087 Pkt/sec.

Tabel 6. Hasil Uji Respone Time

Pengujian (P)	Cowrie Honeypot (Pkt/sec)	Snort Inline-mode (Pkt/sec)
P1	0.083	0.125
P2	0.125	0.025
P3	0.058	0.125
P4	0.167	0.167
P5	0.100	0.125
P6	0.005	0.083
P7	0.083	0.026
P8	0.083	0.008
P9	0.076	0.004
P10	0.090	0.005
Rata-rata	*0.087*	*0.069*



Gambar 6. Grafik Hasil Pengujian *Respon Time*



Gambar 7. Grafik Hasil Uji Rata-Rata Respon Time

Data hasil uji respon time *Cowrie Honeyport* dan *Snort Inline-mode* pada Tabel 6 dapat digambarkan dalam bentuk grafik pada Gambar 6. Waktu rata-rata *respon time* dari ke sepuluh pengujian digambarkan dalam grafik (Gambar 7), selisih dari kedua IPS tersebut adalah 0.018 Pkt/Sec.

Data pada Tabel 7 menunjukkan bahwa hasil pengujian parameter akurasi pendeteksian dan pemblokiran baik pada *cowrie honeypot* maupun *snort inline-mode* menggunakan jenis serangan *brute force* dan *DDoS* sebanyak 10 (sepuluh) kali serangan mengindikasikan bahwa kedua IPS memiliki nilai persentase akurasi yang sama (100%). Kedua IPS secara optimal dapat mendeteksi dan melakukan pemblokiran akses terhadap serangan.

Tabel 7. Hasil Uji Akurasi Pendeteksian dan Pemblokiran

Tools	Jumlah Serangan		Jumlah Terdeteksi	
	Brute Force	DDoS	Brute Force	DDoS
Cowrie Honeypot	10	10	10	10
Snort Inline-mode	10	10	10	10
Persentase Akurasi Deteksi				*100%*

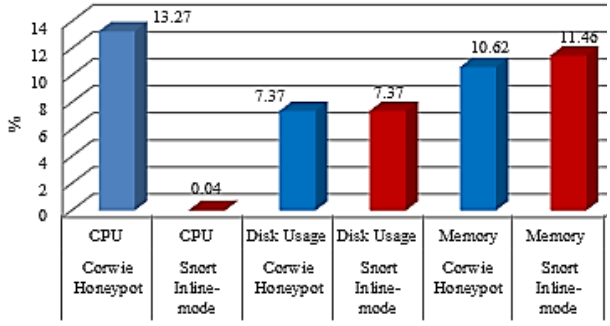
Hasil pengujian penggunaan *resources* (CPU, *memory* dan *Disk Usage*) pada Tabel 8 dilakukan selama 60 menit dengan menggunakan serangan *brute force*.

DOI: https://doi.org/10.29207/resti.v5i1.2825

Berdasarkan pengujian yang dilakukan sebanyak 10 (Sepuluh) kali diperoleh data bahwa penggunaan sumber daya terbaik untuk CPU adalah *Snort Inline-mode* (0.04%), untuk memori yaitu *Corwie Honeypot* (10.62%), penggunaan *disk usage* untuk kedua IPS memiliki nilai persentase dan nilai rata-rata yang sama.

Tabel 8. Hasil Uji Penggunaan *Resources*

Pengujian	*Corwie Honeypot*			Snort Inline-mode		
	CPU (%)	*Memory (%)*	*Disk Usage (%)*	*CPU (%)*	*Memory (%)*	*Disk Usage (%)*
P1	0.3	10.4	7.37	0.05	11.6	7.37
P2	1.0	10.7	7.37	0.03	11.1	7.37
P3	32.9	11.4	7.37	0.05	10.9	7.37
P4	15.3	10.3	7.37	0.03	11.1	7.37
P5	36.14	10.9	7.37	0.03	11.7	7.37
P6	0.3	11.1	7.37	0.07	11.9	7.37
P7	0.3	10.2	7.37	0.03	10.8	7.37
P8	1.0	10.4	7.37	0.03	11.9	7.37
P9	15.3	10.4	7.37	0.05	12.5	7.37
P10	30.2	10.4	7.37	0.03	11.1	7.37
Rata-rata	*13.27*	*10.62*	*7.37*	*0.04*	*11.46*	*7.37*



Gambar 8. Grafik Hasil Pengujian Penggunaan Resources

Gambar 8 merupakan grafik dari data Tabel 8. Hal signifikan yang terlihat pada grafik adalah perbedaan nilai uji antara *cowrie honeypot* dan *snort inline-mode* untuk penggunaan resources CPU, yang mana selisihnya mencapai 13.23%.

Hasil uji integritas (*response time*, akurasi dan penggunaan resources) menunjukkan bahwa sistem keamanan jaringan menggunakan *sno*rt *inline-mode* lebih baik dibandingkan *cowrie honeypot*. IPS *snort inline-mode* unggul pada parameter respon time (rata-rata 0.069 Pkt/Sec) dan penggunaan CPU (0.04%). Hal ini sesuai dengan hasil riset [15] yang menunjukkan bahwa Snort sebagai IPS dapat mengurangi penggunaan CPU yang diujikan pada *Session Initiation Protocol* (*SIP)-based flood* dengan serangan DoS/ DDoS pada kajian IP *telephony system*.

Kedua IPS (*Cowrie honeypot* dan *snort inline-mode*) saling membantu dalam meningkatkan integritas sistem, dimana sistem menjadi lebih responsif dalam menangani dan mendeteksi serangan yang terjadi pada server

4. Kesimpulan

Berdasarkan hasil uji dengan serangan *Brute Force* dan DDoS menggunakan 3 (Tiga) parameter uji keamanan jaringan menunjukkan parameter confidentialitas (83.3%), parameter availabilitas (93.3%) dan parameter integritas untuk *snort inline-mode* nilai rata-rata (response time 0.069 Pkt/Sec, akurasi 100%, penggunaan resources: CPU 0.04%; RAM 11.46%; Disk Usage 7.37%); untuk *cowrie honeypot* nilai rata-rata (response time 0.087 Pkt/Sec, akurasi 100%, penggunaan resources: CPU 13.37%; RAM 10.62%; Disk Usage 7.37%). Uji parameter integritas secara keseluruhan *IPS snort inline-mode* lebih unggul dibandingkan *cowrie honeypot*. Mengacu kepada uji parameter integritas secara keseluruhan IPS snort inline-mode lebih direkomedandasikan untuk digunakan dalam sistem keamanan jaringan dibandingkan *cowrie honeypot*.

Pengembangan studi dapat dilakukan dengan penambahan parameter keamanan seperti *authentication, access control* dan *non-repudiatiation* kemudian konfigurasi IP *Blacklist* secara manual dapat dikembangkan menjadi otomatis.

Daftar Rujukan

[1] Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), 2020. *Laporan Survei Internet APJII 2019-2020 (Q2).* [Online] Tersedia di: https://apjii.or.id/survei

[2] Qing W., and Hongju C. 2016. Computer Network Security and Defense Technology Research. *In 2016 8th International Conference on Measuring Technology and Mechatronics Automation, ICMTMA*. Macau, China 11-12 March 2016. IEEE. doi: 10.1109/ICMTMA.2016.47

[3] Kacar, M. S., and Oztoprak, K. 2017. Network Security Scoring. *In 11th International Conference on Semantic Computing, ICSC*. San Diego, USA 30 Jan-1 Feb 2017. IEEE. doi: 10.1109/ICSC.2017.86

[4] Raji A., and Adam M. 2020. Enhancing Public Cloud Security by Developing a Model For User Authentication and Data Integrity Checking. In 7th *International Conference on Computer Science and Information Technology (SCCSIT7)7*. Khartoum, Sudan. doi: 10.1145/1234567891

[5] Vishnevsky A., and Klyucharev P. 2017. A Survey of Game-Theoretic Approaches to Modeling Honeypots. In *the VIII All-Russian Scientific and Technical Conference on Secure Information Technologies (BIT 2017)*, 2081 (4), pp.139-142. urn:nbn:de:0074-2081-4

[6] Sagala A., 2015. Automatic SNORT IDS Rule Generation Based on Honeypot Log. In *7th International Conference on Information Technology and Electrical Engineering (ICITEE)*. Chiang Mai, Thailand 29-30 Oct 2015. IEEE. doi: 10.1109/ICITEED.2015.7409013

[7] Pratama, R. F., Suwastika, N. A., and Nugroho, M. A. 2018. Design and Implementation Adaptive Intrusion Prevention System (IPS) for Attack Prevention in Software-Defined Network (SDN) Architecture. In *6th International Conference on Information and Communication Technology (ICoICT*). Bandung, Indonesia 3-5 May 2018. IEEE. doi: 10.1109/ICoICT.2018.8528735

[8] Cabral W.Z., Valli C., Sikos L.F., and Wakeling A.G. 2019. Review and Analysis of Cowrie Artefacts and Their Potential to be used Deceptively. In *2019 International Conference on Computational Science and Computational Intelligence (CSCI*). Las Vegas, United States 5-7 December 2019. IEEE. doi: 10.1109/CSCI49370.2019.00035

[9] Lakh Y., and Shymkiv R. 2019. Using Honeypot Programs for Providing Defense of Banking Network Infrastructure. In *2019 International Scientific-Practical Conference Problems of*

Infocommunications. Science and Technology. Kyiv, Ukraina 8-11 Oct 2019. IEEE. doi: 10.1109/PICST47496.2019.9061550

[10] Kyriakou A., and Sklavos N. 2018. Container-Based Honeypot Deployment for the Analysis of Malicious Activity. In *Global Information Infrastucture and Networking Symposium (GIIS)*. Thessaloniki, Greece 23-25 Oct 2018. IEEE. doi: 10.1109/GIIS.2018.8635778

[11] Nugroho, OW. 2020. Implementasi Sistem Keamanan Jaringan Intrusion Prevention System (IPS) Menggunakan IPTables dengan Notifikasi berbasis Telegram pada SMK Siang Surabaya. *Jurnal Manajeman Informatika*, 11 (1) 99.1-16

[12] Ma'sum M.S., Irwansyah M.A., and Priyanto H. 2017. Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snrt dan Netfilter. *Jurnal Sistem dan Teknologi Informasi* (JUSTIN), 5 (1) pp.56-60

[13] Rianafirin K., and Kurniawan M.T. 2017.Design Network Security Infrastructure Cabling Using Network Development Life Cycle Methodology and ISO/IEC 27000 Series in Yayasan Kesehatan (Yakes) Telkom Bandung. In *4th International Conference on Computer Applications and Information Processing Technology (CAIPT)*. Kuta Bali, Indonesia 8-10 Agustus 2017. IEEE. doi: 10.1109/CAIPT.2017.8320681

[14] Sulistyanto I.H. 2015. Implementasi High Availability Server Dengan Teknik Failover Virtual Computer Cluster. Skripsi. Universitas Muhammadiyah Surakarta.

[15] Cadet F., and Fokum D.T. 2016. Coping with denial-of-service attacks on the IP telephony system. In *SoutheastCon 2016*. Norfolk, VA, USA 30 March-3 April 2016. IEEE. doi: 10.1109/SECON.2016.7506691

DOI: https://doi.org/10.29207/resti.v5i1.2825