

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**

**NOVEMBER 2017**



Fakultas Ilmu Komputer  
Jl. A. Yani No. 3 Kampus Utama Plaju - Palembang  
Website : <http://sentikom.binadarma.ac.id>  
Email : [seminar.mahasiswa@binadarma.ac.id](mailto:seminar.mahasiswa@binadarma.ac.id)

# 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 tenaga 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 akhrit kata, kami 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**

<b>NO</b>	<b>Penulis</b>	<b>Judul Artikel</b>	<b>Halaman</b>
1	Antoni, Ahmad Haidar Mirza, Fatmasari	SISTEM PENDUKUNG KEPUTUSAN PENEMPATAN PEGAWAI MENGGUNAKAN METODE MULTI FACTOR EVALUATION PROCESS (MFEP) (Studi Kasus : Badan Kepegawaian Daerah Kota Prabumulih)	1-6
2	Muhammad Agustian, Muhammad Akbar, Siti Sauda	APLIKASI SPAM FILTERING PADA GMAIL MENGGUNAKAN GOOGLE API DAN ALGORITMA BAYESIAN NETWORK	7-12
3	Novan Junaidi, Andri, Fitri Purwaningtias	SISTEM INFORMASI GEOGRAFIS HASIL MONITORING DAN EVALUASI PEMBANGUNAN FISIK BAPPEDA KABUPATEN SIMEULUE	13-17
4	Andini Puspita Sari, Deni Erlansyah, Fitri Purwaningtias	SISTEM INFORMASI PENJUALAN PADA TOKO DIAH FASHION BERBASIS WEB DENGAN METODE UP SELLING	18-24
5	Wahyu Rahmadi, Rusmin Syafari, Nia Oktaviani	Evaluasi Sistem Informasi Geografis Kependudukan Badan Pusat Statistik Kota Palembang Menggunakan Metode Information Utility System	25-31
6	Amelda, Andri, Fitri Purwaningtias	PENERAPAN METODE UP-SELLING PADA SISTEM INFORMASI PENJUALAN PERANGKAT KOMPUTER DI TOKO CHANDRA KOMPUTER	32-37
7	M. Nuzul Irhammullah, Muhammad Nasir, Fatmasari	SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN BIBIT UNGGUL PADA DINAS PERKEBUNAN PROVINSI SUMATERA SELATAN MENGGUNAKAN METODE ELECTRE	38-43
8	Arie Dian Irawan, Suyanto, Muhamad Ariandi	SISTEM INFORMASI GEOGRAFIS PERSEBARAN DBD DI WILAYAH KOTA PALEMBANG DENGAN MENGGUNAKAN ARCGIS	44-49
9	Alfi Heri Rahmadi, Vivi Sahvitri, Suyanto	SISTEM INFORMASI PRODUKSI DAN EKSPOR FIBREBOARD PADA PT. HLRF BERBASIS WEB DENGAN METODE ECONOMIC PRODUCTION QUANTITY (EPQ)	50-54
10	Enggi Ardius, Deny Erlansyah, Yesi Novaria Kunang	SISTEM INFORMASI EKSEKUTIF BERBASIS WEB PADA BAGIAN SECURITY NETWORK PADA BANK SUMSEL BABEL PUSAT	55-60
11	Rifaldi Okta Reza, Jemakmun, Ria Andryani	PERANGKAT LUNAK PENGADUAN DAN MONITORING FASILITAS UMUM KOTA PALEMBANG BERBASIS ANDROID SECARA REAL TIME (STUDI KASUS : DINAS PEKERJAAN UMUM DAN PENATAAN RUANG KOTA PALEMBANG)	61-66
12	Muhamad joni, Muhammad Nasir, Zaid Amin	BASIS DATA TERDISTRIBUSI PENERIMAAN DAN PENGELUARAN BARANG PROYEK PT. ADHI KARYA PALEMBANG	67-72
13	Rico Riansyah, Nyimas Sopiah, Siti Sauda	REKAYASA PERANGKAT LUNAK BOOKING TIKET MOBIL PADA YOANDA PRIMA BERBASIS MOBILE	73-78

14	Ebit Alfiando, Widyanto, Taqrin Ibadi	PERANGKAT LUNAK RESTORAN DAN RUMAH MAKAN HALAL DI KOTA PALEMBANG BERBASIS ANDROID	79-83
15	Sherly Monica, Zaniel Mazalisa, Evi Yulianingsih	PENERAPAN SEGMENTASI CITRA PADA TEKNOLOGI SIMULASI IDENTIFIKASI TANDA TANGAN DENGAN MENGGUNAKAN METODE THRESHOLD	84-88
16	Sigit Pamungkas, Fatoni, Timur Dali Purwanto	PENGEMBANGAN SISTEM INFORMASI PERSEDIAAN DAN PEMESANAN BARANGBERBASIS WEB PADA PT CAHAYA MURNI SRIWINDO MENGGUNAKAN METODE AGILE	89-94
17	Muhamad Yogi, Yesi Novaria Kunang, Evi Yulianingsih	RANCANG BANGUN E-COMMERCE TIKET PADA CINEMA 21 PALEMBANG INDAH MALL MENGGUNAKAN METODE PAYMENT GATEWAY	95-99
18	M Agung Nugroho, Deni Erlansyah, Susan Dian Purnama	SISTEM INFORMASI BIMBINGAN AKADEMIK DENGAN METODE CASE BASED REASONING BERBASIS WEBSITE DI UNIVERSITAS BINA DARMA	100-105
19	Muhamad Syarifudin, A. Haidar Mirza, Qoriani Widayati	PROTOTIPE SISTEM INFORMASI LOKET PEMBAYARAN TAGIHAN CV. SRIWIJAYA INDAH PALEMBANG BERBASIS GLOBAL POSITIONING SYSTEM (GPS)	106-108
20	Hendri Maszuki Alamsyah, Leon Andretti Abdillah, Susan Dian Purnamasari	REDESIGN JARINGAN KOMPUTER INTERNET DAN INTRANET PADA PT.SEKAWAN KONTRINDO	109-114
21	Sari Marvinionita, M.Nasir, Kiky Rizky Nova Wardani	EVALUASI SISTEM PEMBAYARAN TAGIHAN ONLINE (WEPAY) PADA CV SRIWIJAYA INDAH MENGGUNAKAN METODE HOT-FIT	115-119
22	Ide Gantama cahyadi, Muhammad Nasir, Kiky Rizky Nova Wardani	ANALISIS DATA MINING PADA DATA PEMBAYARAN DAN PENUNGGAKAN SEWA RUMAH SUSUN SEDERHANA SEWA KASNARIANSYAH MENGGUNAKAN METODE ASSOCIATION RULE	120-125
23	Marwan, Nyimas Sopiah, Febriyanti Panjaitan	ANALISIS METODE DAN LAYANAN LINK AGGREGATION PADA SERVER DATA DI DINAS TENAGA KERJA DAN TRANSMIGRASI PEMKAB OGAN ILIR	126-129
24	Among Firdaus, Widiyanto , Suzi Oktavia Kunang	PEMANTAUAN KEAMANAN LOCAL AREA NETWORK MENGGUNAKAN NMAP DAN HPING3 (STUDI KASUS LAN UNIVERSITAS BINA DARMA)	130-135
25	Endrico Aldrian, Kurniawan, Susan Dian Purnamasari	PENERAPAN METODE LEAST SQUARE PADA SISTEM INFORMASI PENJUALAN UNTUK PERAMALAN SALES REVENUE (STUDI KASUS PT GARUDA INDONESIA (PERSERO) TBK BRANCH OFFICE PALEMBANG)	136-142

26	Muhammad Ghufron, Linda Atika, Susan Dian Purnamasari	PENERAPAN DATA MINING UNTUK KLASIFIKASI PAKAN TERNAK AYAM MENGGUNAKAN METODE CLASSIFICATION RULE	143-146
27	Hendri, Alex Wijaya, Hutrianto	ANALISIS DAN PERANCANGAN VTP SERVER DAN VTP CLIENT PADA JARINGAN VLAN MENGGUNAKAN METODE RSJK (REKAYASA SISTEM JARINGAN KOMPUTER) PADA DINAS PENDIDIKAN PEMUDA DAN OLAHRAGA KABUPATEN BANGKA BARAT	147-152
28	Fauzal Halik, Muhammad Sobri, Nia Oktaviani	REKAYASA PERANGKAT LUNAK PUSAT INFORMASI UMKM DI KOTA PALEMBANG	153-158
29	Defry Andani, Syahril Rizal, Evi Yulianingsih	PERANCANGAN VIRTUAL PRIVATE NETWORK PADA STIK BINA HUSADA	159-163
30	Toni Pratama Yuda, Afriyudi, Ilman Zuhriyadi	SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN LOKASI TANAH PADA PT SGI MENGGUNAKAN METODE TOPSIS	164-170
31	Derry Isvandiar, Darius Antoni, Edy Surya Negara	JARINGAN INTERNET PADA CV SRIWIJAYA MAJU BERSAMA UNTUK MEMFASILITASI MASYARAKAT DESA DALAM MENGAKSES E-GOVERNMENT	171-176
32	M Hendry Hidayat, Deni Erlansyah, Hutrianto	PERANGKAT LUNAK PEMINTAAN BUNKER DI PT PERTAMINA MARINE REGION II PLAJU	178-183
33	Dicky Prayogo, Alex Wijaya, Timur Dali Purwanto	INVESTIGASI FORENSIK REMOTE EXPLOIT MELALUI JAVA APPLEFT ATTACK METHOD	184-188
34	Bambang Setiawan, Alex Wijaya, Febriyanti Panjaitan	PERANCANGAN CETAK BIRU PENGEMBANGAN JARINGAN KOMPUTER PADA BALAI BAHASA PROVINSI SUMATERA SELATAN	189-194
35	Ahmad Redho Rivai, Fatoni, Taqrim Ibadi	OPTIMASI KEAMANAN WEBSERVER RUMAH SAKIT UMUM DAERAH PALEMBANG BARI (rsudbari.palembang.go.id)	195-199
36	Adi Mandala Putra, Diana, Rahmat Novrianda	RANCANG BANGUN FILE STORAGE ONLINE MENGGUNAKAN VIRTUAL PRIVATE SERVER (VPS) PADA STIPER SRIWIGAMA PALEMBANG	200-204
37	Fitri Handayani, Baibul Tujni, Ari Muzakir	REKAYASA PERANGKAT LUNAK E-HEALTH DALAM PENGENALAN OBAT-OBATAN BERBASIS MOBILE DENGAN TEKNOLOGI CROSS PLATFORM	205-210
38	Wira Anggara, Zaniel Mazalisa, Ria Andryani	SISTEM INFORMASI PENDAFTARAN DAN PLACEMENT TEST BAHASA INGGRIS MAGENTA LANGUAGE ACADEMY BERBASIS WEB MOBILE	211-217
39	Ni Ketut Sukarni, Ilman Zuhri Yadi, R.M Nasrul Halim	PERANGKAT LUNAK PENENTUAN KONSENTRASI PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS ILMU KOMPUTER PADA UNIVERSITAS BINA DARMA BERBASIS ANDROID	218-223
40	Muhamad Aulladun Solihin, M. Akbar, Febriyanti Panjaitan.	PERANCANGAN SERVER VOIP MENGGUNAKAN TEKNOLOGI OPEN SOURCE PADA UNIVERSITAS BINA DARMA PALEMBANG	224-229



41	Eko Firnando , A. Haidar Mirza, Siti Sau'da	PENERAPAN METODE CLUSTERING DALAM ANALISIS DATA EVENT PARIWISATA TERHADAP KUNJUNGAN WISATA DI KOTA PALEMBANG	230-234
42	Renaldo Anugrah Pratama, Megawaty, Irman Effendy	PENERAPAN ALGORITMA <i>MERGE SORT</i> UNTUK PELATIHAN PSIKOTES CPNS BERBASIS ANDROID	235-240
43	Siti Yusmalinda, Wydyanto, Devi Udariansyah	IMPLEMENTASI ALGORITMA <i>DIJKSTRA</i> PADA PROTOKOL <i>ROUTING OPEN SHORTEST PATH FIRST</i> DENGAN MENGGUNAKAN SIMULASI GNS3	241-245
44	Polandri, Usman Ependi, Suryayusra	PENERAPAN SISTEM KEAMANAN <i>HONEYPOT</i> DAN <i>IPS</i> PADA JARINGAN NIRKABEL DI UNIVERSITAS BINA DARMA	246-251
45	Doni Mustafa <sup>1</sup> , Afriyudi <sup>2</sup> , Iin Seprina <sup>3</sup>	STUDI DAN IMPLEMENTASI KONSEP <i>BUSINESS TO CUSTOMER (B2C)</i> DENGAN TEKNOLOGI <i>M- COMMERCE</i> BERBASIS <i>HTML5</i> PADA EVERBEST PALEMBANG	252-258
46	Octa Tri Wahyudi, M. Izman Herdiansyah Eka Puji Agustini.	EVALUASI KUALITAS SISTEM INFORMASI SEKOLAH TINGGI ILMU KESEHATAN MITRA ADIGUNA PALEMBANG MENGGUNAKAN METODE <i>SERQUAL</i>	259-263

---

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

<sup>1</sup>Polandri, <sup>2</sup>Usman Ependi, <sup>3</sup>Suryayusra

<sup>1,2,3</sup> Universitas Bina Darma Palembang

<sup>1,2,3</sup> Jalan Jendral Ahmad Yani No.12 Palembang

<sup>1</sup>poalndri@gmail.com, <sup>2</sup>u.ependi@binadarma.ac.id, <sup>3</sup>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 interactionHoneyclient* yaitu *Honeyd* dan *Intrusion Prevention System* menggunakan *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 dibutuhkan 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

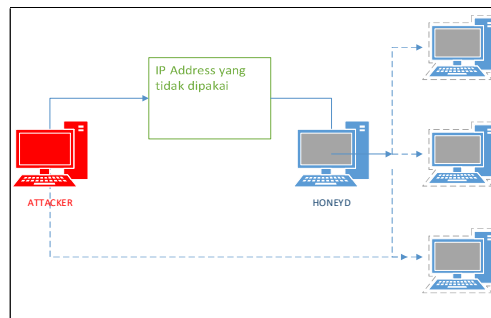
Merupakan sebuah aplikasi untuk mengimplementasikan RDBMS yang didistribusikan secara gratis. Pada penelitian ini MySql digunakan untuk menyimpan log lalu-lintas serangan pada *Honeyd*.

#### c. Apache 2

*Apache* adalah sebuah nama *web server* yang bertanggung jawab pada *request-response* HTTP dan *logging* informasi secara detail(kegunaan dasarnya). Digunakan sebagai *web server* untuk 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 dilakukan. Pada penelitian ini portsentry digunakan sebagai IPS dikarenakan kemampuannya dalam memblokir 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.

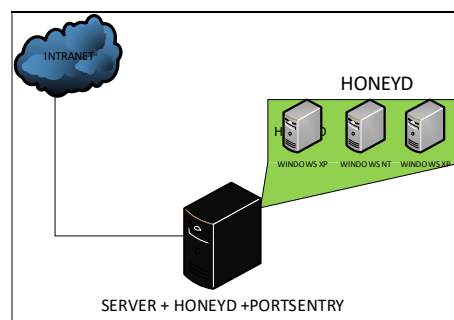
h. Nmap

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 instalisasi Ubuntu 15.04 lalu penulis melakukan instalisasi Honeyd dengan cara mendownload langsung dari repository dengan mengetikkan `apt-get install honeyd`. Lalu setelah instalisasi 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 negalamanan 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

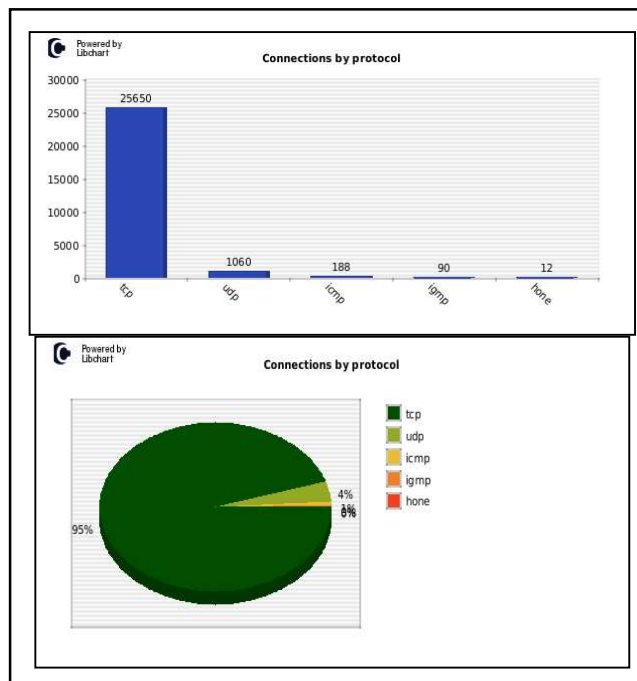
#### 2.5. Pembelajaran (*Learning*)

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 dilakukan pada protokol TCP, UDP, ICMP, IGMP, DAN HONE.



---

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 **attacker** adalah sebuah pesan peringatan.

#### 4. SIMPULAN

Berdasarkan pengujian dan Analisis yang telah dilakukan terhadap penelitian *Honeyd* dan *IPS* pada jaringan *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 pengujian yang dilakukan *Portsentry* akan langsung meblokir 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 antara *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 2011*
- 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 Honeyd*, 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 Computer Science Vivekanandha College of Arts and Sciences for Women, Namakkal, Tamil Nadu, India.
- Setiawan. D. (2010), *Intrusion Prevention System (IPS) dan Tantangan dalam pengembangannya., Sistem Komputer FASILKOM UNSRI*.
- Sofana I. (2012), *CISCO CCNA dan Jaringan Komputer*, Informatika
- Sofana I. (2012), *CISCO CCNP dan Jaringan Komputer*, Informatika