IMPLEMENTASI HONEYPOT UNTUK MENGUNGKAP POLA *PORT SCANNING ATTACKS* DALAM JARINGAN

Raditya Aji Habsoro
Teknologi Jaringan
Sekolah Vokasi
Universitas Gadjah Mada
raditya.aji.h@mail.ugm.ac.id

Nur Rohman Rosyid
Teknologi Jaringan
Sekolah Vokasi
Universitas Gadjah Mada
nrohmanr@ugm.ac.id

Hidayat Nur Isnianto
Teknologi Jaringan
Sekolah Vokasi
Universitas Gadjah Mada
hnisnianto@ugm.ac.id

Intisari—Gangguan yang ada dalam sistem jaringan sangat bermacam-macam, mulai dari virus, atau *worm, malware, port scanning,* penanaman *backdoor*, hingga penyerangan *denial of service.* Dampak dari serangan ini dapat menyebabkan suatu server jaringan mati dan mematikan aktivitas yang ada. Saat ini banyak aplikasi keamanan jaringan seperti anti-virus berbasis kesamaan *signature*, namun teknik ini rentan terhadap *false negative* disaat pustaka *signature* sudah tidak mutakhir.

Tindakan antisipatif dengan mengetahui ancaman lebih dini menjadi salah satu solusi yang baik. *Honeypot* merupakan sistem yang sengaja dibangun untuk diselidiki, diserang ataupun dikompromikan. Penerapan honeypot akan mendapatkan data penyerangan pada suatu jaringan. Makalah ini melaporkan pola distribusi penyerangan yang berupa serangan *port scanning* dari data yang sudah didapat. *Honeypot* diterapkan pada jaringan internet pada area *perimeter* di lingkungan kampus Teknologi Jaringan, Sekolah Vokasi, UGM.

Kata Kunci : *Port scanning*, Honeypot, Dionaea

Abstract—existing disorders in the network system are very diverse, ranging from viruses, or worms, malware, port scanning, planting backdoor, to denial of service attacks. The impact of this attack can cause a network server dead and deadly activity there. Today many network security applications such as anti-virus signature-based similarity, but this technique is vulnerable to false negative when the signature is not the latest well-known reference.

Anticipatory action by early knowing the threat is to be one a good solution. Honeypot is a system that purposely built to be investigated, attacked or compromised. Implementation of the honeypot will get data on a network attack. This paper reports the distribution pattern of the attacks in the form of port scanning attacks from the data that has been obtained. Honeypot is applied to the Internet in a campus perimeter at the Network Technology Program, Vocational School, UGM.

Keywoards : Port scanning, Honeypot, Dionaea

I. LATAR BELAKANG

Gangguan yang ada dalam sistem jaringan sangat bermacam-macam mulai dari virus, atau *worm, malware, port scanning,* penanaman *backdoor*, hingga penyerangan *denial of service.* Saat ini banyak aplikasi keamanan jaringan seperti anti-virus berbasis kesamaan *signature*, namun teknik ini rentan terhadap *false negative* disaat pustaka *signature* sudah tidak mutakhir. Teknik kesamaan *signature* ini menuntut kemutakhiran pustaka *signature*, namun tidak mudah untuk mendapatkannya. Setiap saat penyerang akan dengan mudah membuat variasi malware sehingga *signature* -nya akan terus berubah.

Perang melawan malware, virus, worm, dan kegiatan yang bersifat merusak tidaklah mudah. Tindakan antisipatif menjadi salah satu solusi yang baik. Suatu serangan memiliki tahap-tahap yang diawali dengan kegiatan spionase untuk mengetahui kelemahan sistem target serang dengan cara pemindaian. Pemindaian ini atau dikenal dengan *port scanning* akan mengirimkan paket TCP ataupun UDP dengan nomor *port* tertentu untuk mengetahui kemungkinan kelemahan target serang melalui tanggapan yang didapat dari target serang.

Teknik yang paling mudah dan cukup handal untuk mengetahui adanya pemindaian adalah dengan menggunakan *honeypot* sebagai perekam lalu lintas data *port scanning*. *Honeypot* sendiri adalah suatu komputer yang akan memiliki nilai yang sangat berharga apabila frekuensi serangan terhadapnya tinggi. Hal ini dikarenakan dia adalah komputer yang berpura-pura memiliki layanan-layanan umum dengan membiarkan kelemahannya terbuka, sehingga menarik penyerang untuk melakukan penyerangan. Sebagai alat keamanan, *honeypot* dapat diatur untuk menjebak penyerang yang berusaha menyerang sistem komputer target melalui penelusuran, *scan*, dan penyusupan [1].

Penelitian ini menggunakan *honeypot* untuk merekam data *port scanning* yang masuk pada jaringan kampus. Data *port scanning* terkumpul selama 7 bulan mulai bulan November 2014 – Juni 2015 menggunakan Dionaea Honeypot. Ekstrasi log data menghasilkan visualisasi pola distribusi serangan *port scanning* yang mencerminkan perilaku penyerang pada jaringan kampus. Dengan adanya visualisasi ini dapat membantu administrator jaringan melakukan tindakan prefentif untuk mengamankan jaringan yang dikelolanya.

II. KAJIAN PUSTAKA

A. *Peran port scanning Dalam Identifikasi Sistem Target Serang.*

Penggunaan komputer dan jaringan internet menjadi hal yang penting bagi semua kalangan saat ini, baik dunia kerja maupun dunia pendidikan. Sebagai hasil dari penggunaan komputer dan jaringan internet tersebut, keamanan untuk jaringan internet menjadi prioritas utama di kalangan internasional [2]. Terdapat bermacam-macam serangan yang dapat mengganggu jaringan internet, salah satunya adalah *port scanning*. *Port* scanning dianggap sebagai metode intrusi jaringan berbahaya dikarenakan metode ini dipakai untuk menemukan saluran komunikasi pada jaringan atau *port* yang terbuka kemudian menyimpan informasi yang dapat digunakan untuk melakukan serangan. [3]

B. *Port Scanning*

Port scanning adalah bentuk yang lebih bertarget dari pengumpulan informasi yang mencoba untuk profil layanan yang dijalankan pada target potensial. *Port Scanning* adalah salah satu teknik popular yang digunakan para penyerang untuk mencari celah sehingga mereka dapat masuk ke suatu layanan. Semua sistem yang terhubung ke jaringan LAN ataupun internet melalui modem menjalankan layanan dengan *port* yang sudah dikenal dan tidak dikenal. *Port scanning* terdiri dari penyelidikan sejumlah jaringan untuk mencari *port* yang terbuka.

C. *Honeypot* sebagai sensor dan *logger* serangan *port scanning*.

Secara umum, *honeypot* dapat didefinisikan sebagai sebuah sumberdaya sistem informasi yang berguna untuk mendeteksi kasus penggunaan yang tidak dapat terotorisasi atau tidak diperbolehkan secara hukum dari sumber daya tersebut. [4]. *Honeypot* adalah sistem komputer yang sangat fleksibel pada internet yang dapat menjadi alat keamanan dan diatur untuk menjebak penyerang yang berusaha menyerang sistem komputer target melalui penelusuran, *scan*, dan penyusupan. Selain itu *Honeypot* adalah perangkap untuk mendeteksi, menangkap, menyesatkan para penyusup yang mencoba untuk menyerang sistem atau mendapatkan akses tidak sah. Kegunaan honeypot terletak pada saat terjadi penyerangan.[5].

D. *Dionaea*

Dionaea merupakan penerus dari Nepenthes, python sebagai bahasa pemrogramannya, menggunakan libemu untuk mendeteksi *shellcodes*, mendukung ipv6 dan tls, serta dibuat oleh Markus Kotter. Dionaea dapat mendeteksi *malware* yang menyerang ke sistem dengan mengemulasikan protokol SMD, HTTP, FTP, TFTP, MSSQL, MySQL, dan SIP[6].

SIPSession (*Session Initiation Protocol*) adalah protokol *signaling* yang digunakan untuk membuat, mengelola dan mengakhiri sesi di jaringan berbasis IP. *Session* bisa menjadi panggilan telepon dua arah yang sederhana atau bisa menjadi sesi konferensi multi-media kolaboratif. Hal ini memungkinkan untuk menerapkan layanan seperti suara yang diperkaya e-commerce, halaman web klik untuk memanggil atau Instant Messaging yang berbasis IP (SIPtutor). SIP telah menjadi pilihan bagi layanan yang berkaitan dengan Voice over IP (VoIP) di masa lalu. Ini adalah standar (RFC 3261) yang diajukan oleh *Internet Engineering Task Force* (IETF).

Layanan SIPcall adalah bagian dari SIP. Pada server dionaea, terdapat modul SIP yang digunakan untuk menjebak para penyerang. Serangan yang dilakukan oleh penyerang menggunakan SIPcall yang secara bersamaan dalam jumlah banyak. Masih seperti pada SIPSession yang termasuk dalam SIP, dimana SIP adalah VoIP untuk Dionaea honeypot. Protokol VoIP yang digunakan adalah SIP karena itu adalah standar de facto untuk VoIP saat ini. Berbeda dengan beberapa *honeypot*s VoIP lainnya, modul ini tidak tersambung ke VoIP registrar / server eksternal. Ini hanya menunggu pesan masuk SIP (misalnya PILIHAN atau bahkan INVITE), log semua data insiden *honeypot* dan / atau pembuangan data biner (lalu lintas RTP), dan bereaksi sesuai, misalnya dengan menciptakan sesi SIP termasuk saluran audio RTP.

Mssqld adalah bagian dari Microsoft Sql server. Dalam Dionaea terdapat modul dari Sql server (http://dionaea.carnivore.it/). Bisa dikatakan bahwa penyerang menyerang bagian tersebut. Mssqld mempunyai port 1433. Jadi bisa dikatakan bahwa saat melakukan penyerangan menggunakan *service* Mssqld, penyerang melakukan serangan terhadap port 1433.

Mysqld juga dikenal sebagai MySQL Server, adalah program utama yang melakukan sebagian besar pekerjaan di instalasi MySQL. MySQL Server mengatur akses ke direktori data MySQL yang berisi *database* dan tabel. Direktori data juga lokasi default untuk informasi lain seperti file log dan file status. Ketika server MySQL dijalankan, ini akan mengelola koneksi jaringan dari program client dan mengelola akses ke *database* atas nama klien-klien. MySQL mempunyai port 3306. Jadi bisa dikatakan bahwa saat melakukan penyerangan menggunakan *service* MySQL, penyerang melakukan serangan terhadap *port* 3306.

E. *Data Mining Digunakan Untuk Mencari Pola Serangan Port Scanning*

Keamanan sistem komputer dan keamanan data beresiko terus menerus. Pertumbuhan pesat internet dan peningkatan serangan jaringan mendorong untuk membuat sistem yang dapat mengetahui serangan pada jaringan komputer. Sebuah sistem yang dipasang dalam jaringan untuk mengetahui suatu serangan contohnya adalah honeypot. Honeypot yang dipasang akan menyimpan data dari penyerang jaringan. Data yang tersimpan tersebut misalkan saja IP penyerang, *service*, *port* sumber, *port* tujuan dan lain sebagainya. Setiap serangan yang masuk ke honeypot akan tersimpan di *database*. Data tersebut yang akan diolah sehingga dapat menjadi sebuah informasi.

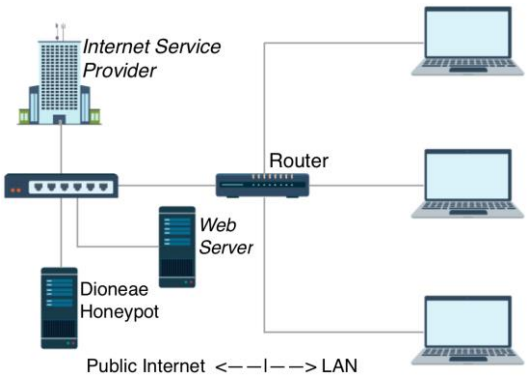
F. *Pola Serangan Port Scanning Sebagai Indikator Potensi Serangan*

Aktivitas penyerangan jaringan dapat dilihat dari pola yang tidak sesuai dengan perilaku normal[7]. Dengan jumlah data yang besar akan menjadi lebih penting dan menantang untuk mencari tahu bagaimana perilaku serangan. Data yang terkumpul akan diamati bagaimana polanya. Pola tersebut menjadi visualisasi dari data yang ada. Menggunakan visualisasi dapat memberikan pandangan dalam melakukan pengamatan data. Dengan cara tersebut maka perilaku akan terdeteksi secara visual[8].

III. METODOLOGI DAN PERCOBAAN

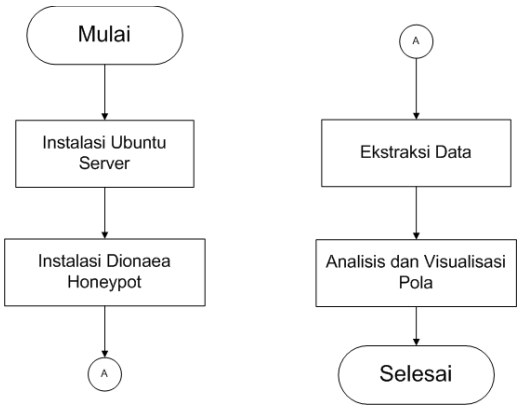
A. *Rancangan Topologi Jaringan Honeypot*

Pada percobaan ini digunakan Dioneae honeypot dan dipasang pada jaringan kampus. Instalasi Dioneae honeypot diletakkan pada segmen *backbone* jaringan bersama dengan server layanan-layanan kampus lainnya seperti Web Server. Gambar 1 memperlihatkan topologi jaringan honeypot yang digunakan dalam percobaan ini.



Gambar 1 Rancangan Topologi

B. *Prosedur Penelitian*



Gambar 2. *Flowchart* Pembuatan Pola

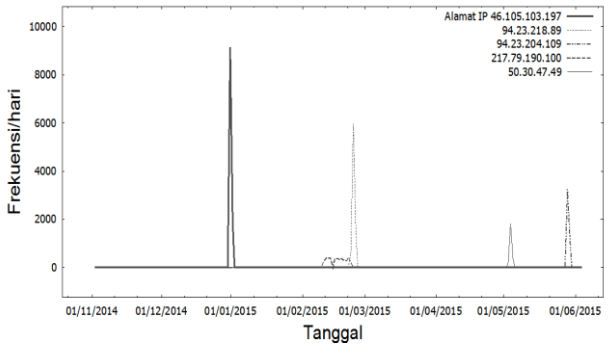
Metodelogi percobaan pada penelitian ini diawali dengan instalasi sistem operasi Linux Ubuntu server. Dionaea Honeypot dipasang pada platform Ubuntu server dengan alamat IP publik x.x.34.235. Selama 7 bulan mulai dari tanggal 3 November 2014 sampai 4 Juni 2015 data diambil dan disimpan didalam basisdata. Langkah berikutnya adalah ekstraksi log data untuk mendapatkan *preprocessing data* yang berisi data *connection timestamp*, alamat IP honeypot, protokol layanan, dan alamat IP penyerang.

Preprocessing data ini selanjutnya dilakukan penggalian data untuk mendapatkan visualisasi pola distribusi serangan *port scanning.* Diungkap 5 layanan yang memiliki frekuensi diserang paling tinggi, selanjutnya pada tiap-tiap layanan tersebut diambil 5 alamat IP penyerang. Kemudian dilakukan visualisasi pola distribusi serangan *port scanning.*

IV. HASIL DAN PEMBAHASAN

A. *Pola Distribusi Penyerangan Layanan SIPSession*

Distribusi pola serangan pada layanan SIPSession diperlihatkan pada Gambar 3.

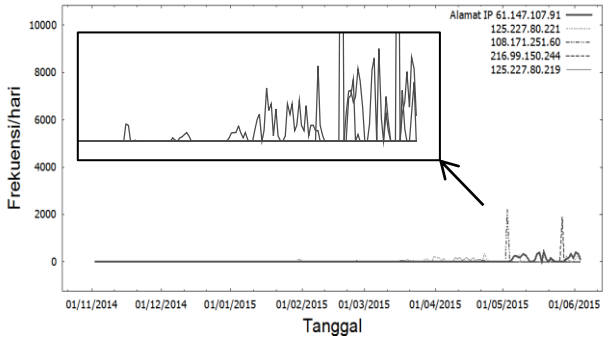


Gambar 3. Pola Distribusi Penyerangan Layanan SIPSession

Frekuensi *port scanning* (serangan) yang dilakukan oleh alamat IP 46.105.103.197 mencapai 9160 serangan pada bulan Januari 2015 dan tidak berlangsung lama. Alamat IP selanjutnya adalah 94.23.218.89 dengan frekuensi serangan tertinggi mencapai 5975 serangan pada tanggal 24 Februari 2015. Penyerangan dilakukan selama 3 hari dimulai taggal 23 sampai 25 Februari 2015. Penyerangan dari alamat IP 94.23.204.109 berjumlah 4410 selama 2 hari. Serangan terbesar terjadi tanggal 29 Mei 2015 dengan jumlah 3226. Alamat IP 217.79.190.100 melakukan sejumlah serangan sebanyak 3967 secara tersebar selama 14 hari dengan frekuensi tidak lebih dari 500 tiap serangan. Sementara alamat IP 50.30.47.49 memiliki 2304 total serangan yang dilakukan selama tiga hari.

Pola distribusi serangan dengan target layanan SIPSession ini cenderung tidak dilakukan secara terus-menerus. Serangan terjadi dengan periode yang sempit untuk masing-masing penyerang. Terlihat pada Gambar 3 bahwa setiap alamat IP tidak melakukan perulangan serangan. Bisa jadi perilaku serangan ini adalah serangan yang disengaja dilakukan.

B. Pola Distribusi Penyerangan Layanan Mssqld

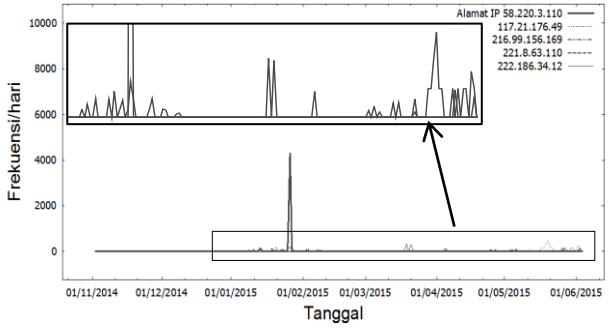


Gambar 4. Pola Distribusi Penyerangan Layanan Mssqld

Pola distribusi serangan pada layanan Mssqld yang dihasilkan oleh 5 alamat IP terlihat tersebar mulai bulan Januari 2015 dan secara intensif pada tiga bulan terakhir, seperti tergambar pada Gambar 4. Terlihat bahwa ada dua alamat IP yang melakukan serangan masing-masing hanya sekali saja dengan durasi yang cukup pendek, yaitu 108.171.251.60 dan 216.99.150.244. Kedua alamat IP tersebut masing-masing menyerang dengan total frekuensi 2208 dan 1858.

Sementara tiga alamat IP lainnya adalah 61.147.107.91, 125.227.80.221 dan 125.227.80.219 menyerang dengan durasi yang cukup lama dan bervariasi. Alamat IP 61.147.107.91 melakukan serangan mulai tanggal 5 Mei sampai 4 Juni 2015, dengan total frekuensi serangan mencapai 4730. Pada tanggal 28 Januari sampai 3 Juni 2015 terjadi serangan dengan total frekuensi 3766 yang dilakukan oleh alamat IP 125.227.80.221, terlihat frekuensi serangan perharinya cukup bervariasi. Sementara alamat IP 125.227.80.219 yang masih dalam blok alamat IP yang sama dengan alamat 125.227.80.221 melakukan serangan pada tanggal 4 Februari 2015 dan dilanjutkan mulai tanggal 9 – 23 April 2015 dengan total frekuensi serangan sebesar 1329. Pola distribusi serangan yang menyebar dalam waktu yang cukup lama bisa dibangkitkan oleh komputer yang terinveksi malware sehingga melakukan *scanning* secara *background process* tanpa diketahui oleh pemiliknya.

C. Pola Distribusi Penyerangan Layanan Mysqld

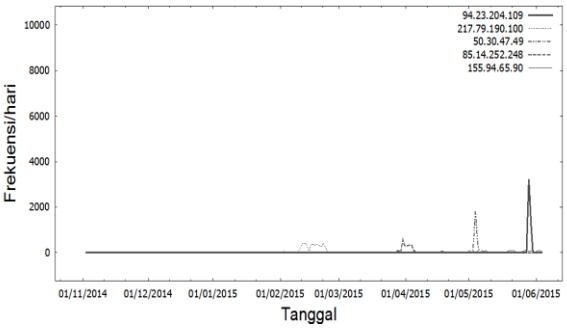


Gambar 5. Pola Distribusi Penyerangan Layanan Mysqld

Pola distribusi serangan pada layanan Mysqld digambarkan pada Gambar 5. Dari kelima alamat IP yang diamati, terlihat satu alamat IP yang sangat intensif dibandingkan dengan keempat alamat IP lainnya. Alamat IP 58.220.3.110 adalah penyerang dengan frekuensi serangan tertinggi selama Dioneae Honeypot terpasang, yaitu 4334. Serangan ini hanya terjadi selama satu hari saja pada tanggal 27 Januari 2015, meskipun sebelumnya pada tanggal 14 Januari 2015 alamat IP ini telah menyerang dengan frekuensi yang rendah sekali, yaitu 96. Hal ini dicurigai berasal dari penyerang yang sengaja dan dilakukan secara manual bukan dari robot.

Alamat IP lainnya melakukan penyerangan dengan periode serangan yang lebih menyebar dalam beberapa hari saja. Pada tanggal 12 Mei sampai 3 Juni 2015 alamat IP 117.21.176.49 memiliki frekuensi serangan yang bervariasi setiap harinya. Alamat IP 219.99.156.169 terlihat menyerang dengan total frekuensi hanya 186 pada tanggal 9 Januari sampai 14 Februari 2015 setelah itu menghilang. Pola distribusi serangan seperti ini dapat dipertimbangkan ditimbulkan dari komputer personal yang terinveksi malware.

D. Pola Distribusi Penyerangan Layanan SipCall

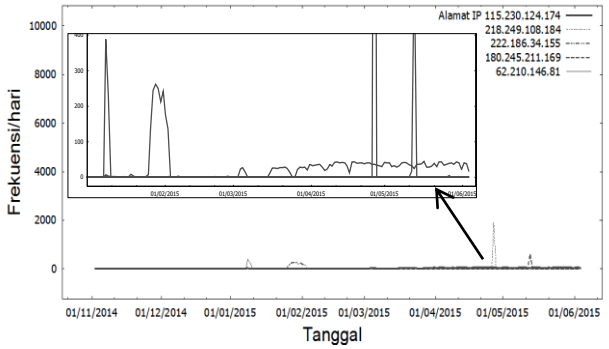


Gambar 6. Pola Distribusi Penyerangan Layanan SipCall

Gambar 6. Memperlihatkan pola distribusi layanan SipCall dari setiap alamat IP yang berbeda. Jumlah serangan yang dilakukan dari kelima alamat IP cukup beragam. Serangan terbesar berasal dari alamat IP 94.23.204.109. Serangan ini dilakukan selama dua hari pada tanggal 29 dan 30 Mei 2015 dengan total frekuensi serangan 4410. Alamat IP selanjutnya adalah 217.79.190.100 melakukan penyerangan dengan durasi 20 hari pada tanggal 3 - 23 Februari 2015. Frekuensi serangan terbesarnya mencapai 419. Frekuensi serangan yang dilakukannya cukup bervariasi setiap harinya dengan frekuensi total serangan menyentuh 3991. Sementara alamat IP 50.30.47.49 melakukan serangan selama 3 hari dengan frekuensi total serangan 2304. Selama 3 hari penyerangan, hari pertama frekuensinya mencapai 135, hari kedua meningkat signifikan mencapai 1806, dan pada hari ketiga turun kembali pada nilai 363. Alamat IP 85.14.252.248 melakukan serangan selama 11 hari. Puncak penyerangan dari alamat IP ini mencapai 576. Awal penyerangannya hanya terekam 44 serangan, kemudian semakin meningkat hingga hari ketiga dengan jumlah 576, memasuki hari keempat dan kelima jumlah serangan turun menjadi 294. Pada hari keenam terjadi peningkatan dengan jumlah serangan 315, kemudian mengalami penurunan hingga hari ke sebelas dan

kemudian terlihat tidak melakukan aktifitas serangan kembali. Alamat IP yang terakhir adalah 155.94.65.90. Serangan dari almat IP tersebut terjadi selama berhari-hari. Serangan awal dimulai 27 Februari 2015 dengan 6 serangan, kemudian menghilang. Serangan terjadi kembali tanggal 8 April hingga 4 Juni 2015. Serangan dari alamat IP tersebut terjadi berhari-hari, akan tetapi frekuensi serangan yang dilakukan setiap harinya tidak melebihi 100 serangan. Perilaku penyerangan yang terjadi cenderung diawali dengan sedikit, kemudian meningkat hingga mencapai puncak serangan, lalu turun dan kemudian menghilang.

E. Pola Distribusi Penyerangan Layanan Pcap



Gambar 7. Pola Distribusi Penyerangan Layanan Pcap

Pola distribusi serangan pada layanan Pcap dapat dilihat pada gambar 7. Frekuensi total penyerangan tertinggi dilakukan oleh alamat IP 115.230.124.174. Pola serangannya bersifat *low rate* maksimum 50 serangan per hari secara terus-menerus selama 6 bulan mulai dari tanggal 7 Januari dan berakhir 4 Juni 2015 (akhir dari data, dan cenderung masih terjadi sampai data honeypot diambil). Selanjutnya adalah alamat IP 218.249.108.184, melakukan serangan pada tanggal 27 April 2015 dengan frekuensi serangan 1891. Serangan yang dilakukan hanya sehari dengan jumlah besar, tidak ditemukan aktivitasnya pada hari yang lain. Alamat IP berikutnya adalah 222.186.34.155, serangan yang datang dari alamat IP tersebut dimulai sejak 19 Januari 2015 dengan 7 serangan dan berlanjut hingga 3 Februari 2015 dengan frekuensi serangan tertinggi terjadi pada tanggal 29 Januari 2015 dengan 261 serangan. Perilaku yang nampak adalah datang dengan sedikit serangan yang semakin hari semakin naik hingga memuncak, dan setelah itu turun hingga hari terakhir penyerangan. Alamat IP 180.245.211.169 melakukan serangan selama 2 hari diawali dengan frekuensi rendah kemudian meninggi dan berhenti. Serangan terjadi pada tanggal 12 dan 13 Mei 2015 dengan frekuensi serangan total mencapai 623 serangan. Pada hari pertama terlihat hanya 16 dan hari kedua meninggi sampai 607 lalu tidak ada aktivitas lagi dari almat IP tersebut. Tidak jauh berbeda yang terjadi pada alamat IP 62.210.146.81 yang melakukan penyerangan pada tangggal 9 dan 10 Januari dengan frekuensi total serangan 619. Serangan yang berlangsung selama 1 sampai 3 hari dapat dipertimbangkan serangan tersebut sengaja dilakukan oleh pihak tertentu untuk mencoba masuk jaringan.

V. KESIMPULAN

1. Setiap penyerang mempunyai pola tersendiri dan juga spesialisasi target serangnya.
2. Perilaku penyerang yang menyerang *port* pada layanan tertentu dapat diketahui melalui pola yang terbentuk. Penyerang yang menyerang pada *layanan* Sipcall cenderung datang sesaat dan tidak berlanjut. Untuk penyerang layanan Mssqld terdapat penyerang yang menyerang secara terus menerus dan juga hanya datang dan tidak datang kembali. Penyerang layanan Mysqld mempunyai perilaku yang hanya sekali datang lalu menghilang dan juga ada beberapa yang hanya datang selama satu bulan lalu menghilang.
3. Perilaku penyerangan SipCall terlihat naik hingga akhir penelitian meskipun berbeda alamat IP penyerangannya.
4. Perilaku penyerang Pcap bervariasi. Teradapat alamat IP yang menyerang tidak lama namun jumlah serngannya banyak, terdapat juga alamat IP yang menyerang setiap hari hingga akhir penelitian dengan jumlah yang tidak banyak, yaitu dibawah 100.
5. Setiap pola perilaku yang terbentuk dapat membantu administrator jaringan untuk melakukan tindakan preventif dalam pengamanan jaringan.

DAFTAR PUSTAKA

[1]. Thomas, T. M. (2004). Network Security First-Step. Boston: Pearson Education,Inc, publishing as Cisco Press.

[2]. Dabbagh, Mehiar, dkk. 2011. *Slow Port Scanning Detection***.** Department of Electrical and Computer Engineering American University of Beirut.

[3]. U. Kanlayasiri, S. Sanguanpong and W. Jaratmanachot. 2000. *A Rulebased Approach for Port Scanning Detection*. Chiangmai: 23nd Electrical Engineering Conference (EECON 23)

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

[5]. Keerthi, T Divya Sai. 2012. *Locating the Attacker of Wormhole Attack by Using the Honeypot* . India : Electrical Communication Engineering Department Indian Institute of Science

[6]. http://dionaea.carnivore.it/, diakses pada 1 Oktober 2014.

[7]. Das, Kaustav. 2009. *Detecting Patterns of Anomalies.* Pittsburgh : Machine Learning Department School of Computer Science Carnegie Mellon University.

[8]. Arindam Banerjee, Varun Chandola, Vipin Kumar, Jaideep Srivastava, dkk. *Anomaly Detection: A Tutorial*. University of Minnesota