SISTEM KEAMANAN *OPEN CLOUD COMPUTING* MENGGUNAKAN IDS (*INTRUSION DETECTION SYSTEM*) DAN IPS (*INTRUSION PREVENTION SYSTEM*)

Shah Khadafi, Budanis Dwi Meilani, Samsul Arifin

Sistem Komputer-Institut Teknologi Adhi Tama Surabaya
Jl. Arief Rahman Hakim No.100 Surabaya
Email : khadafi@itats.ac.id

ABSTRACT

The development of information technology is currently getting faster, especially network security technology that became one of the technologies to be considered when a system or technology is connected to a network. The rise of cases of attacks on computer networks occurs because without realizing that the computer is attacked does not know that there has been an attack in the system. One of the technologies of computer network development is cloud computing, which should also be required to utilize network security system. Therefore, necessary to implement IDS (intrusion detection system) in open cloud computing environment using snort, barnyard2, and BASE. Firewalls are also implemented as applications to block data traffic from IP addresses or suspicious data packets that were previously matched with a previous rule set. Testing of open cloud security system based on IDS and IPS using two scenarios, the first test when IPS systems active and the second test when IPS systems non active. The results of both tests show, that the open cloud security system based on IDS and IPS is able to provide response and alert to the data traffic monitored and blocking attacks. indicators the first test seen on CPU usage servers between 59.8% - 85.5%, while the second test, CPU usage server between 2% s / d 4% in this case back to normal condition.

Keywords : *open cloud computing, intrusion detection system, intrusion prevention system, snort, firewall*

ABSTRAK

Perkembangan teknologi informasi saat ini semakin cepat, khususnya teknologi keamanan jaringan yang menjadi salah satu teknologi yang harus diperhatikan ketika suatu sistem atau teknologi terkoneksi dengan jaringan. Maraknya kasus serangan pada jaringan komputer terjadi karena tanpa disadari bahwa pihak komputer yang diserang tidak mengetahui bahwa telah terjadi serangan di dalam sistemnya. Salah satu dari teknologi perkembangan jaringan komputer yaitu *cloud computing*, yang semestinya juga diharuskan memanfaatkan sistem keamanan jaringan. Dengan demikian diperlukan mengimplementasikan IDS (*intrusion detection system*) di dalam lingkungan *open cloud computing* menggunakan snort, barnyard2, dan BASE. Penggunaan iptables sebagai firewall pada sistem keamanan jaringan ini. Snort digunakan sebagai aplikasi untuk memantau aktivitas jaringan yang memanfaatkan sistem IPS berjalan pada mode inline, kemudian menampilkan hasilnya melalui aplikasi BASE. *Firewall* juga diimplementasikan sebagai aplikasi untuk memblokir trafik data dari alamat IP ataupun paket-paket data yang mencurigakan yang sebelumnya dilakukan pencocokan dengan rule yang di-set sebelumnya. Pengujian sistem keamanan *open cloud* berbasiskan IDS dan IPS menggunakan dua skenario, pertama pengujian sistem IPS aktif dan yang kedua pengujian menggunakan sistem IPS non aktif. Hasil dari pengujian menunjukan, bahwa sistem keamanan *open cloud* berbasiskan IDS dan IPS mampu memberikan respon dan *alert* terhadap traffic data yang dipantau dan melakukan pemblokiran adanya serangan. Indikator pengujian yang pertama terlihat pada CPU *usage server* berkisar antara 59.8% - 85.5%, sedangkan pengujian yang kedua CPU *usage server* berkisar antara 2% s/d 4% dalam hal ini kembali ke keadaan normal.

Kata kunci : *open cloud computing, intrusion detection system, intrusion prevention system, snort, firewall*

PENDAHULUAN

Keamanan menjadi salah satu teknologi yang perlu diperhatikan ketika suatu sistem yang terkoneksi dengan system jaringan komputer menjadi hal yang sangat krusial. Pada saat ini kebutuhan manusia sangat tergantung dengan adanya informasi ataupun data, khususnya informasi atau data digital. Semakin besar kebutuhan adanya informasi semakin meningkat pula insiden atau gangguan keamanan terhadap system jaringan yang meningkat tajam. Hal ini umumnya terjadi dikarenakan masih kurangnya kepedulian terhadap keamanan sebuah sistem khususnya pada infrastruktur *hardware* jaringan komputer yang masih sangat kurang.

Dikutip dari sebuah sumber yang membahas tentang serangan *cyber* pada sebuah system keamanan bahwa terjadi peningkatan selama tahun 2015 dan tahun 2016 dengan jumlah serangan sebanyak 5,197 dan 6,068. Data ini mengemukakan bahwa jumlah kenaikan yang dramatis terhadap teknologi *cloud cyber security* yang berbasis *cloud* telah membantu beberapa perusahaan melihat pola serangan yang rumit untuk terdeteksi secara manual. Dengan total kenaikan jumlah serangan yang mengakibatkan beberapa *attacker* berpotensial melakukan serangan terhadap sebuah teknologi yang berbasikan *cloud*, ini mengindikasikan bahwa kejadian serangan *cyber* terhadap system keamanan cenderung meningkat pada rentang tahun 2015 dan 2016[1]. Perkembangan dari teknologi komunikasi yang mengarah ke IoT (*internet of things*) juga tidak luput juga dari ancaman para *attacker* yang bisa juga mencegat pesan yang lewat dari sumber ke tujuan sehingga privasi dari sebuah messange bisa bocor dan isi pesan juga rentan dimodifikasi, sehingga pengiriman pesan yang aman diperlukan di IoT [2].

Salah satu teknologi yang memanfaatkan jaringan adalah *cloud computing*. *Cloud computing* merupakan teknologi komputasi modern yang mulai berkembang penggunaanya pada tahun 2005 yang menggunakan layanan jaringan komputer atau jaringan internet. Di dalam teknologi *cloud computing* menyediakan 3 layanan yaitu, *Software as a Service* (SaaS), *Platform as a Service* (PaaS) dan *Infrastructure as a Service* (IaaS). IaaS merupakan salah satu layanan *cloud computing* yang menyediakan perangkat keras berupa pemroses, penyimpan, jaringan dan beberapa *resource* yang lain mengenai komputasi dasar. Perusahaan seperti Oracle dan Amazon yang memulainya teknologi *cloud computing modern*, dimana oracle mengembangkan perangkat lunak CRM yang berbasikan SaaS, sedangkan amazon menghasilkan EC2 (*elastic computer cloud*). Meskipun teknologi *cloud computing* modern menyajikan layanan yang sangat menarik dan juga manfaat yang dapat memberikan penggunanya dapat menghemat biaya, akan tetapi juga memberikan risiko dan peluang baru untuk eksploitasi bidang keamanan system di dalamnya.

Pembahasan pada jurnal ini membahas teknik monitoring dan pencegahan keamanan *cloud computing*. Salah satu faktor keamanan adalah melindungi infrastruktur di dalam *cloud computing* dari serangan jaringan. Selain itu, sistem *firewall* juga merupakan salah satu perangkat lunak yang mampu mencegah beberapa serangan dari luar, namun *firewall* tidak dapat memberikan peringatan terhadap serangan yang cukup kompleks seperti, D-Dos dan serangan pada port-port tertentu.

Lebih spesifik lagi, system yang dirancang ini menggunakan *Intrusion Prevention System* (IPS) berbasis jaringan atau disebut NIPS (*network intrusion prevention system*) untuk layanan *Infrastrukture as a Service* (IaaS) yang diimplementasikan pada aplikasi *open cloud computing*. Tujuanya digunakan untuk memantau dan memproteksi serangan penyusup dari luar yang hendak masuk ke system, dan selanjutnya memberikan laporan ke administrator jaringan jika terdapat serangan yang terjadi di dalam lingkungan *cloud*.

TINJAUAN PUSTAKA

Cloud Computing

Cloud computing[2], sebuah model komputasi *online*, dimana *resource* komputer seperti *processor*, *storage*, *network*, dan *software* berada di pusat data yang menyediakan layanan *cloud*. Di dalamnya diberikan sebuah layanan (aplikasi) melalui akses jaringan/internet yang menggunakan pola akses remote. Kelebihan sistem *cloud computing* adalah memberikan kenyaman *on-demand* sesuai kebutuhan dari penggunanya, mudah dikontrol, dinamik dan skalabilitas. Teknologi yang di dalam *cloud computing* memiliki 5 kriteria yaitu : broad *network access, rapid*

elasticity, *resource pooling*, *measured service* dan *on-demand self-service*. Cloud computing memiliki 3.

Cloud computing menyediakan 3 layanan antara lain yaitu SaaS, Paas, dan IaaS. Yang pertama SaaS (*Storage as a service*) merupakan layanan yang mana penyedia *cloud* menyediakan *software* yang bisa digunakan oleh pengguna di dalam lingkungan *cloud*. Software yang disediakan bisa diakses dari beberapa *user interface* antara lain seperti *web browser*. Salah satu layanan SaaS adalah GoogleDocs, Office365, Adobe Creative Cloud. Yang kedua yaitu PaaS (*Platform as a service*) layanan ini memberikan layanan kepada user agar bisa menggunakan aplikasi ataupun bahasa pemrograman yang disediakan oleh *provider* (penyedia sistem *cloud*), serta dapat menyimpan data-data pada sistem *cloud computing*. Dalam hal ini *user* yang menggunakan layanan PaaS tidak mengelolah atau mengontrol infrastruktur *cloud* seperti *network*, *server*, *operating system* atau *storage*. Salah satu penyedia layanan PaaS adalah Amazon web service, Windows Azure, dan GoogleApp Engine. Selanjutnya yang ketiga yaitu IaaS (*Infrastructure as a service*) merupakan sebuah layanan yang menyediakan Infrastruktur IT berupa *storage*, *networks* dan *resource* komputasi yang lain. Dalam hal ini *user* dapat mengkonfigurasi sendiri infrastruktur yang disewanya seperi aplikasi dan sistem operasi yang ingin digunakan. Disini pengguna dapat mengontrol sistem operasi, storage dan pengembangan aplikasi. Salah satu penyedia IaaS adalah Amazon EC2, Rackspace, dan Windows Azure.

Proxmox

Dalam teknologi *cloud computing* terdapat beberapa *software* untuk membuat sebuah sistem *cloud computing* yang bersifat *open source*. Manfaat *open source cloud computing* disini memberikan banyak pilihan bagi para pengembang untuk berinovasi mengembangkan system cloud computing dengan mudah tanpa dipersulit tentang lisensi sebuah *software*. Salah satu software untuk mengembangkan sistem *cloud computing* yang bersifat open yaitu Proxmox [4]. Proxmox merupakan salah satu *open source cloud computing* yang menggunakan GNU/Linux Debian. Proxmox berdasarkan 2 teknologi virtualisasi yaitu *Kernel-based Virtual Machine* (KVM) dan *Container Virtualization* OpenVZ [5]. OpenVZ merupakan salah satu teknologi yang menggunakan *container-based virtualization* untuk Linux. OpenVZ membuat *container* yang aman dan terisolasi (dikenal dengan VE dan VPS) pada *real server*. Sedangkan *Kernel-based Virtual Machine* (KVM) merupakan solusi *Full Virtualization* untuk system yang menggunakan linux pada hardware berbasiskan x86 yang memiliki *virtualization extensions* (seperti Intel VT dan AMD-V). Dengan menggunakan KVM ini memungkinkan untuk menjalankan beberapa *virtual machine* mode *unmodified image* Linux atau Windows.

Intrusion Prevention System

Intrusion Prevention System (IPS) adalah suatu metode yang mengkombinasikan teknik *firewall* dan metode *Intrusion Detection System* (IDS). Perangkat lunak *Intrusion Detection System* adalah aplikasi berbasikan Linux yang dapat memantau sistem atau trafik jaringan dari penyalah gunaan atau aktivitas jahat yang kemudian dapat menghasilkan laporan ke dalam sistem [6]. Sistem pada IPS dapat mencegah serangan yang akan masuk ke jaringan lokal dengan memeriksa dan mencatat semua paket data serta mengenali paket data sensor, disaat attack telah teridentifikasi, IPS akan menolak akses (*block*) dan mencatat *log* semua paket data yang telah teridentifikasi.

Intrusion Detection and Prevention System

Intrusion Detection and Prevention System [7], atau disingkat dengan IDPS ini dapat dibagi dua, yaitu sistem yang menggunakan metode IDS dan IPS. Penggunaan IDS digunakan hanya untuk memantau trafik jaringan atau paket data bila terdapat intrusi, sedangkan IPS dapat digunakan untuk menghentikan atau blok *threats* atau ancaman. Baik IDS maupun juga IPS terdapat dua jenis deteksi ancaman yaitu *host-based* ataupun *network-based*. Sistem di dalam IDPS ini memonitor lalu lintas jaringan baik yang terkoneksi lokal maupun *online* (internet) pada segmen jaringan atau perangkat jaringan tertentu, yang kemudian menganalisa mengenai protokol jaringan yang digunakan, untuk mengidentifikasi aktivitas yang mencurigakan. Selain itu, IDPS yang berbasiskan jaringan juga dapat memberikan layanan pengumpulan informasi dengan

memanfaatkan database. Dalam hal ini IDPS dapat mengumpulkan informasi hasil dari monitoring host dan juga aktivitas lalu lintas trafik jaringan

Firewall

Firewall adalah suatu aturan-aturan yang mekanismenya bertujuan untuk melindungi *hardware* dan *software*. Perlindungan dapat dilakukan dengan menyaring, membatasi, atau bahkan menolak suatu atau semua hubungan/kegiatan dari suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Salah satu tool firewall yang umum digunakan pada sistem Linux yaitu Iptables. Iptables memungkinkan untuk seorang admin jaringan untuk merancang dan mengkonfigurasi setingan firewall. Selain itu juga admin juga dapat mengkonfigurasi rantai-rantai atau biasa disebut dengan *chains* dan *rules* di dalam system Linux.

Snort

Snort merupakan suatu *tools* yang berjalan di dalam system LinuX yang dapat digunakan untuk mendeteksi adanya penyusup (*threats*) dan mampu menganalisis paket yang melintasi jaringan secara *real time traffic* dan *logging* ke dalam *database*. Snort juga mampu mendeteksi berbagai serangan yang berasal dari luar jaringan. Snort bisa digunakan pada *platform* sistem operasi Linux, Free BSD, Debian, dan Windows. Snort memiliki arsitektur yang terdiri dari 4 basic komponen, yaitu *sniffer*, *preprocessor*, *detection engine*, dan *output.*

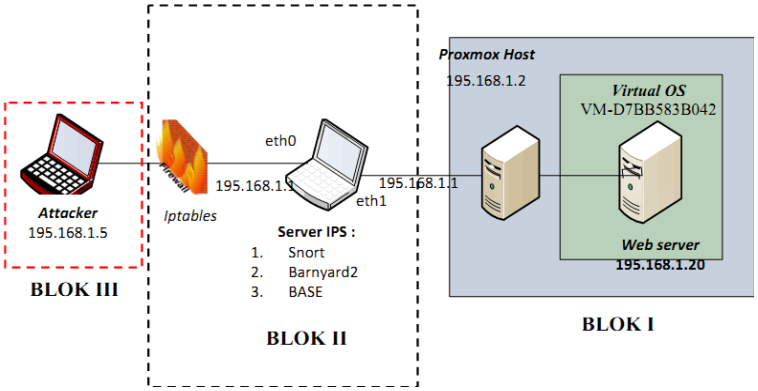
Jenis Serangan Cyber

Beberapa jenis serangan yang umum terjadi pada system keaman diantaranya *port scanning*, *sniffing*, ICMP *flood*, dan *hijacking*. *Port scanning* merupakan suatu proses untuk mencari dan membuka pada port komunikasi pada sebuah celah jaringan komputer. Dari hasil serangan tersebut akan didapatkan celah atau lubang kelemahan sebuah server yang diserang. *Packet sniffing* merupakan pencegatan data paket-paket yang mengalir pada jaringan. Dengan sebuah aplikasi yang beroperasi pada lapisan ke 2 OSI dan juga kombinasi dari NIC yang berada pada *mode promiscuous* (mode mendengar) untuk menangkap semua traffic yang mengalir dari dan menuju ke jaringan internet pada suatu jaringan. ICMP *flood* dilakukan oleh seorang *hacker* dengan cara melakukan eksploitasi ke system *server* dengan tujuan untuk membuat suatu target menjadi *hang*, yang disebabkan oleh pengiriman sejumlah paket yang besar ke arah target *server*. Exploting sistem ini dilakukan dengan mengirimkan suatu *command ping* dengan tujuan *broadcast* ataupun *multicast* dimana si pengirim dibuat seolah-olah adalah target *host*. Hijacking atau yang disebut dengan *man-in-the-middle-attack* (MITM) sebuah teknik serangan yang memanfaatkan kelemahan dari protokol TCP/IP. Serangan dilakukan ketika terdapat diantara 2 *user* yang sedang berkomunikasi, tetapi terdapat seseorang yang lain yang secara aktif memonitor, men-*capture*, dan mengontrol komunikasi tersebut secara transparan.

METODE

Topologi Cloud Computing

Metode keamanan yang dikerjakan terhadap sistem cloud computing ini dikerjakan secara bertahap, yang setiap pengerjaannya dilakukan pada tiap-tiap bagian. Terdapat 3 bagian, yang pertama yaitu bagian perancangan open cloud computing, bagian yang kedua yaitu perancangan system keamanan cloud computing, dan yang bagian yang ketiga yaitu perancangan scenario penyerangan terhadap system. Perancangan masing-masing bagian sesuai digambarkan sesuai dengan topologi jaringan yang nampak seperti pada gambar 1.



Gambar 1. Topologi Jaringan Sistem Kemanan Cloud Computing

Perancangan Hardware dan Software

Rancangan sistem keamanan cloud computing ini terkait erat dengan spesifikasi hardware yang digunakan dan juga kebutuhan software yang nantinya diimplementasikan ke rancangan sistem keamanan *cloud computing* yang dikerjakan ini. Dalam penelitian ini dibagi dalam 2 tahapan yaitu perancangan hardware, dan perancangan software. Untuk kebutuhan hardware yang digunakan sistem dipaparkan seperti keterangan berikut ini :

I. Spesifikasi *server cloud* :
   a. Processor minimal Dual core 2.0 Ghz
   b. CPU : 64 bit support Intel VT/AMD-V
   c. RAM minimal 3 Gb
   d. Harddisc min 80 Gb
   e. NIC min 1 buah

II. *Server* NIPS
   a. Processor minimal Intel Pentium IV
   b. RAM minimal 1 Gb
   c. Hardsisc minimal 80 Gb
   d. NIC 2 buah

III. Komputer *client* (*attacker*)
   a. Processor Intel I3
   b. RAM 2 Gb
   c. NIC 1 buah

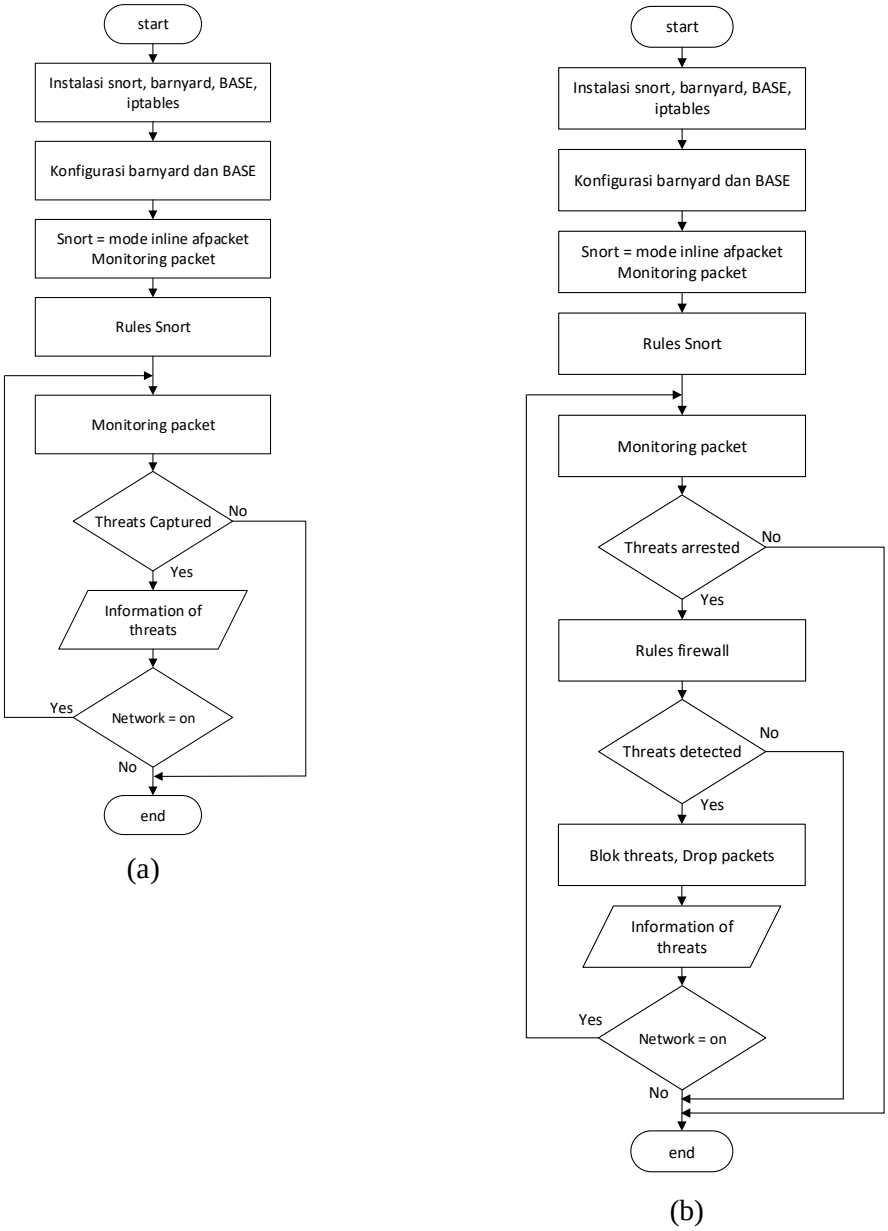
Sedangkan untuk kebutuhan software yang digunakan sistem dipaparkan seperti keterangan berikut ini :

I. Spesifikasi *server cloud* :
   a. *Cloud computing* : Proxmox VE 3.4.
   b. *Virtual* OS : Windows 2003 server
   c. Layanan : Web server

II. Server NIPS
   a. Sistem operasi : Linux Ubuntu 14.04
   b. IDS : snort, barnyard2
   c. IPS : snort (*mode inline*)
   d. *Database* : MySQL, Base
   e. *Firewall* : iptables

III. Komputer *client* (*attacker*)
   a. *Sniffing* : cain and abel
   b. *Scanning* : nmap
   c. D-DoS : Hoic

Flowchart Sistem IDS (*Intrusion Detection System*) dan IPS (*Intrusion Prevention System*)



Gambar 2. a) Flowchart IDS, b) Flowchart IPS

Sistem keamanan *open cloud* berbasiskan IDS dan IPS menggunakan *snort*, *firewall* dan BASE. Nampak pada gambar 2 (a), proses perancangan sistem keamanan *open cloud* berbasiskan IDS. Pertama-tama melakukan instalasi *tools* (aplikasi) berbasiskan Linux yaitu snort, barnyard, BASE dan firewall. Selanjutnya, melakukan konfigurasi pada snort pada file *snort.conf* terkait beberapa variabel snort terkait antara lain yaitu Ipvar HOME_NET, Ipvar EXTERNAL_NET, RULE_PATH, SO_RULE_PATH, PREPROC_RULE_PATH, menjadikan *snort inline type afpacket* (config daq_dir, config daq_mode, config daq_var), pengaturan *output* snort terkait dengan *snort.log*, dan pembuatan *rules* (aturan) snort yang dilakukan pada file *local.rules* pada directori /etc/snort/rules/. Sedangkan, untuk konfigurasi barnyard dilakukan pada file *bardnyard2.conf* pada directori /etc/snort/. Selanjutnya, untuk konfigurasi BASE membutuhkan sebuah *database* yang dapat menyimpan *alert snort*, dalam hal ini menginstall aplikasi *database* MySQL. Setelah melakukan beberapa konfigurasi, maka system yang dirancang ini dapat digunakan untuk memonitoring paket-paket dari traffic jaringan selama komputer terhubung ke dalam jaringan komputer. Dengan demikian, bila system ini mendeteksi adanya *threats* (ancaman)

ketika dilakukan monitoring maka system akan memberikan pesan alert bahwa terdapat *threats* yang memasuki jaringan yang digunakan system ini.
Deskripsi gambar *flowchart* 2 (b) yaitu system IPS dalam hal ini melanjutkan deskripsi gambar flowchar 2 (a), hasil monitoring dan alert yang dilakukan oleh sistem IDS kemudian dicocokan dengan sistem *firewall* yang dirancang. Perancangan *firewall* melalui mekanisme IPTABLES berfungsi untuk memblokir atau mendrop paket-paket dari traffic jaringan yang dianggap sebagai *threats*.

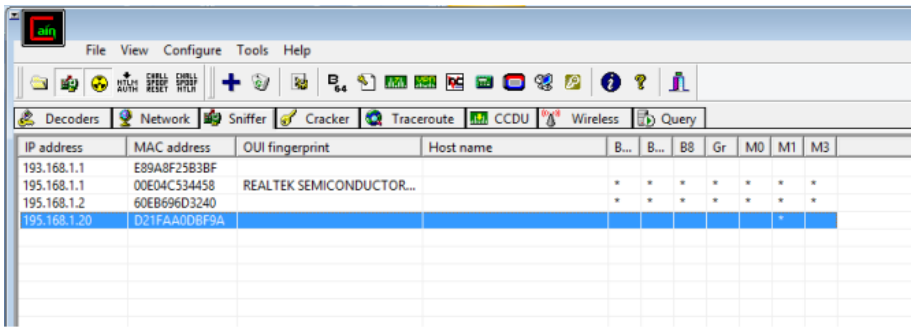
Snort, digunakan sebagai pendeteksi dan juga untuk mencegah bila diketahui sebuah traffic atau paket data yang teridentifikasi sebagai *threats* (ancaman). Snort juga mempunyai *rules* (aturan) sebagai pendeteksi threats dengan memantau aktivitas *traffic* di dalam jaringan. Untuk merubah snort dari mode IDS menjadi IPS, snort harus dijalankan pada *mode inline* dengan data aquisition (DAQ), yang salah satu jenis DAQ yaitu AFPACKET. AFPACKET menggunakan skema FORWARDING yang berarti menerukan traffic atau paket data dari satu interface ke interface, dimana seperti yang nampak pada gambar 1, bahwa computer IPS menggunakan 2 NIC (*Network Interface Card*). Firewall, penggunaannya digunakan ketika paket data melewati sistem IPS maka traffic atau paket data tersebut di-*capture* dan juga telah dideteksi oleh snort. Selanjutnya data tangkapan tersebut dibandingkan, apabila rules yang mengenai paket tersebut tidak sesuai dan terdeteksi maka paket data akan diblok atau *drop* oleh sistem *firewall* yang menggunakan mekanisme IPTABLES. BASE [8], merupakan pencarian dan pemroses *database* yang di dalamnya berisikan kejadian-kejadian keamanan yang dicatat oleh oleh sistem pemantau jaringan IPS dan firewall.

HASIL DAN PEMBAHASAN

Jenis-jenis Serangan Terhadap Sistem Keamanan

Berbagai cara dilakukan oleh PC *attacker* untuk menguji kehandalan dari sistem keamanan *open cloud* berbasiskan IDS dan IPS ini. Jenis-jenis serangan yang dilakukan, antara lain yaitu *sniffing*, *scanning*, dan D-DoS (*Denial of Service*). Dengan memanfaatkan beberap *tools* pengujian, sistem keamanan ini akan diuji dengan menggunakan beberapa tools untuk melakukan *hacking* ke beberapa komputer target yang ditentukan. Dalam hal ini komputer yang menjadi target yaitu komputer server menggunakan sistem operasi Windows 2003 server dengan IP *address* 192.168.1.20 yang menjalankan layanan *web server*.

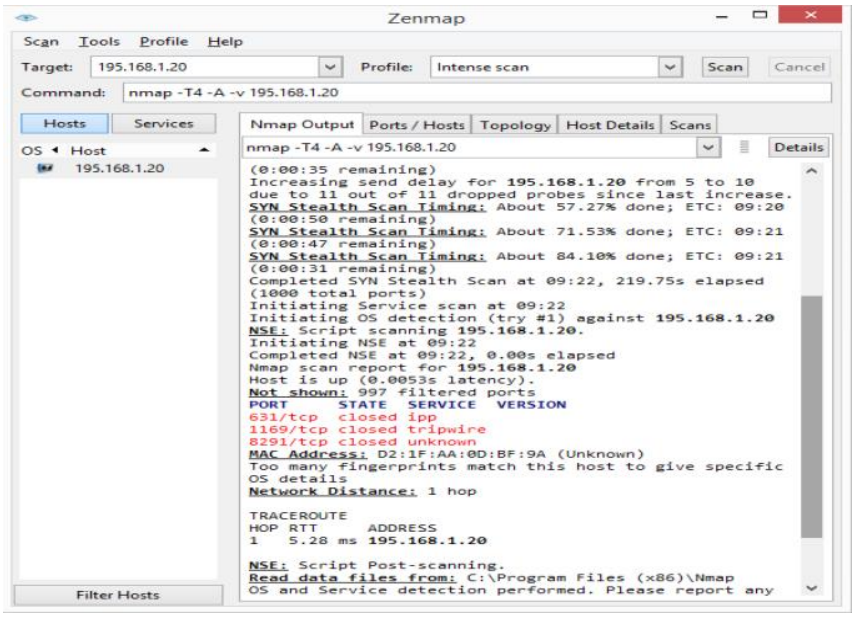
Sniffing



Gambar 3. Tampilan Proses *Sniffing* Terhadap Komputer Target

Pengujian serangan pertama terhadap sistem keamanan *open cloud* berbasiskan IDS dan IPS menggunakan cain and abel [9]. Dalam hal ini *attacker* melakukan proses *sniffing* terhadap komputer yang terkoneksi jaringan lokal. menggunakan Cain & Abel untuk mengetahui alamat IP komputer dan hostname komputer yang menjadi target. Nampak pada gambar 3, bahwa dengan menggunakan *tools* cain and abel komputer penyerang dapat mengetahui IP *address* dan MAC *address* yang digunakan oleh komputer *web server* (target serangan).

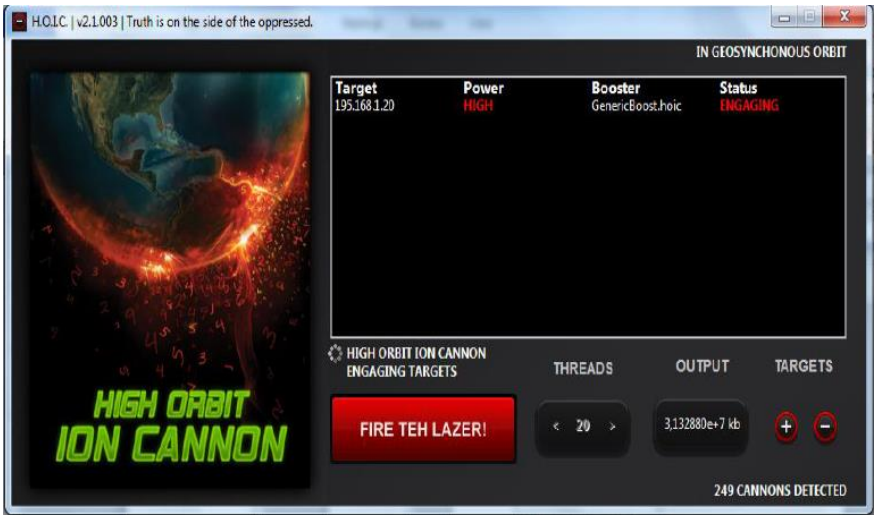
Scanning



Gambar 4. Tampilan Proses *Sniffing* Terhadap Komputer Target

Setelah mendapatkan IP *address* dan *hostname* komputer target, pengujian serangan selanjutnya terhadap sistem keamanan *open cloud* berbasiskan IDS dan IPS yaitu *scaning* menggunakan Nmap [10]. Dalam hal ini *attacker* melakukan *scaning* pada sistem menggunakan Nmap untuk mengetahui port apa saja yang *open* dan *services* apa saja yang berjalan di dalam komputer yang menjadi target. Nampak pada gambar 4, bahwa dengan menggunakan *tools* zenmap komputer penyerang dapat mengetahui *port* berapa saja yang *open* ataupun close beserta no *port* yang digunakan, dan *service* (layanan) apa saja yang running di dalam komputer *web server* (target serangan).

D-DoS



Gambar 5. Tampilan Proses D-DoS Terhadap Komputer Target

Setelah mengetahui port apa saja yang terbuka dan layanan apa saja yang berjalan pada komputer target, pengujian serangan selanjutnya terhadap sistem keamanan *open cloud* berbasiskan IDS dan IPS yaitu D-DoS. Serangan Distributed Denial of Service (DDoS) adalah upaya untuk membuat layanan *online* tidak tersedia dengan mengirimkan sangat banyak traffic atau paket data

dari berbagai sumber [11]. Dalam hal ini *attacker* mencoba melakukan serangan terhadap komputer target sehingga dapat melumpuhkan atau computer target menjadi *error*. Teknik serangan D-DoS ini dilakukan dengan cara menghabiskan sumber daya (*resource*) yang dimiliki oleh komputer target sampai komputer tersebut tidak dapat lagi dapat lagi menjalankan layanan *web* dengan baik. Nampak pada gambar 5, bahwa dengan menggunakan *tools* HOIC komputer penyerang dapat mengirimkan paket-paket dalam jumlah yang sangat besar atau trafiik data yang besar menuju komputer *web server* (target serangan).

Pembahasan Hasil Pengujian

Pembahasan yang akan disajikan ini meliputi hasil dari pengujian proses serangan scaning dan D-DoS. Hasil dari serangan yang menggunakan teknik *scaning* terhadap sistem keamanan *open cloud* berbasiskan IDS dan IPS menunjukkan bahwa sistem keamanan ini berjalan dengan baik. Terbukti dari durasi komputer *attacker* melakukan serangan *scaning* lebih lama yang nampak pada tabel 1. Selain itu juga mampu menutup port-port dan layanan-layanan yang tersedia pada komputer target.

Tabel 2. Hasil Pengujian Scaning

No	Jenis Pengujian	Scaning Port Komputer Target		Durasi (s)
		No port	Status port	
1	Scaning IDS dan IPS non aktif	7, 9, 13, 17, 19, 42, 53, 80, 135, 139, 445, 1025, 1028, 1032, 1033	Open	219,75
2	Scaning IDS dan IPS aktif	631, 169, 8291	Close	1,35

Pembahasan selanjutnya adalah membahas hasil dari serangan yang menggunakan teknik D-DoS terhadap komputer server open cloud berbasiskan IDS dan IPS. Yang dijadikan target yaitu komputer web server open cloud dengan IP address 195.168.1.2. Ketika sistem sistem keamanan *open cloud* berbasiskan IDS dan IPS diaktifkan nilai CPU *usage* mengindikasikan pada kisaran nilai normal. Namun, ketika sistem keamanan *open cloud* berbasiskan IDS dan IPS tidak aktif nilai CPU *usage* mengindikasikan pada kisaran nilai yang sangat tinggi. Prosentase dari nilai CPU usage komputer *open cloud* nampak pada table 2. Analisa selanjutnya yaitu adalah membahas hasil dari serangan yang menggunakan teknik D-DoS terhadap komputer server *open cloud* berbasiskan IDS dan IPS. Yang dijadikan target yaitu komputer *web server* dengan IP address 195.168.1.20. Prosentase dari nilai CPU usage komputer web server nampak pada table 3.

Tabel 3. Hasil Pengujian D-DoS

No	Jenis Pengujian	Percobaan ke	Server CPU usage (%)	
			Open cloud	Web server
1	IDS dan IPS non aktif	1	59,8	57
		2	83,1	61
		3	85,5	67
2	IDS dan IPS aktif	1	27,5	4
		2	21	2
		3	23,7	2

KESIMPULAN

Kesimpulan yang diambil dari penelitian terkait sistem keamanan *open cloud* berbasiskan IDS dan IPS adalah :

1. Server IPS mampu menerapkan snort dengan *mode inline afpacket* yang dapat mengindentifikasi jenis-jenis serangan yang terjadi di dalam jaringan.

2. *Rules* di dalam snort dapat dikombinasikan dengan *rules* di dalam firewall yang mampu mendeteksi dan menolak paket yang terdeteksi sebagai ancaman.
3. Server IPS berhasil mendeteksi jenis-jenis serangan yaitu sniffing, scanning dan D-DoS yang dapat menampilkan *alerts* yang tercatat pada log di dalam *database* snort.
4. Server IPS mampu mencegah serangan D-DoS yang teridentifikasi dari nilai CPU usage, dimana sistem IPS diaktifkan berkisar antara 59,8% - 85,5% dan ketika sistem IPS diaktifkan CPU Usage Server kembali ke keadaan normal berkisar 2% - 4%.

DAFTAR PUSTAKA

[1] http://variety.com/2015/digital/news/sony-hack-anniversary-cybersecurity-data-1201633671/
[2] Saali Pooja Anilbhai, Chandres Parekh, Intrusion Detection and Prevention System for IoT, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Volume 2, Issue 6, 2017, ISSN: 2456-3307.
[3] Armbrust M, Fox A, Griffith R, Joseph AD, Katz R, Konwinski A, Lee G, Patterson D, Rabkin A, Stoica I, Zaharia M: A view of cloud computing. Commun ACM 2010, 53(4):50–58.
[4] Purbo, Ono. W, "Membuat Sendiri Cloud Computing Server Menggunakan Open Source", Yogyakarta: Andi Offset , 2012
[5] Simon M.C Cheng, 2014. Proxmox High Availability. Packt Publishing. Oktober 2014. ISBN: 9781783980888.
[6] J.Jabez, B.Muthukumar.Dr, Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, International Conference on Computer, Computer and Convergence (ICC 2015), Volume 48, 2015, Pages 338-346, ISSN: 1877-0509.
[7] Bilal Maqbool Beigh, Prof.M.A.Peer, Intrusion Detection and Prevention System: Classification and Quick Review, ARPN Journal of Science and Technology, Vol. 2, No. 7, August 2012, ISSN: 2225-7217
[8] http://www.oracle.com/technetwork/systems/articles/snort-base-jsp-138895.html
[9] http://www.oxid.it/cain.html
[10] https://nmap.org/
[11] https://www.digitalattackmap.com/understanding-ddos/