Implementasi Honeypot Sebagai Pendeteksi Serangan dan Melindungi Layanan Cloud Computing

Dedy Panji Agustino[1)], Yohanes Priyoatmojo[2)], Ni Wayan Wiwin Safitri[3)]
STMIK STIKOM Bali
Jalan Raya Puputan No.86 Renon Denpasar - Bali, Telp. +62(361)244445
e-mail: panji@stikom-bali.ac.id

Abstrak

Cloud Computing adalah sebuah bentuk layanan yang membuka peluang untuk dapat diakses di manapun, memberikan kenyamanan, serta akses jaringan yang on-demand untuk penggunaan sumber daya komputasi terkonfigurasi. Sebagai salah satu layanan yang memanfaatkan jaringan komputer sebagai medianya, Cloud Computing juga tidak terlepas dari ancaman keamanan. Ancaman keamananan tersebut dapat berupa upaya login ke sistem dan serangan malware. Dalam penelitian ini, upaya pengamanan yang dilakukan adalah dengan menggunakan Honeypot. Honeypot adalah perangkat yang akan berprilaku dan menanggapi seperti sistem nyata. Tujuan dari penelitian ini adalah untuk membangun sistem Honeypot pada layanan Cloud Computing, melindungi layanan Cloud Computing dari serangan brute force dan malware, membangun sistem Honeypot pada Cloud Computing berbasis IaaS, mendeteksi serangan brute force dengan Kippo dan serangan malware dengan Dionaea. Dalam penelitian ini, memfokuskan pada 2 jenis serangan yaitu, serangan brute force dan malware. Metode yang dilakukan dalam penulisan penelitian ini adalah pembuatan flowchart, instalasi, konfigurasi paket software yang dibutuhkan dalam pembangunan sistem dan pengujian serangan. Hasil dari penelitian ini adalah sebuah sistem Honeypot yang dibangun pada VMware. Honeypot dapat melindungi layanan Cloud Computing dari serangan brute force dan malware dengan cara menyediakan port palsu dan sistem palsu yang menyerupai layanan Cloud tersebut. Layanan Cloud Computing berbasis IaaS dibangun dengan menggunakan Proxmox VE. Serangan brute force dideteksi oleh Kippo dan serangan malware dideteksi oleh Dionaea. Sistem Honeypot mencatat dan menampilkan aktifitas serangan ke dalam file log yang berupa file teks dan database MySQL.

Kata kunci: *Cloud Computing, Honeypot, Brute force, Malware.*

1. Pendahuluan

Keamanan jaringan komputer merupakan hal penting di dalam perkembangan teknologi informasi. Keamanan komputer seperti yang dikatakan oleh John D. Howard, seorang *Analisys of Security Incidents on the Internet* pada tahun 1989-1995, mengatakan bahwa : "*Computer Security is preventing attacker form achieving objectives through unauthorized access or unauthorized use of computer and network*". Yaitu proses pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara illegal dari komputer dan jaringan. Faktor-faktor penyebab resiko dalam jaringan komputer meliputi kelemahan manusia (*human error*), kelemahan perangkat keras komputer, kelemahan sistem operasi jaringan dan kelemahan sistem jaringan komunikasi. Beberapa ancaman di dalam jaringan komputer meliputi ancaman fisik berupa pencurian perangkat keras, kerusakan pada komputer dan perangkat komunikasi jaringan, *wiretapping* dan bencana alam. Ancaman yang bersifat logik berupa kerusakan pada sistem operasi atau aplikasi, virus, dan *sniffing*. Ancaman lain berupa *sniffer* (peralatan yang memonitor proses yang sedang berlangsung), *spoofing* (penggunaan komputer untuk meniru, dengan cara menimpa identitas *MAC Address* atau alamat *IP*), *Phreaking* (perilaku menjadikan sistem pengamanan telepon melemah), *remote attack*, *hole* (kondisi dari *software* dan *hardware* yang bisa diakses oleh pemakai yang tidak memiliki otoritas), *hacker* dan *cracker*.

Keamanan jaringan menjadi sangat penting bagi beberapa layanan, baik layanan finansial maupun nonfinansial yang memanfaatkan jaringan computer dalam pengoperasiannya. Salah satu layanan yang memanfaatkan jaringan komputer adalah layanan *Cloud Computing* atau komputasi awan. Menurut

NIST (*National Institute of Standards and Technology*), *Cloud Computing* adalah sebuah bentuk layanan yang membuka peluang untuk dapat diakses di manapun, memberikan kenyamanan, serta akses jaringan yang *on-demand* untuk penggunaan sumber daya komputasi terkonfigurasi (misalya jaringan, *server*, penyimpanan, aplikasi dan layanan) yang dapat dengan cepat dijalankan dengan upaya pengelolaan yang minim atau dengan menggunakan penyedia jasa layanan.

Pada tahun 2013 Akamai melaporkan Indonesia menjadi nomor 1 sebagai sumber serangan Internet (*malicious traffic*). Trafik serangan dari *IP* Indonesia berkisar 38% dari seluruh serangan di internet dibandingkan trafik dari sekitar 175 negara yang diteliti. Trafik serangan ini meningkat hampir 2 kali lipat dibandingkan data sebelumnya yaitu sekitar 21%. Akamai dalam laporan tersebut menyatakan bahwa *IP* yang terdeteksi sebagai sumber serangan bisa jadi tidak mencerminkan lokasi penyerang. Karena bisa saja seorang penyerang dari Amerika Serikat melancarkan serangan dari *IP* Indonesia melalui jaringan *botnet* atau komputer yang terinfeksi *malware*. Selain itu ESSET Indonesia pada bulan Mei 2013 melaporkan tingkat prevelansi *malware* di *ASEAN* cukup tinggi, yaitu sebesar 16,88%. Dari laporan tersebut, *malware* yang banyak beredar di Indonesia di antaranya adalah Ramnit dan Sality. Sedangkan berdasarkan hasil survei *malware* yang dilakukan ID-CERT, 52% *malware* yang dilaporkan adalah *Adware* dan 35%-nya adalah *Trojan*, sisanya merupakan *Virus*, *Worm*, *Keylogger*, *Spyware* dan *Backdoor*.

Berdasarkan uraian masalah keamanan di atas, maka penulis mengimplementasikan sebuah teknik keamanan dengan judul "**Implementasi *Honeypot* Sebagai Pendeteksi Serangan dan Melindungi Layanan *Cloud Computing***". *Honeypot* dapat mengalihkan penyerang dengan seolah-olah menjadi *server* asli sehingga dapat menjadi tempat untuk berinteraksi sementara bagi penyerang yang ingin melakukan serangan ke layanan *Cloud Computing*. Jadi bukan layanan *cloud* yang diserang oleh penyerang, melainkan sistem *honeypot* tersebut. Sehingga dengan *honeypot*, layanan *Cloud Computing* dapat terhindar dari berbagai serangan. *Honeypot* juga dapat mengumpulkan informasi mengenai penyerang yang meliputi identitas dan aktifitas yang dilakukan oleh si penyerang dalam melakukan serangan ke layanan *Cloud Computing*. Dari informasi inilah penyedia layanan *Cloud* nantinya dapat meningkatkan pengamanan pada layanan *Cloud Computing* yang dimilikinya.

2. Metode Penelitian

2.1. Studi Literatur

Studi literatur yang digunakan dalam pengumpulan data dan informasi yang diperoleh dengan cara pencarian materi yang berhubungan dengan implementasi *Honeypot* serta yang berkaitan denga layanan *Cloud Computing*. Materi tersebut berdasarkan buku, skripsi, jurnal online serta dokumen-dokumen terkait.

2.2. Perancangan Sistem

Perancangan sistem menyangkut pembuatan sebuah skema dari alur kerja sistem skema jaringan yang akan dibangun.

2.3. Implementasi Sistem

Implementasi sistem merupakan tahap instalasi *Proxmox VE* sebagai *Cloud Computing*, instalasi Ubuntu Server 14.04 dan instalasi *Honeypot Dionaea* dan *Kippo* pada Ubuntu Server 14.04. Serta tahap konfigurasi jaringan pada *Proxmox VE* dan Ubuntu Server 14.04.

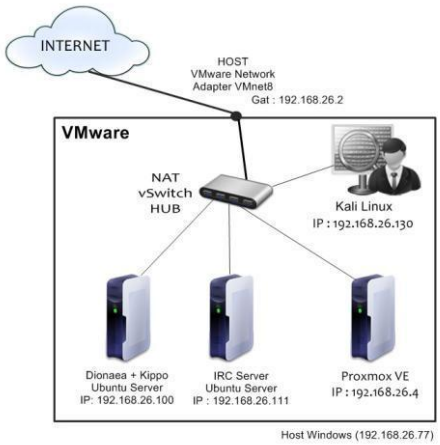
2.4. Pengujian Sistem

Pengujian yang dilakukan pada sistem *Honeypot* dan *Cloud Computing* yang telah dibangun. Pengujian yang dilakukan bertujuan untuk menganalisa dan mendeteksi serangan pada layanan *Cloud Computing* yang telah dibangun. Adapun *tool* yang digunakan dalam pengujian ini, meliputi *Nmap*, Hydra, dan Ncrack.

3. Hasil dan Pembahasan

3.1 Topologi dan Skenario Jaringan

Pada penelitian ini, digunakan topologi seperti pada Gambar 1. VMware berada di dalam *host* Windows. Di dalam VMware dipasang 4 sistem operasi yaitu Ubuntu Server pertama yang di dalamnya dipasang Kippo dan Dionaea. Ubuntu Server kedua sebagai *IRC Server*, Proxmox *VE* sebagai *Cloud Computing* dan Kali Linux sebagai penyerang. Keempat sistem operasi tersebut dihubungkan ke jaringan *NAT* dari VMware, yaitu VMnet8. Adapun rancangan alamat *IP* yang digunakan dalam penelitian ini dapat dilihat pada tabel 1.

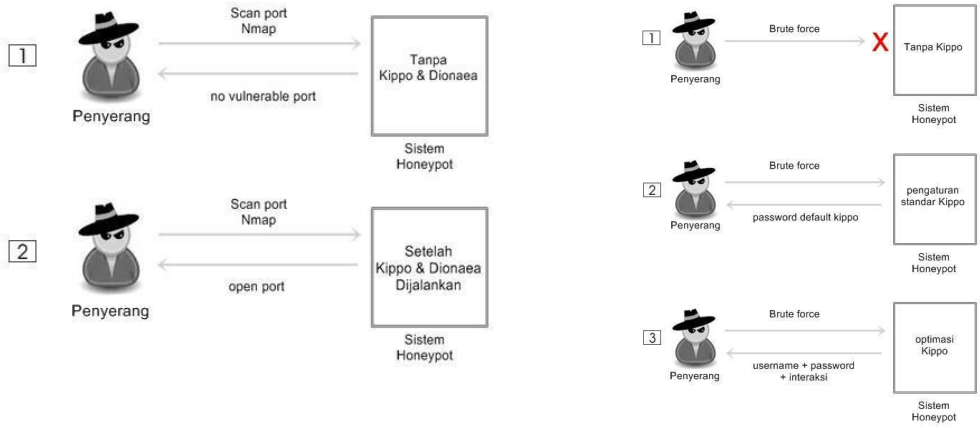


Gambar 1 Topologi Jaringan

Tabel 1 *IP Address*

Hardware	***IP Address***
Host Windows	192.168.26.77/24
Gateway	192.168.26.2/24
Proxmox *VE*	192.168.26.4/24
Ubuntu Server (*Honeypot*)	192.168.26.100/24
Ubuntu Server (*IRC Server*)	192.168.26.111/24
Kali Linux	192.168.26.130/24

Skenario pertama adalah skenario *scanning* jaringan untuk mengetahui informasi *port* yang terbuka. *Scanning* jaringan dilakukan dalam 2 tahap, yaitu tahap pertama ketika penyerang melakukan *scanning* dengan menggunakan *Nmap*, pada saat sistem *Honeypot* tidak dijalankan Kippo dan Dionaea, maka penyerang tidak akan mendapatkan *port* yang mudah diserang. Tahap kedua ketika penyerang melakukan *scanning port* dengan menggunakan *Nmap*, setelah Kippo dan Dionaea dijalankan, maka penyerang akan mendapatkan *port* yang mudah diserang. Skenario yang kedua adalah skenario serangan *brute force*. Serangan *brute force* dilakukan dalam 3 tahap, yaitu tahap pertama ketika penyerang melakukan serangan *brute force*, pada sistem tanpa Kippo, maka penyerang tidak akan mendapatkan *username* maupun *password* karena *port SSH* belum terbuka. Tahap kedua ketika penyerang melakukan serangan *brute force*, pada saat sistem *Honeypot* menggunakan pengaturan standar Kippo, maka penyerang akan mendapatkan *password default* dari Kippo. Tahap ketiga ketika penyerang melakukan serangan *brute force*, pada saat sistem *Honeypot* menggunakan pengaturan optimasi dari Kippo, maka penyerang akan mendapatkan *username* dan *password* lebih banyak yang akan digunakan untuk *login* ke sistem palsu yang disediakan Kippo. Serta interaksi terhadap sistem yang lebih banyak lagi seolah-olah menyerupai sistem yang sebenarnya. Skema skenario dapat dilihat pada gambar 2 :



Gambar 2. Skenario Serangan

3.2 Hasil Pengujian Serangan

Pengujian pertama dilakukan *scanning* terhadap jaringan. *Scanning* menggunakan *tool Nmap* pada Kali Linux. Scanning dilakukan pada 2 tahap yaitu *scanning* sebelum Kippo dan Dionaea dijalankan dan *scanning* setelah Kippo dan Dionaea dijalankan.

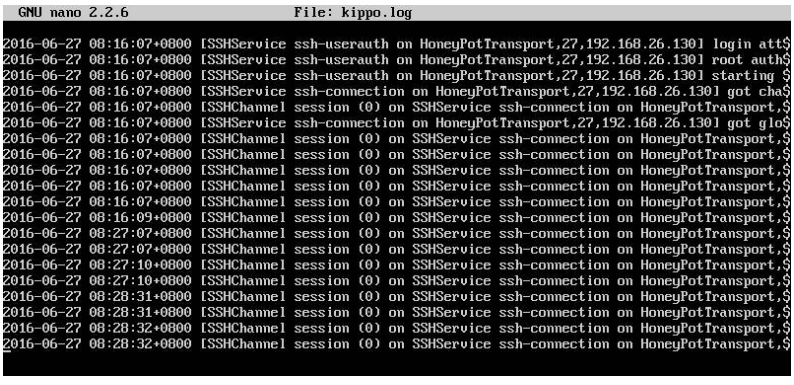
```
Nmap scan report for 192.168.26.4
Host is up (0.00040s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8649/tcp open  unknown
MAC Address: 00:0C:29:3F:0E:C5 (VMware)

Nmap scan report for 192.168.26.100
Host is up (0.00049s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
80/tcp   open  http
8649/tcp open  unknown
8651/tcp open  unknown
8652/tcp open  unknown
MAC Address: 00:0C:29:90:12:ED (VMware)
```

```
Nmap scan report for 192.168.26.4
Host is up (0.016s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8649/tcp open  unknown
MAC Address: 00:0C:29:3F:0E:C5 (VMware)

Nmap scan report for 192.168.26.100
Host is up (0.00061s latency).
Not shown: 986 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
42/tcp   open  nameserver
80/tcp   open  http
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1433/tcp open  ms-sql-s
3306/tcp open  mysql
5060/tcp open  sip
5061/tcp open  sip-tls
8649/tcp open  unknown
8651/tcp open  unknown
8652/tcp open  unknown
MAC Address: 00:0C:29:90:12:ED (VMware)
```

Berdasarkan hasil *scanning* tersebut dapat disimpulkan bahwa, *IP address* 192.168.26.100 yang merupakan *IP address* Ubuntu Sever mengalami perubahan. *Port* yang terbuka lebih banyak ketika Kippo dan Dionaea dijalankan. Hal ini menandakan bahwa Kippo dan Dionaea telah berhasil menyediakan *port-port* palsu. Setelah dilakukan *scanning*, selanjutnya adalah pengujian serangan *brute force*. Pengujian dilakukan dalam 3 tahap, yaitu pengujian tanpa Kippo, pengujian dengan pengaturan standar Kippo dan pengujian dengan optimasi Kippo. Pengujian serangan *brute force* ini menggunakan *tool* Hydra dan Ncrack pada Kali Linux. Serangan *brute force* dilakukan dengan menggunakan *password dictionary*. Dengan 10 kombinasi *password* dan 10 kombinasi *user login*. Adapun hasil dari pengujian serangan *brute force* ini berhasil dideteksi oleh Kippo. Kippo menyimpan aktifitas serangan ke dalam 2 bentuk *log*, yaitu dalam *file* teks dan *database* MySQL. *File log* Kippo dapat dilihat pada Gambar 5 di bawah ini:

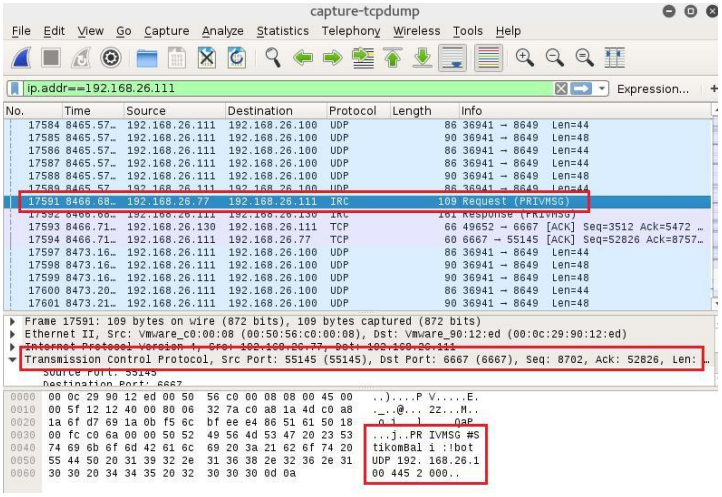


Gambar 3. File Log Kippo

Berdasarkan Gambar 3 Kippo berhasil mendeteksi percobaan *login*. Kippo mencatat kombinasi *username* dan *password* yang digunakan untuk *login* ke sistem Kippo.

Selanjutnya adalah pengujian serangan *malware*. Pengujian ini dilakukan dalam 3 tahap, yaitu pengujian tanpa Dionaea, pengujian dengan pengaturan standar Dionaea dan pengujian dengan optimasi dari Dionaea. *Malware* yang digunakan adalah trojan Kaiten, dengan menggunakan 3 perintah dari trojan Kaiten, yaitu TSUNAMI, *PAN* dan *UDP*. Serangan TSUNAMI dengan perintahnya adalah “TSUNAMI

<target> <secs>" merupakan *PUSH* dan *ACK flooder*. Serangan *PAN* dengan perintahnya adalah "PAN <target> <port> <secs>" merupakan *SYN flooder*. Serangan *UDP* dengan perintahnya "UDP <target> <port> <secs>" merupakan *UDP flooder*. Serangan dilakukan terhadap *port* yang disediakan oleh Dionaea. Serangan dari trojan Kaiten tersebut ditangkap dengan menggunakan *tool* Wireshark. Untuk mengetahui perubahan trafik jaringan pada sistem *Honeypot* saat terjadi serangan digunakan *tool* Ganglia. Adapun hasil dari salah satu serangan tersebut dapat dilihat pada Gambar 4 di bawah ini



Gambar 4. Serangan *UDP* pada *Port* 445

Pada Gambar 4 menunjukan serangan *UDP* pada *port* 445. Data diambil pada baris 17501 yang menunjukan bahwa dari *IP address* 192.168.26.77 melakukan *request* PRIVMSG ke *IP address* 192.168.26.111. melalui *port* 55145 ke *port* 6667. Adapun data yang didapatkan adalah sebuah pesan PRIVMSG pada *channel* #StikomBali dengan isi pesan "!bot UDP 192.168.26.100 445 2000".

4. Simpulan

Kesimpulan yang didapat dari hasil penelitian "Implemetasi *Honeypot* Sebagai Pendeteksi Serangan dan Melindungi Layanan *Cloud Computing*" ini adalah sebagai berikut :

1. Sistem pendeteksi serangan untuk layanan *Cloud Computing* dibangun pada VMware. Di mana sistem *Honeypot*, *Cloud Computing*, dan Sistem Operasi penyerang diinstal pada VMware tersebut. Di dalam VMware juga ditambahkan *IRC Server* karena dalam penelitian ini *malware* yang digunakan adalah Trojan Kaiten yang merupakan *botnet IRC*.
2. Sistem *Honeypot* dapat melindungi layanan *Cloud Computing* dari serangan *brute force* dan *malware* dengan cara menyediakan *port-port* palsu. Serta menyediakan sistem palsu seolah-olah seperti layanan *Cloud Computing* yang sebenarnya. Di dalam sistem palsu tersebut penyerang dapat berinteraksi seperti layaknya sistem nyata, seperti melihat, membuat dan menghapus *file* atau *folder* di dalamnya. Walaupun penyerang berhasil membuat atau menghapus *file* atau *folder* di dalam sistem palsu tersebut, namun *file* atau *folder* tersebut sebenarnya tidak terhapus atau berubah karena masih tersimpan di dalam program yang disimulasikan oleh *Honeypot*. Sehingga layanan *Cloud Computing* dapat terlindungi dari serangan.
3. *Cloud Computing* berbasis *IaaS* (*Infrastructure as a Service*) dibangun dengan menggunakan Proxmox *VE*. Sistem *Honeypot* tersebut dikonfigurasikan pada jaringan komputer yang sama dengan layanan *Cloud Computing*. Pada Proxmox *VE* dilakukan konfigurasi *firewall* untuk mengijinkan beberapa trafik yang diperlukan dan memblokir trafik yang ingin dilindungi pada layanan *Cloud Computing* ini. Dalam penelitian ini trafik yang diijinkan adalah yang masuk ke *localhost*, *port* 8649 (Ganglia) dan *port* 8006 agar Proxmox *VE* dapat diakses secara *remote* melalui *web*. Sedangkan trafik lainnya diblokir adalah semua trafik selain yang diijinkan tersebut.
4. Serangan *Brute force* dideteksi oleh *Honeypot* Kippo. Kippo mensimulasikan *port SSH* (22) dan menyediakan *filesystem* palsu sebagai tempat interaksi sementara. Aktifitas serangan disimpan di dalam *log* kippo yang berupa *file* teks yaitu "kippo.log" dan berupa *database* MySQL dengan nama *database* "kippo".
5. Serangan *malware* dideteksi oleh *Honeypot* Dionaea. Dionaea mensimulasikan beberapa *port* berupa *port FTP* (21), *Name Server* (42), *HTTP* (80), *MSRPC* (135), *HTTPS* (445), *SMB* (445), *MySQL*

(3306), *MSSQL* (1433), *SIP* (5060). Serta menyimpan aktifitas serangan ke dalam *file log* berupa *file* teks bernama "dionaea.log".

Daftar Pustaka

[1] Dewannata D. Tujuan, Risiko dan Ancaman pada Keamanan Jaringan Komputer. www.ilmukomputer.com. Tanggal akses terakhir: 28 Juli 2016.

[2] ID-CERT. *Laporan Survey Malware*. Indonesia Computer Emergency Response Team. 2015.

[3] Leoresta AE. Implementasi *Honeypot* Sebagai Pendeteksi Malware Pada Layanan Cloud Computing. Yogyakarta: Universitas Islam Negeri Sunan Kalijaga; 2014.

[4] Husnan S. Implementasi *Honeypot* untuk Meningkatkan Sistem Keamanan Server dari Aktivitas Serangan. Surakarta: Universitas Muhammadiyah; 2013.

[5] Harjono. Deteksi Malware dalam Jaringan Menggunakan Dionaea. Techno. 2013; 14(2): 64-69.

[6] Mustofa MM, Aribowo E. Penerapan Sistem Keamanan *Honeypot* dan IDS pada Jaringan Nirkabel (Hotspot). Jurnal Sarjana Teknik Informatika. 2013; 1(1): 111-118.

[7] Tambunan B, Raharjo WS, Purwadi J. Desain dan Implementasi *Honeypot* dengan Fwsnort dan PSAD sebagai Intrusion Prevention System. ULTIMA Computing. 2013; 5(1): 1-7.

[8] Hatem SS, Wafy MH, El-Khouly MM. Malware Detection in Cloud Computing. IJACSA. 2014; 5(4): 187-192.

[9] Sadasivam GK, Hota C. Scalable *Honeypot* Architecture for Identifying Malicious Network Activities. Hyderabad: BITS, Pilani – Hyderabad Campus; 2015.

[10] Kheirkhah E, Amin SMP, Sistani HAJ, Acharya H. An Experimental Study of SSH Attacks by using *Honeypot* Decoys. Indian Journal of Science and Technology. 2013; 6(12): 5567–5578.

[11] Nestler V, Harrison K, Hirsch M, Conklin WMA. Principle of Computer Security Lab Manual. Edisi Keempat. United States: McGraw-Hill Education. 2015.

[12] Tan E. Dionaea – A Malware Capturing *Honeypot*. http://www.edgis-security.org/*Honeypot*/dionaea/. Tanggal akses terakhir: 4 Maret 2016.

[13] Pratama IPAE. Smart City Beserta Cloud Computing dan Teknologi-teknologi Pendukung Lainnya. Bandung: Informatika Bandung. 2014.

[14] Stallings W, Brown L. Computer Security Principles and Practice. United States: Pearson Education. 2015.

[15] Gunawan I. Pengembangan Brute Force Attack dan Penerapannya pada Crypt8 dan CSA-Rainbow Bagian 2. Jurnal Elektronik ROTOR. 2013; 1(2): 40-49.

[16] Department of Computation Linguistic. *Hydra Instalation Manual*. Institute for Bulgarian Language. 2012.

[17] Hantzis F. Ncrack. https://nmap.org/ncrack/man.html. Tanggal akses terakhir: 6 Maret 2016.

[18] Nmap. Panduan Referensi Nmap. https://nmap.org/man/id. Tanggal akses terakhir : 12 Maret 2016.

[19] Stalling W. Protocol Basic: Secure Shell Protocol. The Internet Protocol Journal. 12(4).

[20] Ubuntu. The Ubuntu Story. http://www.ubuntu.com/about/about-ubuntu. Tanggal akses terakhir: 7 Maret 2016.

[21] Arfriandi A. Perancangan, Implementasi, dan Analisis Kinerja Virtualisasi Server Menggunakan Proxmox, VMware EXS, dan Openstack. Jurnal Teknologi. 2012; 5(2): 182-191.

[22] Caraballo D, Lo J. IRC untuk Pemula. http://www.irchelp.org/irchelp/new2irc.html. Tanggal akses terakhir: 4 Juli 2016.

[23] Wireshark. Chapter Introduction. https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html. Tanggal akses terakhir: 13 Juli 2016.

[24] Jacobson V, Leres C, McCanne S. Tcpdump. http://tcpdump.org/tcpdump_man.html. Tanggal akses terakhir: 17 Juli 2016.

[25] Zarlis M, Handrizal. Algoritma & Pemrograman : Teori dan Praktik dalam Pascal. Edisi Kedua. Medan: USU Press. 2008.

[26] Bhatia JS, Sehgal RK, Kumar S. Botnet Command Detection Using Virtual Honeynet. IJNSA. 2011; 3(5): 177-189.

[27] Kumar S, Sehgal R, Singh P, Chaundhary A. Nephentes *Honeypot* based Botnet Detection. Journal of Advances in Information Technology. 2012; 3(4): 215-221.