ISBN : 978-979-3877-40-2

Universitas Bina Darma

PROSIDING

Bina Darma Conference Series on Computer Science (BDCSoCS)

SECURITY FOR SMART CITY

Fakultas Ilmu Komputer
Universitas Bina Darma

NOVEMBER 2017

Prosiding Bina Darma Conference Series on Computer Science

Fakultas Ilmu Komputer
Jl. A. Yani No. 3 Kampus Utama Plaju - Palembang
Website : http:// sentikom.binadarma.ac.id
Email : seminar.mahasiswa@binadarma.ac.id

ISBN : 978-979-3877-40-2

PROSIDING

Bina Darma Conference Series on Computer Science

(BDCSoCS)

SECURITY FOR SMART CITY

Fakultas Ilmu Komputer
Universitas Bina Darma
2017

Penerbit :
PPP-UBD Press
Published by:
Pusat Penerbitan dan Percetakan Universitas Bina Darma Press (PPP-UBD Press) Palembang

Committee

Reviewer dan Editor :

1. Suyanto, M.Kom.
2. Fatoni, M.Kom.
3. Nyimas Sopiah, M.Kom.
4. Kurniawan, M.Kom.
5. Heri Suroyo, M.Kom.
6. Febriyanti Panjaitan, M.Kom
7. Fitri Purwaningtyas, M.Kom.

KATA PENGANTAR

Bina Darma Conference Series on Computer Science (BDCSoCS) adalah konferensi nasional diselenggarakan untuk memfasilitasi mahasiswa dalam menyelesaikan tugas akhir/skripsi untuk mempublikasikan karya ilmiahnya. Seminar ini juga dilaksanakan guna meningkatkan Sumber Daya Mahasiswa (SDM), terutama tenga pengajar (dosen) yang juga merupakan peneliti perguruan tinggi dan berperan secara aktif dalam mengembangkan, memperbaiki dan memperkenalkan teknologi dalam menghadapi perdagangan bebas.

Seminar ini diselenggarakan secara berkala setiap tahunnya oleh Fakultas Ilmu Komputer Universitas Bina Darma dengan tema "***SECURITY FOR SMART CITY"***. Seminar ini mengundang pemangku kepentingan bidang teknologi, pelaku dan akademisi.

Sebagai akhit kata, kemi seluruh panitia berharap buku prosiding ini dapat bermanfaat bagi kita semua dan pada kesempatan ini kami mohon maaf jika terdapat hal-hal yang kurang berkenan. Kami mengucapkan banyak terimakasih pada semua pihak yang telah membantu terlaksananya BDCSoCS 2017.

Palembang, Desember 2017.

Panitia BDCSoCS 2017.

DAFTAR ISI

PENERAPAN SISTEM KEAMANAN *HONEYPOT* DAN *IPS* PADA JARINGAN NIRKABEL DI UNIVERSITAS BINA DARMA

[1]Polandri, [2]Usman Ependi, [3]Suryayusra
[1,2,3] Universitas Bina Darma Palembang
[1,2,3] Jalan Jendral Ahmad Yani No.12 Palembang
[1]poalndri@gmail.com, [2]u.ependi@binadarma.ac.id, [3]suryayusra@binadarma.ac.id

ABSTRACT

In today's network a computer never get out of weakness in security side. With so many vulnerabilities to make a computer network is very vulnerable exploited by an attacker to steal information and important data. Attack cases are caused due to a lack of improved security systems. For a university-level educational institutions of course, network security quality processing is needed, especially on wireless networks. The research method used in this study using action research methods or Honeypot action research combined with IPS using Portsentry provide solutions to the problem. IPS functions as a system that monitors network activity through IPS systems in inline mode and blocks suspicious IP addresses after data streams are matched with existing signatures, whereas Honeypot works to determine attacker activity and all activities leading to the honeypot are considered suspicious. The results showed that the ability of Honeypot combined with Portsentry can complement each other in detecting attacks that are not known by the IPS system.

Keywords : *Intrusion Prevention system, Honeypot, Portsentry, Honeyd*

I. PENDAHULUAN

Kasus serangan adalah disebabkan karena kurangnya peningkatan sistem keamanan. Bagi sebuah instansi pendidikan sekelas universitas tentunya pengolahan kualitas keamanan jaringan sangatlah diperlukan terutama pada jaringan *nirkabel*. Universitas Bina Darma sebagai instansi pendidikan yang menjadi tempat studi kasus penelitian ini sudah memakai jaringan *nirkabel*. Bagi Universitas Bina Darma penggunaan jaringan *nirkabel* tentu sangat memberikan kemudahan dalam mengakses internet karena jaringan *nirkabel* bisa memberikan layanan internet yang lebih cepat dan mudah. Akan tetapi dibalik kemudahan tersebut ternyata jaringan *nirkabel* juga memiliki beberapa kelemahan disisi keamanan, karena jaringan *nirkabel* tidak memiliki jalur pertahanan yang jelas sehingga para pengguna harus siap terhadap resiko yang harus dihadapi.

Honeypot merupakan sebuah sistem/komputer yang sengaja dijadikan umpan untuk menjadi target serangan dari penyerang (*attacker*). Komputer tersebut melayani serangan yang dilakukan oleh *attacker* dalam melakukan penetrasi terhadap *server* tersebut seolah-olah seperti *server* asli. *Intrusion Prevention System* (IPS) adalah teknik yang mengkombinasikan metode pencegahan yaitu *Intrusion Detection System* (IDS) dengan *Firewall* sebagai *filtering* terhadap akses yang tidak sah oleh pihak yang tidak bertanggung jawab.

Dalam penelitian ini penulis mengkombinasikan antara *Honeypot* dan *Intrusion Prevention System*. Jenis *Honeypot* yang digunakan adalah *low interactionHoneypotclient* yaitu *Honeyd* dan *Intrusion Prevention System* mengunakan *Portsentry* yang merupakan sebuah perangkat lunak yang dirancang untuk mendeteksi adanya *portscanning* dan merespon secara aktif jika ada *portscanning.*

2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode penelitian tindakan atau action research. Menurut Guritno, Sudaryono, dan Raharja (2011:46) *Action Research* merupakan bentuk penelitian tahapan (*applied research*) yang bertujuan mencari cara efektif yang menghasilkan perubahan disengaja dalam suatu lingkungan yang sebagian dikendalikan (dikontrol).

Action research menurut Davison, Martinsons dan Knock(2004) yaitu penelitian tindakan yang mendeskripsikan, menginterpretasi dan menjelaskan suatu situasi sosial atau pada waktu bersamaan dengan melakukan perubahan atau intervensi dengan tujuan perbaikan atau partisipasi. Adapun tahapan penelitian yang merupakan bagian dari *action research* ini, yaitu:

2.1Melakukan *diagnose* (Diagnosing)

Jaringan nirkabel Universitas Bina Darma menggunakan sistem keamanan *Firewall* dan *Proxy Server.* Kerusakan yang terjadi pada suatu jaringan akan mengakibatkan pertukaran data yang terjadi pada

jaringan tersebut akan melambat atau bahkan akan merusak suatu sistem jaringan. Insiden keamanan jaringan adalah suatu aktivitas terhadap keamanan sistem yang secara langsung atau tidak bertentangan dengan *security policy* sistem tersebut.

Pada dasarnya, *firewall* adalah titik pertama dalam pertahanan sebuah sistem jaringan komputer. Seharusnya *firewall* diatur agar melakukan penolakan (*deny*) terhadap semua *traffic* yang masuk kedalam sistem dan kemudian membuka lubang-lubang yang perlu saja. Jadi tidak semua lubang dibuka ketika sistem melakukan hubungan ke jaringan luar. Idealnya *firewall* diatur dengan konfigurasi seperti diatas. Beberapa *port* yang harus dibuka untuk melakukan hubungan keluar adalah *port* 80 untuk mengakses *internet* atau *port* 21 untuk FTP *file server.* Tiap-tiap *port* ini mungkin penting untuk tetap dibuka tetapi lubang-lubang ini juga merupakan potensi kelemahan atas terjadinya serangan yang akan masuk kedalam jaringan. *Firewall* tidak dapat melakukan pemblokiran terhadap jenis serangan ini karena *administrator* sistem telah melakukan konfigurasi terhadap *firewall* untuk membuka kedua *port* tersebut. Untuk tetap dapat memantau *traffic* yang terjadi dikedua *port* yang terbuka tersebut dibutuhkan sebuah sistem yang dapat melakukan pencegahan terhadap *traffic* yang membahayakan dan berpotensi menjadi sebuah serangan.

Penerapan sistem keamanan *Honeypot* dan *Intrusion Prevention System* Adalah salah satu solusi yang bisa digunakan untuk membantu seorang *Adminisrtor* jaringan dalam memantau lalu lintas dan memfilter paket-paket data yang lewat. Dan juga supaya bisa mencegah paket data yang berbahaya dan penyusup yang ingin memasuki sistem secara ilegal.

2.2 Membuat rencana tindakan(*Action Planning*)

Adapun dalam rencana tindakan akan dilakukan dengan cara membuat perancangan sistem keamanan *Honeypot* dan *Intrusion Prevention System* pada jaringan nirkabel Universitas Bina Darma. Adapun hal-hal yang dibutuhan adalah sebagai berikut:

1) Kebutuhan Perangkat Keras

a) Satu unit *Switch*
b) Satu unit laptop sebagai server *Honeypot dan IPS* dengan spesifikasi :
c) System Manufacturer: LENOVO
d) System Model: 80E4
e) BIOS: B0CN97WW
f) Processor: Intel(R) Core(TM) i7-5500U CPU @ 2.40GHz (4 CPUs), ~2.4GHz
g) Memory: 4096MB RAM
h) Available OS Memory: 4010MB RAM
i) Page File: 2403MB used, 2374MB available
j) Windows Dir: C:\WINDOWS
k) DirectX Version: DirectX 12

2) Kebutuhan Perangkat Lunak

a. Ubuntu 15.04

Merupakan salah satu sitem operasi distribusi linux berbasis Open Source yang biasanya digunakan sebagai server. Pada penelitian ini Ubuntu digunakan sebagai server bagi Honeypot dan IPS.

b. MySql

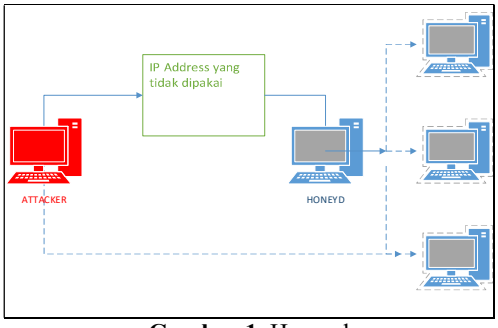
Merupakan sebuah aplikasi untuk mengimplementasikan RDBMS yang dididtribusikan secara gratis. Pada penelitian ini MySql digunakan untuk menyimpan log lalu-lintas serangan pada Honeyd.

c. Apache 2

Apache adalah sebuah nama *web server* yang bertanggung jawab pada *request-response* HTTP dan *logging* informasi secara detail(kegunaan basicnya). Digunakan sebagai *web server* utuk menjalankan *Honey-viz (*tempat melihat log hasil serangan berbasis *web diagram*).

d. Honeyd

Honeyd merupakan produk Honeypot yang dibuat oleh Niels Provos. Inti dari Honeyd, sistem ini akan mensimulasikan tingkah laku sebuah komputer beserta sistem operasinya, sehingga bisa mensimulasikan sebuah router cisco atau sebuah komputer lengkap dengan sistem operasi dan Webserver. Honeyd memiliki kemampuan untuk mensimulasikan TCP dan UDP selain itu sistem ini mampu memahami dan merespon ICMP dengan baik, selain itu Honeyd memiliki kemampuan untuk membuat virtual Honeypot dengan nomer IP yang banyak secara bersamaan.



Gambar 1. Honeyd

e. Portsentrys

Menurut Saeful Anwar (2012:31), PortSentry adalah sebuah perangkat lunak yang dirancang untuk mendeteksi adanya portscanning dan merespon secara aktif jika ada portscanning. Portscan adalah proses scanning berbagai aplikasi servis yang dijalankan di server Internet. Portscan adalah langkah paling awal sebelum sebuah serangan di lakukan. Pada penelitian ini portsentry digunakan sebagai IPS dikarenakan kemampuannya dalam memblok IP dari komputer attacker.

f. PHP 5

PHP adalah *bahasa pemrograman script server-side yang didesain untuk pengembangan web. Karena Honey-viz yang digunakan untuk mencatat log dari serangan ke server merupakan sebuah aplikasi berbasis web yang berjalan di bahasa pemrograman PHP maka dari itu PHP digunakan pada penelitian ini.*

g. Zenmap

Zenmap merupakan aplikasi penetration testing yang mampu melakukan scanning terhadap port-port yang aktif pada server target. Zenmap sendiri merupakan pengembangan dari Nmap. Kegunaan Zenmap pada penelitian kali ini adalah untuk melakukan port scanning terhadap server.

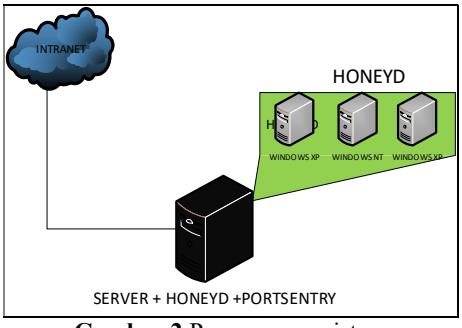
h. Nmap

Nmap merupakan tools berbasis linux yang digunakan untuk melakukan scanning terhadap port yang aktif.

i. Honey-viz

Merupakan tools berbasis web application yang digunakan untuk melihat statistik dan traffic dari lalu-lintas data serta serangan yang terjadi pada Honeyd.

3. Topology Perancangan Sistem



Gambar 2 Perancangan sistem

2.3. Melakukan tindakan(*Action Taking*)

Setelah melakukan installisasi Ubuntu 15.04 lalu penulis melakukan instalisasi Honeyd dengan cara mendownload lansung dari repository dengan mengetikkan apt-get install honeyd. Lalu setelah instalisai berhasil maka selanjutnya adalah membuat file konfigurasi honeyd. File konfigurasi memberitahu Honeyd sistem operasi apa yang akan ditiru, ports yang akan dibuka service apa yang akan dijalankan, dan lain-lain.

2.4. Melakukan evaluasi (*Evaluating*)

Peneliti meakuan evaluasi hasil temuan setelah proses simulasi, pada tahapan evauasi penelitian yang di lakukan adalah hasil penerapan sistem keamanan jaringan nirkabel Universitas Bina Darma. Pengujian ini akan di lakukan dengan beberapa skenario penyerangan. Hal ini dilakukan untuk menguji sejauh mana sistem keamanan yang di buat dapat berjalan dalam meghaapi berbagai serangan, adapun negalamatan IP *Address* adalah sebagai berikut:

Tabel 1 IP Address

Aplikasi	**IP Address**
Server + Portsentry	10.237.3.213
Honeyd 1	10.237.3.212
Honeyd 2	10.237.3.214
Honeyd 3	10.237.3.216

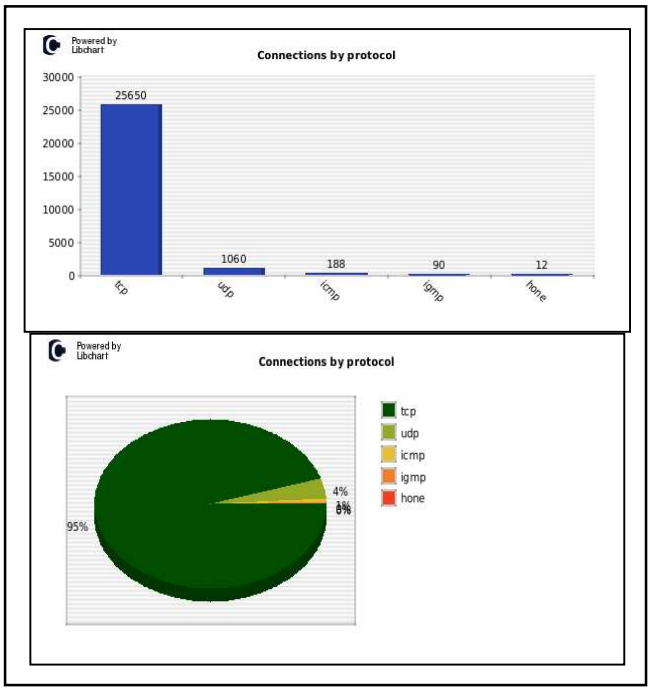
2.5. Pembelajaran (*Learning*)

Setelah masa simulasi*(action research)* dianggap cukup, kemudian peneliti melaksanakan *review* tahap demi tahap dan memahami prinsip kinerja pada sistem keamanan yang dibuat pada Universitas Bina Darma Palembang.

3. HASIL

a. Connection by Protocols

Dibawah ini menunjukkan lalu lintas data yang melewati protokol TCP, UDP, ICMP dan IGMP dapt kita lihat berapa jumlah data yang melewati protokol tersebut, yang paling yaitu pada TCP dan yang paling sedikit adalah HONE. Banyaknya jumlah yang terjadi pada protokol TCP adlah dikarenakan DdoS yang dilakukan mengunnaka aplikasi LOIC.

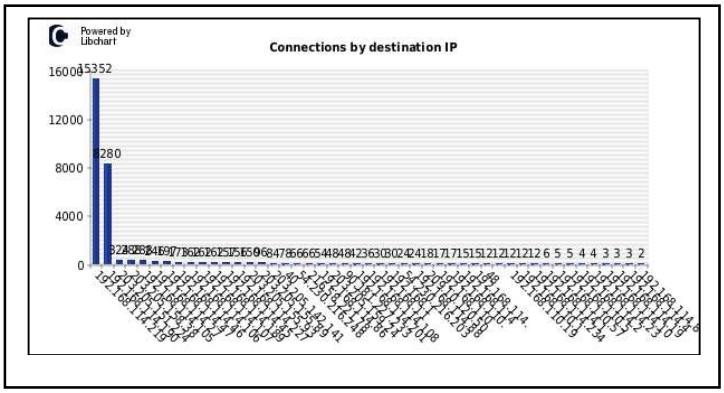


Gambar 3. Connection by Protocols

Gambar diatas menunjukkan bahwa koneksi yang diakukan pada protokol TCP, UDP, ICMP, IGMP, DAN HONE.

b. Connection Destintion by IP

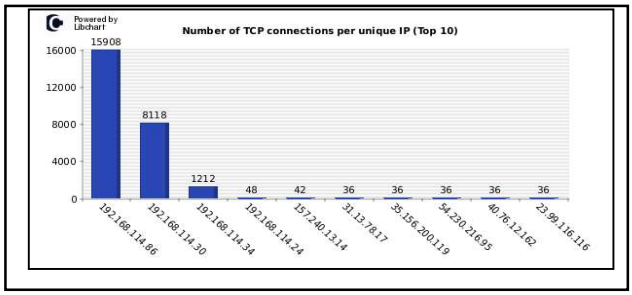
dibawah ini meunjukkan IP Adress yang paling banyak melakukan serangan dan melakukan interaksi dengan Honeyd . dapat kita lihat pada gambaar bahwa IP Address yang paling banyak melakukan srangna adalah 192.168.114.219 dan 192.168.114.190.



Gambar 3. Connection by Destination IP

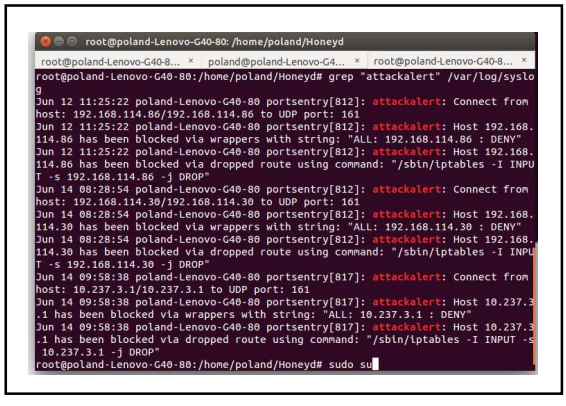
c. Number of TCP ,UDP, ICMP connections per unique IP

.Dapat dilihat dibawah ini 10 ip Address yang paling sering melakukan penyerangan terhadap sistem Honeyd. Yaitu melalui protokol TCP, UDP, ICMP.



Gambar 4. Number of TCP ,UDP, ICMP connections per unique IP

2. Analisis serangan terhadap Portsentry



Gambar 5 Serangan Terhadap Portsentry

Setelah dilakukan pengujian pada server yang telah terinstal Portsentry maka dilakukan analisis terhadap serangan yang telah Gambar diatas menunjukkan bahwa ada beberapa IP Address yang telah di blokir oleh Portsentry sehingga tidak bisa lagi melakukan koneksi untuk melakukan penyerangan yang mana **attackalert** adalah sebuah pesan peringatan.

4. SIMPULAN

Berdasarkan pengujian dan Analisis yang telah dilakukan terhadap penelitian *Honeypot* dan *IPS* pada jaringn *nirkabel* Universitas Bina Darma maka dapat disimpulkan:

1. *Honeyd* merupakan sebuah sistem atau komputer server yang sengaja dikorbankan untuk menjadi target serangan bagi penyerang, yang melayani setiap penyerangan yang dilakukan oleh penyerang dalam penetrasi terhadap server utama dengan menipu atau memberikan data palsu apabila ada *attacker* dengan maksud menyerang ketika ia masuk pada sistem atau server utama.
2. Pengujian *honeyd* dan *Portsentry* pada jaringan *nirkabel* Universitas Bina Darma telah membuktikan bahwa serangan dari *attacker* cukup mumpuni dan sistem keamanan yang diuji dapat bekerja dengan baik.
3. *Honeyd* akan merekam aktivitas dari *attacker* yang melakukan penyerangan terhadap server yang kemudian direspon dengan mengalihkan ke server palsu yang memberikan layanan mirip dengan layanan mirip server asli.
4. Dalam pegujian yang dilakukan *Portsentry* akan lansung me*blokir* setiap paket *scanning port*. Dimana ini merupakan langkah awal yang dilakukan oleh *attacker* untuk mencari kelemahan sistem atau yang disebut dengan *information gathering*.
5. Kombinasi anatara *Honeyd dan Portsentry* memberikan sebuah sistem keamanan berlapis yang memungkinkan *attacker* akan lebih sulit untuk menerobos sistem.

DAFTAR PUSTAKA

Ependi, U. (2015). Implementasi dan Pengujian Antarmuka Sistem Informasi Penanggulangan Kemiskinan Di Kabupaten Ogan Komering Ilir. *SISFO*, *5*.

Gondohanindijo J. (2011*), Sistem Untuk Mendeteksi Adanya Penyusup (IDS : Intrusion Detection System),* Fakultas Ilmu Komputer Universitas AKI. *Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei 2011*

Gondohanindijo J. (2012), *Sistem Keamanan Jaringan NIRKABEL,* Fakultas Ilmu Komputer Universitas AKI. *Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, Mei 201*

Gondohanindijo J. (2012), *IPS (Intrusion Prevention System) Untuk Mencegah Tindak Penyusupan / Intrusi*. *Majalah Ilmiah INFORMATIKA Vol. 3 No. 2, sept 2012*

Guritno, Sudaryono, dan Raharja (2011), Theory and application of IT Research – metodologi penelitian teknologi informasi, Andi.

K. D. Yesugade, K. D. Yesugade, Medankar Sanika Avinash, Nagarkar Sanika Satis Shah Charmi Sandeep, Surabhi Malav (2015*), Infrastructure Security Using IDS, IPS and Honeypot,* Computer Department, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India.

Manuaba I. B. V. H., Hidayat R., Kusumawardani S. S., (2012), *Evaluasi Keamanan Akses Jaringan Komputer Nirkabel (Kasus : Kantor Pusat Fakultas Teknik Universitas Gadjah Mada)*. *JNTETI, Vol. 1, No. 1, Mei 2012*

Oktaviani (2008), *Mengenal FIREWALL, Guna Darma*

Permadi A.F., Raharjo D.S, Christyowidiasmoro (2013), *Keamanan Jaringan pada IPTV, Teknik Elektro, Fakultas Teknologi Industri, Institut Teknologi Sepuluh Nopember (ITS) Jl. Arief Rahman Hakim, Surabaya 60111*

Pranata, H., Abdillah, L. A., & Ependi, U. (2015). Analisis Keamanan Protokol Secure Socket Layer (SSL) Terhadap Proses Sniffing di Jaringan. *arXiv preprint arXiv:1508.05457*.Ramya. (2015), *Securing the system using honeypot in cloud computing environment,*

R M. Phil Research Scholar,Department of ComputerScience VivekanandhaCollege of Arts and Sciencesfor Women, Namakkal,Tamil Nadu, India.

Setiawan. D. (2010), *Intrusion Prevention System (IPS) dan Tantangan dalam pengembanganya., Sistem Komputer FASILKOM UNSRI.*

Sofana I. (2012), *CISCO CCNA dan Jaringan Kompter,* Informatika

Sofana I. (2012), *CISCO CCNP dan Jaringan Kompter,* Informatika