ANALISIS LOG AKSES PENGGUNA PADA LAYANAN WEB SERVER PUBLIK UNTUK EVALUASI KEAMANAN SERVER

Imam Suharjo
Program Studi Teknologi Informasi Fakultas Teknologi Informasi
Universitas Mercu Buana Yogyakarta, Jl. Wates Km. 10 Yogyakarta 55753
Imam@mercubuana-yogya.ac.id

ABSTRAK

Server internet memberikan layanan beragam antara lain *web server, email server*, SSH, pop3, imap dan masih banyak yang lain. Hal yang cukup penting dalam sebuah *server* adalah menjaga supaya *server* tetap berjalan dengan normal dan aman dari gangguan. Dalam hal ini perlu melihat aspek keamanan sistem. Penelitian ini bertujuan untuk melakukan evaluasi *server web*, dari log yang tersimpan di *server*. Log akses yang dievaluasi berupa log akses ke SSH dan akses ke email dari auth.log yang ada di *server* linux. Data diambil dari log *server* pada *web server* yang menggunakan virtualmin sebagai *control panel*nya. Dari hasil penelitian didapatkan hasil bahwa masalah keamanan terhadap serangan ke SSH lebih sering terjadi di *server public* daripada serangan ke email. Serangan ke SSH rata-rata terjadi dalam 5 kali dalam setiap menit. Alamat IP penyerang dari data statistik paling banyak dari China. Meskipun data ini hanya data IP asal saja, belum tentu mencerminkan asal pelaku yang sebenarnya.

Kata kunci: log *server*, virtualmin, linux, *ssh server, email server*.

LOG ANALYSIS IN THE USER ACCESS ON THE WEB SERVICES SERVER FOR SECURITY SISTEM EVALUATION

ABSTRACT

Internet servers provide a variety of services including a web server, mail server, SSH, POP3, IMAP, and many others. It is quite important in a server to keep the server continues to run as normal and safe from tampering. In this case the need to look at the security aspects of the system. This study aims to evaluate webserver, from the log stored on the server. Log in evaluation in the form of access to the SSH access log and access to email from auth.log in linux server. Data retrieved from the server logs of webservers that use virtualmin as the control panel. From the results of the study showed that the issue of security against attacks to SSH servers are more common in the public than to attack email. SSH attacks to occur on average in five times in every minute. IP address of the attacker from statistical data is mostly from China. Although this data is only the IP data origin only, this does not directly reflect the actual origin of the perpetrator.

Keywords: log server, virtualmin, linux, sshserver, email server.

PENDAHULUAN

Web server merupakan salah satu layanan yang ada di dalam jaringan. *Web server* bisa bekerja

secara lokal maupun internet dengan akses publik (umum). *web* yang diteliti merupakan yang sudah berjalan dan sudah dikenal di Internet. *Web* memiliki domain dan IP Publik sehingga setiap orang punya akses bisa melakukan akses secara bebas pada halaman yang memang dibuka secara *public*. Sementara dalam *web server* ada bagian tertentu yang hanya bisa diakses oleh pengguna yang punya hak akses seperti untuk *update* informasi atau pengelolaan *server*.

Perencanaan jaringan yang benar dan sesuai standar menjadi hal yang penting dalam operasional jaringan dan mengatasi permasalahan yang ada. Selain perencanaan dalam tahap operasional diperlukan manajemen yang tepat untuk mengelola sistem yang ada. Salah satu hal yang penting dalam manajemen jaringan adalah Teknik *monitoring*. Sebuah sistem jaringan komputer yang juga kompleks membutuhkan pemantauan secara kontinu dan terintegrasi. *Monitoring* diperlukan untuk melihat kondisi yang aktual dan mempermudah analisa jika terjadi permasalahan di dalam jaringan. Topologi jaringan yang ada mempunyai konsep yang hampir sama. Yang membedakan umumnya adalah jumlah dan tipe perangkat yang digunakan.

Penelitian ini direncanakan untuk implementasi di jaringan kampus yang sudah berjalan. *Platform* jaringan yang menjadi objek penelitian ini adalah *webserver* yang berjalan pada *platform* sistem operasi Linux. Lebih khususnya linux yang digunakan adalah Debian *Server*. Penelitian ini bertujuan untuk melakukan analisis *logging* dari *server web* yang diakses oleh pengguna dari Internet. *Web* yang diteliti merupakan yang sudah berjalan dan sudah dikenal di Internet. *Web* memiliki domain dan IP Publik sehingga setiap orang punya akses dan bisa

mengakses secara bebas. Hal yang akan diamati adalah catatan log akses yang ada di *server*, beban kerja dan trafik jaringan yang masuk ke *server*. Kontribusi penelitian ini bagi pengembangan ilmu pengetahuan teknologi khususnya di bidang teknologi informasi yaitu menghasilkan suatu pengetahuan dan tambahan keilmuan mengenai *monitoring* dan evaluasi keamanan *server*.

Jaringan komputer adalah ”interkoneksi” antara minimal terdapat 2 komputer *autonomous*. Komputer ini terhubung dengan media transmisi kabel atau tanpa kabel (*wireless*). *Autonomous* adalah apabila sebuah komputer tidak melakukan kontrol terhadap komputer lain dengan akses penuh, sehingga dapat membuat komputer lain, *restart*, *shutdowns*, kehilangan *file* atau kerusakan sistem.

Berdasarkan jenis jaringannya, teknologi LAN dapat dibedakan menjadi tiga karakteristik yakni: ukuran, teknologi transmisi, dan topologinya. LAN mempunyai ukuran yang terbatas, yang berarti waktu transmisi dalam keadaan terburuknya terbatas dan dapat diketahui sebelumnya. LAN saat ini seringkali menggunakan teknologi transmisi kabel UTP.LAN tradisional beroperasi pada awalnya dengan kecepatan 10Mbps kemudian 100Mbps. Sedangkan saat ini kecepatan LAN yang umum dengan kabel UTP 100/1000 Mbps. (Tanutama, 1996)

Protokol adalah spesifikasi formal yang mendefinisikan prosedur-prosedur yang harus diikuti ketika mengirim dan menerima data. Protokol mendefinisikan jenis, waktu, urutan dan pengecekan kesalahan yang digunakan dalam jaringan. *Transmission Control Protocol/ Internet Protocol* (TCP/IP) merupakan protocol untuk mengirim data antar computer pada jaringan. Protokol ini merupakan protocol yang digunakan untuk akses Internet dan digunakan

untuk komunikasi global. TCP/IP terdiri atas dua protokol yang terpisah. TCP/IP menggunakan pendekatan lapisan (*layer*) pada saat membangun protokol ini.

TCP/IP dikirimkan ke setiap jaringan lokal sebagai subnet yang masing-masing subnet telah diberi alamat. IP yang menggunakan pengalamatan disebut dengan *IP Address*. *IP Address* ini digunakan untuk mengidentifikasi subnet dan *host* secara logik di dalam TCP/IP.

Firewall adalah sebuah sistem atau kelompok sistem yang menerapkan sebuah *access control policy* terhadap lalu lintas jaringan yang melewati titik-titik akses dalam jaringan. Tugas *firewall* adalah untuk memastikan bahwa tidak ada tambahan di luar ruang lingkup yang diizinkan. *Firewall* bertanggung jawab untuk memastikan bahwa *acces control policy* yang diikuti oleh semua pengguna di dalam jaringan tersebut. *Firewall* sama seperti alat-alat jaringan lain dalam hal untuk mengontrol aliran lalu lintas jaringan. Namun, tidak seperti alat-alat jaringan lain, sebuah *firewall* harus mengontrol lalu lintas *network* dengan memasukkan factor pertimbangan bahwa tidak semua paket-paket data yang dilihatnya adalah apa yang seperti terlihat. *Firewall* digunakan untuk mengontrol akses antara *network* internal sebuah organisasi Internet. Sekarang ini *firewall* semakin menjadi fungsi standar yang ditambahkan untuk semua *host* yang berhubungan dengan *network* (Purbo, 2000).

Client Server merupakan model jaringan yang menggunakan satu atau beberapa komputer sebagai *server* yang memberikan *resource*-nya kepada komputer lain (*client*) dalam jaringan, *server* akan mengatur mekanisme akses *resource* yang boleh digunakan, serta mekanisme komunikasi antar *node* dalam jaringan.

Selain pada jaringan lokal, sistem ini bisa juga diterapkan dengan teknologi internet. Dimana ada suatu unit komputer berfungsi sebagai *server* yang hanya memberikan pelayanan bagi komputer lain, dan *client* yang juga hanya meminta layanan dari *server*. Akses dilakukan secara transparan dari *client* dengan melakukan *login* terlebih dulu ke *server* yang dituju.

Server bisa memberikan banyak layanan untuk pengguna/ *client*. Beberapa layanan *server* antara lain : *webserver*, *email server*, ftp, ssh, pop3, imap dan lain-lain. *Web Server* adalah suatu program (dan juga mesin yang menjalankan program) yang mengerti protokol HTTP (*HyperText Transfer Protocol*) dan dapat menanggapi permintaan-permintaan dari *web* browser yang menggunakan protokol http (DGM). Saat ini layanan *web* juga sudah beragam diantaranya adalah https yang merupakan http yang lebih aman dengan tambahan security. Sebuah layanan *web* hosting pada dasarnya adalah sebuah *server* yang didalamnya telah disiapkan

Berbagai macam aplikasi pendukung. Untuk mengatur segala konfigurasi dan pengendalian pada situs yang berada pada sebuah layanan *web hosting*, digunakan sebuah *tool* terintegrasi yang disebut *Web Hosting Control Panel* (Pratama, 2008).

Mail *Server* adalah suatu entitas berupa komputer yang bertindak sebagai sebuah *server* (penyedia layanan) dalam jaringan komputer/ internet, serta memiliki fungsi untuk melakukan penyimpanan (*storing*) dan distribusi yang berupa pengiriman (*sending*), penjaluran (*routing*), dan penerimaan (*receiving*) e-mail. *Mail Server* berjalan dengan beberapa protokol pada TCP/IP, yakni SMTP (port 25), POP3 (port 110), dan IMAP (port 143). *Mail Server* memiliki tiga komponen utama yang menyusunnya,

yakni *Mail Transfer Agent* (MTA), *Mail Delivery Agent* (MDA), dan *Mail User Agent* (MUA). MTA bertugas mengatur pengiriman dan penerimaan e-mail, MDA bertugas mengatur pengiriman e-mail ke alamat yang sesuai pada jaringan lokal, sementara MUA bertugas untuk menjadi antarmuka yang menghubungkan *user* dengan *Mail Server*. (Pratama, 2008).

Virtualmin merupakan Control *panel web* yang merupakan sebuah modul *web*min yang memungkinkan untuk manajemen dengan lebih leluasa pada banyak *server virtual* pribadi yang terletak pada *server* yang sama. Pemilik *server* dapat mengelola Apache, Nginx, PHP, DNS, MySQL, PostgreSQL, kotak surat, FTP, SSH, SSL, Subversion/ Git repositori dan fitur lain yang mendukung aplikasi *webserver*. Virtualmin bisa *diinstall* secara langsung untuk *webserver* dari *web*min.com. Virtualmin memiliki port 10000 untuk akses ke *server*nya.

IANA dari *Internet Assigned Numbers Authority* adalah sebuah organisasi yang didanai oleh pemerintah Amerika Serikat yang mengurusi masalah penetapan parameter protokol internet, seperti ruang alamat IP, dan *Domain Name System* (DNS). IANA juga memiliki otoritas untuk menunjuk organisasi lainnya untuk memberikan blok alamat IP spesifik kepada pelanggan dan untuk meregistrasikan nama domain. IANA akan digantikan oleh sebuah badan non profit internasional yang disebut sebagai *Internet Corporation for Assigned Names and Numbers* (ICANN), karena meningkatnya penggunaan Internet. (IANA, 2015)

METODE

Bahan atau Materi Penelitian

Dalam melakukan evalausi keamanan dan akses ke *server* maka bahan dan meterial utama yang digunakan untuk penelitian ini adalah :

a. Jaringan internet.
b. Akses ke *Server*
c. Data akses log pada *Server web*
d. Data Akses trafik ke *server*

Alat yang dipakai

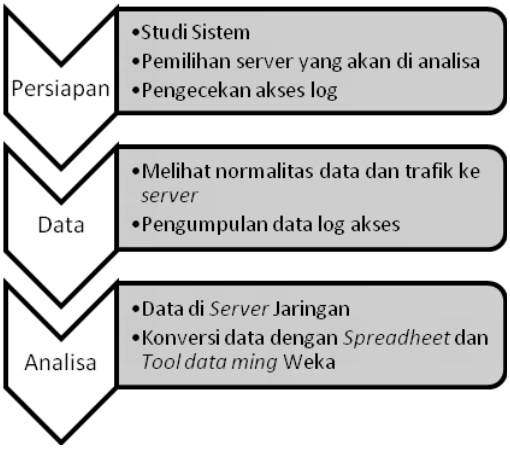
Beberapa alat dan perangkat lunak yang akan digunakan untuk penelitian ini adalah :

a. *PC Server* dan *PC Router*
b. *PC Terminal*
c. *Software* Microsoft Excell dan Weka

Jalan Penelitian

Secara umum dalam penelitian ini ada beberapa langkah-langkah utama yang akan dilakukan. Berikut ini yang akan dilakukan adalah :

1. Pengamatan terhadap sistem yang sudah berjalan dan dokumentasi
2. Pengambilan data log akses dan trafik secara *sampling*
3. Analisa log akses dan trafik yang berjalan
4. Evaluasi hasil analisa.



Gambar 1. Alur penelitian

Analisis Hasil

Analisis data dilakukan dengan menggunakan dan mengamati hasil implementasi dari sistem yang sudah digunakan. Parameter yang diamati dan dianalisa yaitu : fungsionalitas sistem, aksesibilitas, aspek keamanan, trafik jaringan dan beban

kerja perangkat. Data yang diambil dianalisis dengan statitik supaya bisa dibaca hasilnya.

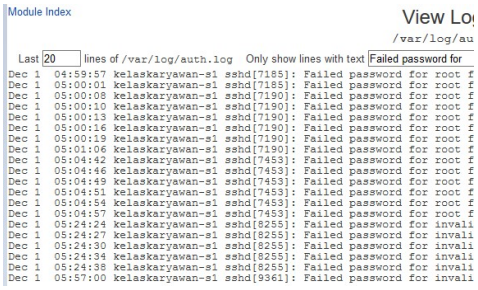
HASIL DAN PEMBAHASAN

Hasil dan pembahasan dalam penelitian ini lebih difokuskan pada hasil dari log penyerangan ke layanan SSH2. Terdapat 2 buah *server* yang digunakan sebagai sampel data dan diambil log pada rentang waktu tertentu. Data yang tersedia untuk analisis ini pada *server* 1 merupakan data dalam waktu 1 bulan, sementara *server* 2 dalam akumulasi data dalam 6 hari.

Server yang dianalisis log-nya menggunakan Virtualmin sebagai *control panel*nya. Untuk analisis data menggunakan Microsoft Excel untuk analisis stastistik data dan Weka untuk analisis dan membantu visualisasi. Alamat IP penyerang juga akan dikonversikan ke Negara asal IP. Yang perlu jadi catatan dalam analisis ini tidak semua pelaku penyerangan berasal dari IP yang terdata, karena dalam kasus yang sering terjadi IP *server* penyerang juga menjadi target serangan dan digunakan untuk menyerang *server* lain.

Keterbatasan dalam analisis ini hanya bisa mengetahui alamat IP yang digunakan untuk menyerang, bukan asal usul dari oknum penyerang yang sesungguhnya. Karena mungkin dia bersembunyi di balik alamat IP yang yang tercatat di *log server*. Mekanisme Pengambilan Data dalam penelitian ini pengambilan data dilakukan dari *control panel server* (virtualmin) untuk mempermudah pengambilan data. Pengambilan data juga bisa dilakukan secara langsung melalui SSH pada *file log* yang pada umumnya terdapat di /var/log/auth.log. Sistem Linux dalam hal ini di virtualmin mencatat berbagai log antara lain auth.log, syslog, cron.log, daemon.log, kern.log dan masih banyak layanan lain yang

tercatat dalam sistem log ini Data log asli sebelum difilter menampilkan semua data dari semua layanan yang dicatat lognya. Sehingga untuk mengambil log *file* tertentu perlu diseleksi terlebih dahulu.



Gambar 2. Seleksi data pada log sever

Dari file auth.log terdapat banyak data yang tertampil saat ini (saat dilihat) adalah data *realtime* (nyata). Untuk melihat log *file* tertentu atau tanggal tertentu bisa dilakukan dengan melakukan seleksi (*filtering*) dengan jumlah yang baris log yang juga bisa dibatasi. Misalkan Gambar 2 didapatkan dari seleksi sebanyak 20 data untuk log "*Failed password for*" yang merupakan catatan kegagalan dari sebuah IP yang akan melakukan akses masuk ke *server*. Dari data log ini akan terlihat beberapa data dalam satu baris yang berupa : data tanggal, jam, *server* yang diakses, id, *user* yang digunakan, IP penyerang, port layanan dan layanan yang diserang. Untuk memisahkan data sesuai dengan labelnya digunakan program bantu *spreadsheet* (Excel) menggunakan fitur *Text to Columns* sehingga bisa dibuat tabel data berupa : tanggal, jam, *server*, id, *user*, IP dan port. Dari data yang sudah dikonversi ini data sudah bisa mulai dianalisis.

Analisis User yang Menjadi Target

Pada tabel 1 ini merupakan data yang diakumulasikan dari semua sampel data yang ada yang

merepresentasikan jumlah *hit* serangan. Serangan yang terjadi dengan cara *brute force* (beruntun) dengan serangan beruntun yang bisa terjadi dalam rentan waktu yang singkat. Pada waktu yang hampir bersamaan bisa saja *server* diserang oleh dua IP yang berbeda asalnya.

Tabel 1. Tabel *user* yang menjadi target

User penyerang ssh	Jumlah	Persentase
Root	8176	85.00%
invalid user test	338	3.51%
invalid user nagios	206	2.14%
invalid user zabbix	142	1.48%
invalid user guest	140	1.46%
www-data	62	0.64%
invalid user zxin10	60	0.62%
invalid user apache	40	0.42%
invalid user Ubuntu	38	0.40%
invalid user zhaowei	36	0.37%
invalid user tomcat	33	0.34%

Dari data *user* yang diserang ke SSH 2 ini 94,19% untuk *server* 2 dan 85% untuk *server* 1 menggunakan *user root* sebagai target serangan dan sisanya menggunakan *user* lain seperti terlihat pada tabel 1. Jumlah menunjukkan *hit* serangan yang bisa saja dilakukan dari alamat IP yang berbeda namun menggunakan target *user* yang sama.

Analisis Alamat IP Asal Negara

Dari IP penyerang dapat dilihat alamat IP berasal dari berbagai IP di luar jaringan internal. Dengan bantuan *tool online* ipligence.com bisa dikonversi asal IP penyerang.

Dari data 1 bulan bisa dilihat ada sekitar 50 IP asal yang menyerang ke *server* 1 dari berbagai Negara. Jumlah menunjukkan jumlah *hit* serangan yang dilakukan oleh sebuah IP. Sebagai contoh 182.100.67.59 yang berasal dari China telah melakukan serangan sebanyak sekitar 23 ribu kali dari *sample* data yang diambil dalam rentang 1 bulan.

Dari tabel di atas IP yang memiliki asal Negara yang sama digabungkan dan dibuat dalam tabel di bawah ini. Tabel ini hanya mengambil 20 besar Negara asal penyerang untuk data selengkapnya bisa dilihat di lampiran yang terdiri dari 193 IP dan dari 38 negara asal. Jumlah alamat IP penyerang paling banyak berasal dari Negara China dengan jumlah 69 alamat IP selama 1 bulan, kemudian terdapat 22 IP dari Amerika.

Alamat IP Negara lain yang melakukan *hit* serangan ke *server* 1 jumlahnya di bawah China dan Amerika.

Gambar 3. Lokasi IP (utrace.de)

Dengan *tool online* untuk mencari lokasi IP bisa diketahui lokasi sebuah IP berada di Negara mana. Seperti contoh di gambar 3 dilakukan dengan *online tool* en.utrace.de. Sebagai contoh Gambar 3 IP 218.16.129.142 berada di China dan dikelola oleh ISP : China Telecom. Dari informasi IP juga bsia diketahui kontak detail dari pemilik/ pengelola IP. Apabila kita akan melakukan komplain bisa ke email pengelola IP yang bersangkutan.

Tabel 2. IP Asal penyerang di *Server* 1

No	*Row Labels*	*Count of Country*
1	China	69
2	United States	22
3	Russian Federation	14
4	Viet Nam	12
5	Netherlands	12
6	France	7
7	Brazil	7
8	Indonesia	5

Pada tabel di bawah ini merupakan sampel 10.000 data dari data yang diambil selama 15 hari menunjukkan data yang berbeda terjadi serangan dari 8 alamat IP yang berbeda-beda. Alamat IP juga sudah dikonversi ke Negara asal IP dan jumlah *count of IP* menunjukkan jumlah serangan yang dilakukan oleh IP masing-masing dengan total serangan dari 8 IP tersebut sebanyak 10 ribu serangan.

Tabel 3. IP Asal Penyerang ke *Server* 1

No	*Row Labels*	*Count of Country*
1	China	18
2	Vietnam	8
3	Netherlands	6
4	United States	5
5	Brazil	4

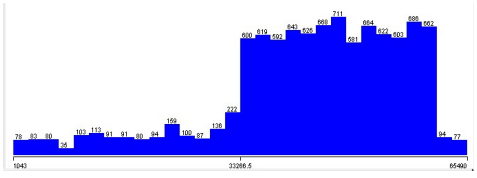
Analisis jumlah hit serangan

Server diserang beberapa kali oleh sebuah IP1 disisi lain IP2 juga memungkinkan menyerang dalam waktu yang hampir bersamaan. Dalam tabel 4 berikut ini merupakan *sample* data selama 6 hari pada *log server* yang diambil di *server* 2.

Tabel 4. Serangan SSH *Server* 2

Row Labels	***Count of date***
Hari 1	11518
Hari 2	15515
Hari 3	1869
Hari 4	10943
Hari 5	1701
Hari 6	8454
Grand Total	**50000**

Rata-rata serangan SSH dalam 6 hari dari 50.000 data serangaan ssh2 yang difilter didapatkan rata-rata serangan per hari sebesar 8333 serangan. Atau dapat dihitung rata-rata serangan terjadi dalam sekitar 5 kali dalam setiap menit. Serangan hampir terjadi setiap waktu. Analisis Port Target Serangan Port layanan di dalam jaringan berkisar antara 0 – 65535. Secara standar nomor *port* layanan SSH ada di *port* 22. Dari gambar terlihat *port* yang diserang sangat beragam namun lebih banyak terjadi pada *port* yang besar diatas 30.000.



Gambar 4. *Port* target sshd

Serangan SSH pada nomor *port* besar (*port* ribuan) diperkirakan 10 kali lebih sering daripada *port* yang bawah (nomor *port* ratusan).

Analis Log Serangan ke EmailSeperti halnya serangan terhadap layanan SSH2 terjadi juga serangan pada layanan email dengan

mencoba akses masuk ke email secara berulang. Di *server* 2 serangan terhadap layanan email lebih besar dari *server* 1. Namun secara umum jumlah serangan email lebih kecil daripada serangan ke layanan SSH.

Untuk melakukan seleksi terhadap layanan dovecot digunakan "dovecot-auth: pam_unix (dovecot: auth): authentication failure" dari *log* yang diseleksi terdapat 2468 *item* dalam *log*

Tabel 5. Target serangan email

No	*Row Labels*	*Count of email*
1	admin@umbyogya.com	183
2	support@umbyogya.com	178
3	marketing@umbyogya.com	176
4	sales@umbyogya.com	176
5	admin@kelaskaryawan-s1.com	100
6	info@kelaskaryawan-s1.com	100
7	mail@kelaskaryawan-s1.com	100
8	office@kelaskaryawan-s1.com	100

Tabel 6. Target Pengguna Serangan

No	*Row Labels*	*Count of user*
1	Support	301
2	Sales	299
3	Admin	298
4	Info	216
5	Test	212
6	Marketing	176
7	postmaster	121
8	*web*master	111
9	Office	105
10	Mail	103

Dari 2468 hit yang terjadi selama 1 bulan berupa serangan login email ke *server* 2 terdidistribusi ke dalam 12 alamat IP asal yang terlihat pada Tabel. *Server* 2 lebih banyak mendapatkan serangan dimungkinkan karena pengguna lebih banyak.

Tabel 7 Daftar IP penyerang svr2

No	*Row Labels*	*Count of ip*
1	95.141.35.85	960
2	149.202.193.235	900
3	87.120.37.12	229
4	202.51.116.222	96
5	94.102.53.178	84
6	80.82.64.28	80
7	155.133.10.76	77
8	185.3.134.111	32
9	5.39.217.6	17
10	186.251.105.100	12
11	118.189.72.127	2
12	186.30.73.137	1
	Grand Total	2490

KESIMPULAN

Dari penelitian yang telah dilakukan bisa disimpulkan beberapa hal sebagai berikut :

1. Serangan ke layanan SSH2 terjadi cukup sering dengan rata-rata serangan sebanyak 6 kali dalam 1 menit. Sementara jumlah serangan ke email lebih sedikit sekitar 3-4 kali dalam 1 jam.
2. Dari data statistik, alamat asal IP penyerang yang paling banyak berasal dari Negara China, hal ini dimungkinkan IP Publik yang berada di China juga masuk dalam kelompok pengguna IP terbesar setelah Amerika. IP penyerang bisa saja menyerang satu *server* saja atau menyerang banyak *server*.
3. Target akses pengguna yang sering digunakan untuk menyerang paling banyak adalah *root* yang biasanya memang menjadi *password default* untuk *server* linux.
4. Meskipun *port default* untuk layanan SSH adalah 22, namun serangan cenderung melakukan *brute force* ke *port-port* atas yang

bernilai ribuan dan serangan cenderung ke arah *port* yang acak.

Ada beberapa yang belum dilakukan dalam penelitian ini yang menarik untuk dilakukan dan bisa jadi penelitain berikutnya di antaranya:

1. Analisis untuk *log* konten yang akses untuk evaluasi keamanan pada level aplikasi seperti adanya: data tampering, *SQL Injection*, adanya Shell, dan lain-lain.
2. Analisis email *spam* atau aktivitas *server* yang digunakan untuk *relay* email atau *spamming*.

DAFTAR PUSTAKA

IANA. (2015). Retrieved from https://id.wikipedia.org/wiki/Internet_Assigned_Numbers_Authority

Arif Wicahyanto, E. W. (2012). Pendaftaran pengguna layanan hotspot berbasis web Pada hotspot mikrotik dan freeradius. *IJNS - Indonesian Journal on Networking and Security*.

Arifin, Y. (2013). IMPLEMENTASI QUALITY OF SERVICE DENGAN METODE HTB (HIERARCHICAL TOKEN BUCKET) PADA PT. KOMUNIKA LIMA DUABELAS. *JELIKU-Jurnal Elektronik Ilmu Komputer Universitas Udayana,* 1(2), 1-7.

Cahyono, K. (2010). Sistem Autentikasi Pengguna pada Pembangunan PC Router Mikrotik di Madrasah Aliyah Negeri Kota Pasuruan. *KARYA DOSEN Fakultas Teknik UM*.

DGM. (n.d.). *Web Essentials*. Retrieved from Web Essentials: http://desource.uvu.edu/dgm/2120/in/steinja/lessons/01/01_05.html

Faulkner. (2001). Internet Bandwith Management Alternatives for Optiizing Network Performance. *Faulkner Information Services*.

Handriyanto, D. F. (2009). Kajian Penggunaan Mikrotik Router Os™ Sebagai Router Pada Jaringan Komputer. *Jurnal Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya*.

Husaini. (2008). Implementasi PC Router, DNS Server, Active Directori dan Proxy Server Menggunakan Windows Server 2003 untuk Pengembangan Jaringan Komputer. *Skripsi, Ilmu Komputer, Universitas Gadjah Mada, Yogyakarta.*

Journal. (2004). Staff of Linux. *Linux Journal Issue 126 October 2004, Build Your Own Router, SSC, Inc*.

Kadek, C. (2012). ANALISIS KINERJA RIP (ROUTING INFORMATION PROTOCOL) UNTUK OPTIMALISASI JALUR ROUTING. *JELIKU - Jurnal Elektronik Ilmu Komputer Universitas Udayana*.

Kribo. (2010). *Radius.* http://net.comlabs.itb.ac.id/blog/?p=378.

Mancill, T. (2002). *Linux Routers : A Primer for Network Administrator, 2nd ed.* Prentice Hall.

Mulyanta, E. S. (2005). *Pengenalan Protokol Jaringan Wireless Komputer.* Penerbit Andi.

Nico Wijaya, d. (2009). Analisis Dan Perancangan Mikrotik Untuk Manajemen Jaringan Pada Pt. Smailing Tour, . *Binus Jakarta*.

Pereira, M. (2007). Encyclopedia of Internet Technologies and Applications. *Information Science Publishing*.

Pratama, A. M. (2008). Perancangan Dan Implementasi Mail Server Berbasis Qmail Pada Jcpanel Web Hosting Control Panel . *SNATI*.

Pressman, R. S. (1992). *Software Engineering.* McGraw-Hill International.

Purbo, O. W. (2000). *Linux Untuk Warung Internet.* Jakarta: Elex Media Komputindo.

Rafiudin, R. (2006). *Membangun Firewalll dan Traffic Filtering Berbasis Cisco.* Yogyakarta: Penerbit Andi.

Riadi, I. (2011). Optimalisasi Keamanan Jaringan Menggunakan Pemfilteran Aplikasi Berbasis Mikrotik. *JUSI UAD*.

Tanenbaum, A. S. (1996). *Jaringan Komputer, edisi Bahasa Indonesia, edisi III.* Jakarta: Prenhallindo.

Tanutama, L. (1996). *Jaringan Komputer.* Jakarta: Elex Media Komputindo.

Taringan, A. (2009). *Bikin Gateway Murah Pakai Mikrotik, .* Yogyakarta: Penerbit Ilmu Komputer.

Werner, F. (1996). *The Encyplopedia of Networking, 2nd ed.* Alamanda, CA: Network Press, Sybex Inc.