

Kode>Nama Rumpun Ilmu: 123/Ilmu Komputer

**LAPORAN AKHIR
PENELITIAN DOSEN PEMULA**



**Evaluasi Keamanan Sistem Informasi Pada Lembaga Pemerintahan Provinsi
Sumatera Selatan**

TIM PENGUSUL

Irwansyah, M.M., M.Kom NIDN : 0211117401

Timur Dali Purwanto, M.Kom. NIDN : 0203108505

**UNIVERSITAS BINA DARMA
November 2015**

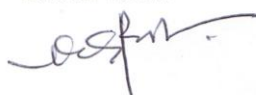
HALAMAN PENGESAHAN

Judul : Evaluasi Keamanan Sistem Informasi Pada Lembaga Pemerintahan Provinsi Sumatera Selatan

Peneliti/Pelaksana
Nama Lengkap : IRWANSYAH M.Kom.
Perguruan Tinggi : Universitas Bina Darma
NIDN : 0211117401
Jabatan Fungsional : Asisten Ahli
Program Studi : Teknik Komputer
Nomor HP : 081367531115
Alamat surel (e-mail) : irwansyah@mail.binadarma.ac.id

Anggota (1)
Nama Lengkap : TIMUR DALI PURWANTO M.Kom
NIDN : 0203108505
Perguruan Tinggi : Universitas Bina Darma
Institusi Mitra (jika ada) : -
Nama Institusi Mitra : -
Alamat : -
Penanggung Jawab : -
Tahun Pelaksanaan : Tahun ke 1 dari rencana 1 tahun
Biaya Tahun Berjalan : Rp 12.500.000,00
Biaya Keseluruhan : Rp 14.200.000,00

Mengetahui,
Direktur Vocasi



(Ir. Mahyudin, MT.)
NIP/NIK 150104424

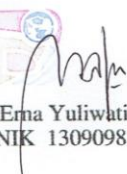
Palembang, 7 - 11 - 2015
Ketua,



(IRWANSYAH M.Kom.)
NIP/NIK 0400110210

Menyetujui,
Ketua Lembaga Penelitian

Universitas Bina Darma
LPPM



(Ir. Erna Yuliwati, MT., Ph.D)
NIP/NIK 13090987/0228076701

DAFTAR ISI

	Halaman
HALAMAN SAMPUL	i
HALAMAN PENGESAHAN	ii
DAFTAR ISI	iii
ABSTRAK	iv
BAB I. PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Perumusan Masalah	2
BAB II. TINJAUAN PUSTAKA	3
2.1 Vulnerability Assesment.....	3
2.2 Aspek – aspek Keamanan Sistem Informasi.....	5
2.3 Security Attack Models.....	6
2.4 Jenis – jenis Ancaman	7
2.5 Internet	8
2.6 Teknik – Teknik Attacking	9
BAB III. TUJUAN DAN MANFAAT PENELITIAN	11
3.1. Tempat Penelitian dan Objek Penelitian.....	11
3.2. Pengumpulan Data	11
3.3. Model Data	12
3.4. Rancangan Penelitian	13
BAB 1V METODE PENELITIAN	14
4.1. Anggaran Biaya.....	14
4.2. Jadwal Penelitian.....	15
BAB V HASIL YANG DICAPAI	14
BAB VI RENCANA TAHAPAN BERIKUTNYA	14
BAB VII KESIMPULAN DAN SARAN	14
DAFTAR PUSTAKA	15

LAMPIRAN	16
-----------------------	-----------

ABSTRAK

Perkembangan serta penggunaan teknologi informasi yang sangat cepat, maka semakin banyak pula aplikasi-aplikasi yang dibutuhkan oleh pengguna, seperti aplikasi di dunia perdagangan bebas secara elektronik (*electronic commerce*), pendidikan (*electronic education*), penyelenggaraan pemerintahan (*electronic government*), dan sebagainya. Keamanan data elektronik menjadi hal yang sangat penting di perusahaan seperti: perusahaan export-import, transportasi, lembaga pendidikan, pemberitaan, lembaga pemerintahan, hingga perbankan. Informasi atau data adalah aset bagi perusahaan ataupun lembaga pemerintahan. Tingkat ketergantungan organisasi ataupun perusahaan – perusahaan pada sistem informasi menimbulkan salah satu risiko adalah risiko keamanan informasi, dimana informasi menjadi suatu yang penting yang harus tetap tersedia dan dapat digunakan, serta terjaga keberadaannya dari pihak yang tidak berwenang. Dari permasalahan ini peneliti akan mengevaluasi keamanan sistem informasi di Lembaga Pemerintahan Provinsi Sumatera Selatan yaitu dari aspek *privacy* atau *Confidentiality*, *Integrity*, *Authentication*, serta *Availability*. Adapun tahapan evaluasi yang terdiri dari *Scanning Vulnerability Web*, penetrasi testing dan klasifikasi kerentanan sistem informasi. Pada penelitian ini menggunakan metode *Action Research* sebagai tahapan penelitian.

Kata Kunci: *Keamanan Sistem Informasi, Data Elektronik, Vulnerability*

BAB I

PENDAHULUAN

1.1 Latar Belakang

Sejalan dengan laju pertumbuhan penggunaan teknologi informasi yang sangat cepat, maka semakin banyak pula aplikasi-aplikasi yang dibutuhkan oleh pengguna, seperti pada aplikasi di dunia perdagangan bebas secara elektronik (*electronic commerce*), pendidikan (*electronic education*), penyelenggaraan pemerintahan (*electronic government*), dan sebagainya. Keamanan data elektronik menjadi hal yang sangat penting di perusahaan penyedia jasa teknologi informasi (TI) maupun industri lainnya, seperti: perusahaan export-import, transportasi, lembaga pendidikan, pemberitaan, lembaga pemerintahan, hingga perbankan yang menggunakan fasilitas TI dan menempatkannya sebagai infrastruktur kritikal (penting). Informasi atau data adalah aset bagi perusahaan ataupun lembaga pemerintahan.

Pada Lembaga Pemerintahan Provinsi Sumatera Selatan sekarang ini hampir semua aktifitas pekerjaan sudah menggunakan sistim informasi sebagai alat bantu pekerjaan. Tingkat ketergantungan organisasi ataupun perusahaan – perusahaan pada sistem informasi menimbulkan salah satu risiko adalah risiko keamanan informasi, dimana informasi menjadi suatu yang penting yang harus tetap tersedia dan dapat digunakan, serta terjaga keberadaannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau tereksposnya data ke pihak eksternal yang tidak diinginkan.

Berdasarkan hasil riset dan survey serta berbagai laporan tentang kejahatan komputer yang terjadi sejauh ini, diketahui bahwa tidak ada satu pun sistem informasi yang diasumsikan 100 persen aman dari serangan virus komputer, *spam*, *e-mail bomb*, atau diterobos langsung oleh para *hackers*. Sangat sulit mencari angka yang pasti tentang peristiwa kejahatan seperti ini karena banyak menyangkut publikasi negatif pada suatu keamanan sistem informasi.

Pada penelitian ini, peneliti akan mengevaluasi keamanan sistem informasi yang ada pada lembaga pemerintahan di Provinsi Sumatera Selatan sebagai pengguna sistem informasi. Evaluasi keamanan sistem informasi yang akan dianalisis yaitu dari aspek *privacy*, dimana

data – data yang bersifat privat dari orang yang tidak berhak mengakses, misalnya user atau password seseorang. Kemudian dari aspek *Integrity*, *Authentication* dan *Availability*.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, maka perumusan masalah yang akan dikaji dalam penelitian ini adalah “bagaimana mengevaluasi keamanan sistem informasi pada lembaga pemerintahan di Provinsi Sumatera Selatan”.

BAB II

TINJAUAN PUSTAKA

2.1 *Vulnerability Assessment*

Vulnerability atau celah keamanan adalah suatu kelemahan yang mengancam nilai *integrity*, *confidentiality* dan *availability* dari suatu aset. *Vulnerability* tidak hanya berupa *software bugs* atau kelemahan *security* jaringan. Namun kelemahan seperti pegawai yang tidak ditraining, dokumentasi yang tidak tersedia maupun prosedur yang tidak dijalankan dengan benar. *Vulnerability* biasa dikategorikan ke dalam tiga bagian, yaitu kelemahan pada *system* itu sendiri, jalur akses menuju kelemahan sistem, serta kemampuan dari seorang hacker untuk melakukan *attacking*. (Hanif Santoso, dkk, 2008:2)

Pengukuran atau *assessment* adalah hal yang mutlak dilakukan untuk mendapatkan peningkatan kualitas. Suatu perusahaan dapat meningkatkan penjualannya bila mengetahui bagaimana efisiensinya. Dengan adanya pengukuran maka perusahaan dapat mengetahui kelemahan yang ada, membandingkannya dengan contoh penerapan di perusahaan lain dan ujungnya adalah peningkatan keuntungan perusahaan. (Anjar Priandoyo, 2006).

Vulnerability Assessment (VA) adalah analisa keamanan yang menyeluruh serta mendalam terhadap berbagai dokumen terkait keamanan informasi, hasil scanning jaringan, konfigurasi pada sistem, cara pengelolaan, kesadaran keamanan orang-orang yang terlibat dan keamanan fisik, untuk mengetahui seluruh potensi kelemahan kritis yang ada. *Vulnerability Assessment (VA)* bukan sekedar melakukan *scanning* dari jaringan menggunakan *Vulnerability Assessment tool*. Hasil *Vulnerability Assessment (VA)* jauh berbeda dengan pentest *blackbox* dan *greybox*. Kedua jenis pentest ini tidak mampu memberikan hasil yang komprehensif karena tidak seluruh potensi kerentanan kritis akan teridentifikasi. Bahkan ditemukan dalam banyak kasus, hasil pentest *blackbox* melaporkan tidak adanya kelemahan kritis, namun saat dilakukan *Vulnerability Assessment (VA)* terdapat beberapa kelemahan kritis (Lumy.2010).

Kelemahan pada website atau aplikasi berbasis web dapat dikategorikan menjadi 4 tingkatan, yaitu:

1. Sangat Tinggi : pada level ini terdapat kelemahan yang berpotensi tinggi menjadi ancaman sedangkan fitur ataupun langkah untuk tingkat pencegahan maupun penanganannya tidak memadai.
2. Tinggi : pada level ini *scoop* kelemahan lebih kecil dibandingkan level sebelumnya. Bersifat lokal. Namun, upaya pencegahan dan penanganan masih tidak memadai.
3. Sedang : pada level ini tingkatan kelemahan bersifat lokal dan upaya penanganan dan pencegahan pun bersifat lokal.
4. Rendah : tingkat kelemahan rendah dan upaya pencegahan dan penanganan yang diharapkan pun sangat memadai.

Kegiatan *Vulnerability Assessment* ini sangat dianjurkan untuk dilakukan secara rutin. Bisa dilakukan per minggu atau perbulan. Hal ini dikarenakan trend ancaman atau serangan selalu berkembang. Mulailah sedini mungkin untuk *aware* melakukan hal-hal kecil yang bisa menjaga keamanan sistem informasi kita karena satu hal yang pasti adalah tidak ada satupun yang aman di dunia maya. (GOV-CSIRT, 2012).

2.2 Aspek – aspek Keamanan Sistem Informasi.

Menurut dari Simson Garfinkel "*PGP : Pretty Good Privacy*", O'Reilly & Associates, Inc, 1995 bahwa Aspek – aspek keamanan komputer dapat dibedakan menjadi, antara lain :

- Privacy / Confidentiality

Yaitu menjaga informasi dari orang yang tidak berhak mengakses, yang dimana lebih ke arah data-data yang bersifat privat, contohnya : Email seorang pemakai (user) tidak boleh dibaca oleh administrator. Sedangkan Confidentiality berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contohnya : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya. Adapun bentuk serangan dalam bentuk usaha penyadapan (dengan program Sniffer), sedangkan usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

- Integrity

Yaitu informasi tidak boleh diubah tanpa seijin pemilik informasi. Contohnya : E-mail di Intercept ditengah jalan, diubah isinya, kemudian diteruskan kealamat yang dituju. Adapun bentuk serangan yang dilakukan adanya virus, trojan horse atau pemakai lain yang mengubah informasi tanpa ijin, "Man in the middle attack" dimana seseorang menempatkan diri ditengah pembicaraan dan menyamar sebagai orang lain.

- Authentication

Yaitu metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Dapat menggunakan dukungan tools yang membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking (untuk menjaga "Intellectual Property" yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature. Acces Control, yaitu

berkaitan dengan pembatasan orang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang) dan sejenisnya.

- Availability

Yaitu berhubungan dengan ketersediaan informasi ketika dibutuhkan. Adapun ancaman yang dapat terjadi meliputi : Denial Of Service Attack (DoS Attack) dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.

2.3 Security Attack Models

Menurut W. Stallings [William Stallings, “*Network and Internetwork Security*,” Prentice Hall, 1995.] serangan (*attack*) terdiri dari :

1. Interruption

Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “denial of service attack”.

2. Interception

Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).

3. Modification

Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan - pesan yang merugikan pemilik web site.

2.4 Jenis-jenis Ancaman

1. DOS/DDOS

Denial of Services dan *Distributed Denial of Services* adalah sebuah metode serangan yang bertujuan untuk menghabiskan sumber-daya sebuah peralatan jaringan komputer, sehingga layanan jaringan komputer menjadi terganggu.

2. *Packet Sniffing*

Packet Sniffing adalah sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.

3. *IP Spoofing*

IP Spoofing dilakukan dengan cara merubah alamat asal sebuah paket, sehingga dapat melewati perlindungan *firewall*.

4. *Forgery*

Salah satu cara yang dapat dilakukan oleh seseorang untuk mencuri data-data penting orang lain adalah dengan cara melakukan penipuan. Salah satu bentuk penipuan yang bisa dilakukan adalah dengan cara membuat sebuah *website* tiruan (misalkan meniru klikbca.com), lalu memancing pihak yang ingin ditipu untuk meng-akses *website* palsu tersebut. Setelah kita memiliki data-data yang diperlukan, kita dapat melakukan akses ke *website* yang asli sebagai pihak yang kita tipu.

2.5. Internet

Internet merupakan kepanjangan dari *Interconnection Networking*. Menurut Jill. H. Ellsworth dan Matthew. V. Ellsworth :

“Internet is : large interconnected network of network computer linking people and computer all over the world, via phone line, satellites and other telecommunication systems”.

Pengertiannya adalah internet adalah jaringan besar yang saling berhubungan dari jaringan-jaringan komputer yang menghubungkan orang-orang dan komputerkomputer

diseluruh dunia, melalui telepon, satelit dan sistem-sistem komunikasi yang lain. Internet dibentuk oleh jutaan komputer yang terhubung bersama dari seluruh dunia, memberi jalan bagi informasi untuk dapat dikirim dan dinikmati bersama. Untuk dapat bertukar informasi, digunakan protocol standar yaitu *Transmission Control Protocol* dan *internet Protocol* yang lebih dikenal sebagai *TCP/IP*.

2.6 Teknik-Teknik Attacking

Terdapat banyak sekali tipe dan jenis serangan yang terjadi di dunia maya. Sesuai dengan sifat dan karakteristiknya, semakin lama model serangan yang ada semakin kompleks dan sulit dideteksi maupun dicegah. Berikut adalah beberapa jenis model serangan yang kerap terjadi. (Richardus:1,_).

1. SQL Injection

Pada dasarnya *SQL Injection* merupakan cara mengeksploitasi celah keamanan yang muncul pada level atau “layer” *database* dan aplikasinya. Celah keamanan tersebut ditunjukkan pada saat penyerang memasukkan nilai “*string*” dan karakter-karakter contoh lainnya yang ada dalam instruksi *SQL*; dimana perintah tersebut hanya diketahui oleh sejumlah kecil individu (baca: *hacker* maupun *cracker*) yang berusaha untuk mengeksploitasinya. Karena tipe data yang dimasukkan tidak sama dengan yang seharusnya (sesuai dengan kehendak *program*), maka terjadi sebuah aktivitas “liar” yang tidak terduga sebelumnya - dimana biasanya dapat mengakibatkan mereka yang tidak berhak masuk ke dalam sistem yang telah terproteksi menjadi memiliki hak akses dengan mudahnya. Dikatakan sebagai sebuah “injeksi” karena aktivitas penyerangan dilakukan dengan cara “memasukkan” *string* (kumpulan karakter) khusus untuk melewati filter logika hak akses pada *website* atau sistem komputer yang dimaksud.

Contoh-contoh celah kerawanan yang kerap menjadi korban *SQL Injection* adalah:

- a. Karakter-karakter kendali, kontrol, atau *filter* tidak didefinisikan dengan baik dan benar (baca: *Incorrectly Filtered Escape Characters*);
- b. Tipe pemilihan dan penanganan *variabel* maupun parameter program yang keliru (baca: *Incorrect Type Handling*);
- c. Celah keamanan berada dalam server basis datanya (baca: *Vulnerabilities Inside the Database Server*);
- d. Dilakukan mekanisme penyamaran SQL Injection (baca: *Blind SQL Injection*); dan lain sebagainya.

2. XSS (Cross Site Scripting)

Cross Site Scripting (CSS) adalah suatu serangan dengan menggunakan mekanisme “*injection*” pada aplikasi web dengan memanfaatkan metode *HTTP GET* atau *HTTP POST*. *Cross Site Scripting* biasa digunakan oleh pihak-pihak yang berniat tidak baik dalam upaya mengacaukan konten website dengan memasukkan naskah program (biasanya *java script*) sebagai bagian dari teks masukan melalui formulir yang tersedia.

3. Missing Function Level Access Control

Hampir semua aplikasi *web* memverifikasi fungsi tingkat hak akses sebelum membuat fungsi yang terlihat di UI. Namun, aplikasi perlu ditampilkan untuk memeriksa kontrol akses yang sama pada *server* ketika setiap fungsi diakses. Jika permintaan tidak diverifikasi, penyerang akan dapat melakukan permintaan mengakses fungsi yang tidak sah.

4. Brute Force Attack

Serangan *brute-force* adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah

integer, dengan menggunakan teknik serangan brute force, penggunaanya hanya dituntut untuk membuat program yang mencoba semua nilai *integer* yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: "When in doubt, use brute-force" (jika ragu, gunakan brute-force).

BAB III

TUJUAN DAN MANFAAT PENELITIAN

3.1 Tujuan Penelitian

Tujuan dari penelitian ini adalah untuk mengetahui sejauh mana keamanan sistem informasi yang digunakan atau diterapkan pada lembaga pemerintahan yaitu Pemrov Sumsel, yang ditinjau dari aspek keamanan sistem informasi, yaitu : Aspek *Privacy* atau *Confidentiality*, *Integrity*, *Autentication*, serta *Avaibility*".

3.2 Manfaat Penelitian

Adapun manfaat dari penelitian keamanan system informasi pada lembaga pemerintahan Sumatera Selatan ini antara lain: dapat dijadikan sebagai bahan informasi dan kajian ulang dalam mengelola, memperbaiki serta mengembangkan Keamanan Sistem Informasi yang digunakan di semua lembaga pemerintahan khususnya Pemrov Sumel. Sehingga terbebas atau aman dari ancaman dan gangguan dari penyusup yang berasal dari internal dan external sistem.

BAB IV

METODE PENELITIAN

4.1 Tempat Penelitian dan Objek Penelitian

Penelitian ini dilaksanakan pada beberapa lembaga pemerintahan di Provinsi Sumatera Selatan, yang menggunakan layanan sistem informasi komputer.

4.2 Pengumpulan Data

Untuk memperoleh data yang digunakan dalam penyusunan penelitian ini maka dilakukan pengambilan data secara primer dan sekunder, yaitu :

a. Data *Primer*

Yaitu data yang dikumpulkan secara langsung dari objek yang diteliti berupa data mengenai Sistem Informasi yang telah digunakan oleh Lembaga Pemerintahan provinsi Sumatera Selatan.

Cara – cara yang dipakai untuk mengumpulkan data tersebut yaitu :

1. *Observasi*

Penulis mengadakan pengamatan langsung pada lembaga pemerintahan di Provinsi Sumatera Selatan, dengan melihat langsung bagaimana penggunaan dan penerapan Sistem Informasi Komputer.

2. *Wawancara*

Mengadakan tanya jawab atau berdialog secara langsung dengan pegawai pada lembaga Pemerintahan tersebut sebagai pengguna sistem informasi, yang berisikan pertanyaan yang berhubungan dengan keamanan sistem informasi yang ada pada lembaga tersebut.

b. Data *Sekunder*

Yaitu pengumpulan data dengan mempelajari masalah yang berhubungan dengan objek yang diteliti serta buku yang dipelajari, yang terdiri dari :

1. *Studi Pustaka*

Penulis menggunakan pengetahuan yang didapat dari buku – buku, *literature* di perpustakaan, jurnal ilmiah dan internet yang erat kaitanya dengan penelitian yang dilakukan.

2. *Dokumentasi*

Penulis mengambil data-data yang diperlukan pada Lembaga Penelitian dan Pengabdian Masyarakat Universitas Bina Darma.

4.2.1. Data Sekunder

Data sekunder diperoleh penulis dengan melakukan studi kepustakaan (*literature*) yaitu dengan mencari bahan dari *internet*, jurnal dan perpustakaan serta buku yang sesuai dengan objek yang akan diteliti.

4.2.2 Rancangan Penelitian

Tabel 4.1 Rancangan Penelitian

Perihal	Deskripsi
Topik	Analisis dan mengidentifikasi kerentanan terhadap <i>Portal Website, Monitoring dan Reporting</i> SPSE LPSE pada Sistem Informasi Penataan Ruang (SIPR) di Sumatera Selatan khususnya pada Kota Lubuklinggau yang disetujui yang mempunyai <i>sub domain</i> http://reportspse.lubuklinggaukota.net dan http://sipr.lubuklinggaukota.go.id .
Masalah	Bagaimana mengidentifikasi kerentanan terhadap <i>sub domain Portal Website</i> Kota Lubuklinggau.
Metode Yang Digunakan	Action Research (Penelitian Tindakan)
Tipe dan Desain Penelitian	
• Tipe penelitian	<i>Field Research</i>
• Desain penelitian	Field Research yaitu melakukan penelitian ke lapangan dengan mendatangi langsung objek yang akan diteliti. <i>Adapun tahapan penelitian</i> yang merupakan siklus dari <i>field research</i> ini, yaitu : 1. Melakukan diagnosa (<i>Diagnosing</i>) Dalam melakukan diagnosa kebutuhan perangkat yang

diperlukan dalam mengidentifikasi kerentanan (*Vulnerability*) pada *sub domain Portal Website* Kota Lubuklinggau.

2. Membuat rencana tindakan (***Action Planning***)

Kemudian merencanakan tindakan yang akan dilakukan untuk mengidentifikasi kerentanan pada *sub domain Portal Website* Kota Lubuklinggau. Dengan pengambilan data awal berupa *Information Gathering* serta *scanning vulnerability tools* pada *sub domain Portal Website* Kota Lubuklinggau.

3. Melakukan tindakan (***Action Taking***)

Mengimplementasikan rencana tindakan berdasarkan rencana yang telah di susun. Pada tahap awal melakukan *Information Gathring*, mengumpulkan informasi tentang celah kerentanan *sub domain Portal Web* Kota Lubuklinggau dan melakukan scanning vulnerability tools misalnya menggunakan : Whatweb, Vega, OWASP-ZAP, W3AF, Acunetix dan Nikto. Secara garis besar *scanning tools* melakukan pencarian celah *Vulnerability* dari target serta mengatur mode serangan, membongkar url yang ada pada *website*, menemukan *error*, *cookies* dan *email* pada *website* serta menemukan jejak admin.

4. Melakukan evaluasi (***Evaluating***)

Setelah dilakukan implementasi (***action taking***) selanjutnya melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai mengevaluasi hasil dari langkah sebelumnya.

5. Pembelajaran (***Learning***)

	<p>langkah ini merupakan tahap akhir yaitu melakukan <i>review</i> dan menjalankan prosedur terakhir yaitu <i>Documentation</i> dan <i>Reporting</i>, terhadap hasil dari tahapan-tahapan yang telah dilalui.</p>
<p>Perencanaan Penelitian</p> <ul style="list-style-type: none"> • Subjek • Peralatan • Prosedur • Teknik Analisis 	<p>WEB SITE Portal dan sub domain Badan Perencanaan Pembangunan Daerah (BAPPEDA) dan Layanan Pengadaan Secara Elektronik (LPSE) Kota Lubuklinggau</p> <p>.</p> <p>Peralatan pengujian yaitu berupa Whatweb, Vega, OWASP-ZAP, W3AF, Acunetix dan Nikto</p> <p>Tahapan awal adalah melakukan pengumpulan informasi atau <i>Information Gathering</i> sebagai data awal untuk menentukan tindakan lebih lanjut, melakukan evaluasi dengan cara melihat jenis kerentanan yang terdapat pada <i>portal website Monitoring</i> dan <i>Reporting</i> SPSE LPSE dan Sistem Informasi Penataan Ruang, kemudian melakukan penutupan terhadap celah kerentanan yang di temukan.</p> <p>Dengan menerapkan Metode penutupan celah kerentanan dengan cara <i>patching bugs</i>, atau memperbaiki kesalahan pada <i>coding script</i> dan hak akses. Rekomendasi perbaikan akan diberikan pada <i>portal website Monitoring</i> dan <i>Reporting</i> SPSE LPSE dan Sistem Informasi Penataan Ruang seperti <i>script</i> yang benar, rekomendasi jenis <i>password</i> dan jenis <i>enkripsi</i> yang baik, mengatur ekstensi file pada fasilitas <i>upload</i>/menghapus fasilitas <i>upload</i> yang rentan.</p>

4.5 Metode analisis data

Data-data yang telah terkumpul selanjutnya di analisis dengan menggunakan metode kualitatif. Menurut Dwiyanto (2006) metode kualitatif adalah tata cara pengumpulan data yang lazim yaitu melalui studi pustaka dan studi lapangan, dilanjutkan oleh rahayu (2000) laporan hasil penelitian kualitatif selalu panjang lebar, karena memang tujuan penelitian kualitatif adalah menghayati dan membuat orang lain memahami masalah yang diteliti.

Data penelitian studi pustaka dan studi lapangan didapatkan dengan memfokuskan pengumpulan data atau *Information Gathering* dan analisis *vulnerability* serta *action planning* yang merupakan rangkaian dari tindakan yang telah dan akan dilakukan pada web *Monitoring* dan *Reporting* SPSE LPSE pada Sistem Informasi Penataan Ruang (SIPR) di Sumatera Selatan khususnya pada Kota Lubuklinggau yang mempunyai *sub domain* <http://reportspse.lubuklinggaukota.net> dan <http://sipr.lubuklinggaukota.go.id>, dengan membatasi tiga jenis *vulnerability* yaitu, *Cross-Site Scripting*, *ClearText Password Over HTTP*, *SQL Injection*. Maka pada tahap ini peneliti akan mencoba melakukan eksploitasi terhadap *vulnerability* tersebut.

4.6 Alat Analisis

Menurut Rahadi (2010), Tujuan pokok suatu penelitian adalah untuk menjawab pertanyaan dan hipotesis. Untuk itu peneliti merumuskan hipotesis, mengumpulkan data, memproses data, membuat analisis dan interpretasi. Analisis data belum dapat menjawab pertanyaan penelitian. Setelah data dianalisis dan diperoleh informasi yang lebih sederhana, hasil analisis tersebut harus diinterpretasi untuk mencari makna dan implikasi dari hasil analisis tersebut.

Analisa data adalah mengelompokkan, membuat suatu urutan, memanipulasi serta menyingkatkan data sehingga mudah untuk dibaca. Step pertama dalam analisa adalah membagi data atas kelompok atau kategori-kategori, kategori tidak lain dari bagian-bagian. Alat analisis data yang di gunakan dalam penelitian ini melakukan eksploitasi terhadap *vulnerability* dengan menggunakan *tools* berikut ini:

1. *XSSER tools* berfungsi untuk melakukan *inject script* melalui *Cross-Site Scripting vulnerability*.
2. *SQLmap* merupakan *tools* penetrasi yang berfungsi melakukan otomatisasi proses deteksi dan eksploitasi kelemahan *SQL Injection* serta memungkinkan untuk mengambil alih *database server*.

3. *Nmap* yang berfungsi untuk melakukan *scanning port* serta mencari tahu mengenai potensial *method* yang bisa digunakan untuk melakukan eksploitasi
4. *RESTclient* berfungsi untuk memastikan *HTTP Request* yang aktif pada *website* target.
5. *Armitage* berfungsi untuk mendeteksi *vulnerability* dan melakukan eksploitasi secara otomatis melalui *vulnerability* yang telah terdeteksi.
6. *Hydra tools* berfungsi untuk mendeteksi *password* yang *match* untuk administrator *website*.
7. *Burp Suite* merupakan *tools* pengujian keamanan aplikasi *web* yang bekerja secara keseluruhan, dari pemetaan awal untuk menemukan dan mengeksploitasi kerentanan keamanan.

4.7 Alat dan Bahan

Alat dan bahan penelitian yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Peralatan Penelitian

Satu unit Laptop dengan spesifikasi :

- a. *Processor Intel® Dual-Core CPU T4200 @ 2.00 GHz*
- b. *RAM 3 GB*
- c. *Hardisk 250 GB*
- d. *Wi-Fi Broadcom 802.11 b/g Wlan NIDS 5.1*
- e. *Access Point 802.11 G yang menggunakan DDWRT*
- f. *Printer Brother BJC210*

2. Bahan Penelitian

- a. *Data hasil information gathering.*
- b. *Data hasil eksploitasi.*
- c. *Data hasil vulnerability.*

BAB V

HASIL YANG DICAPAI

5.1. Survei Action Objek

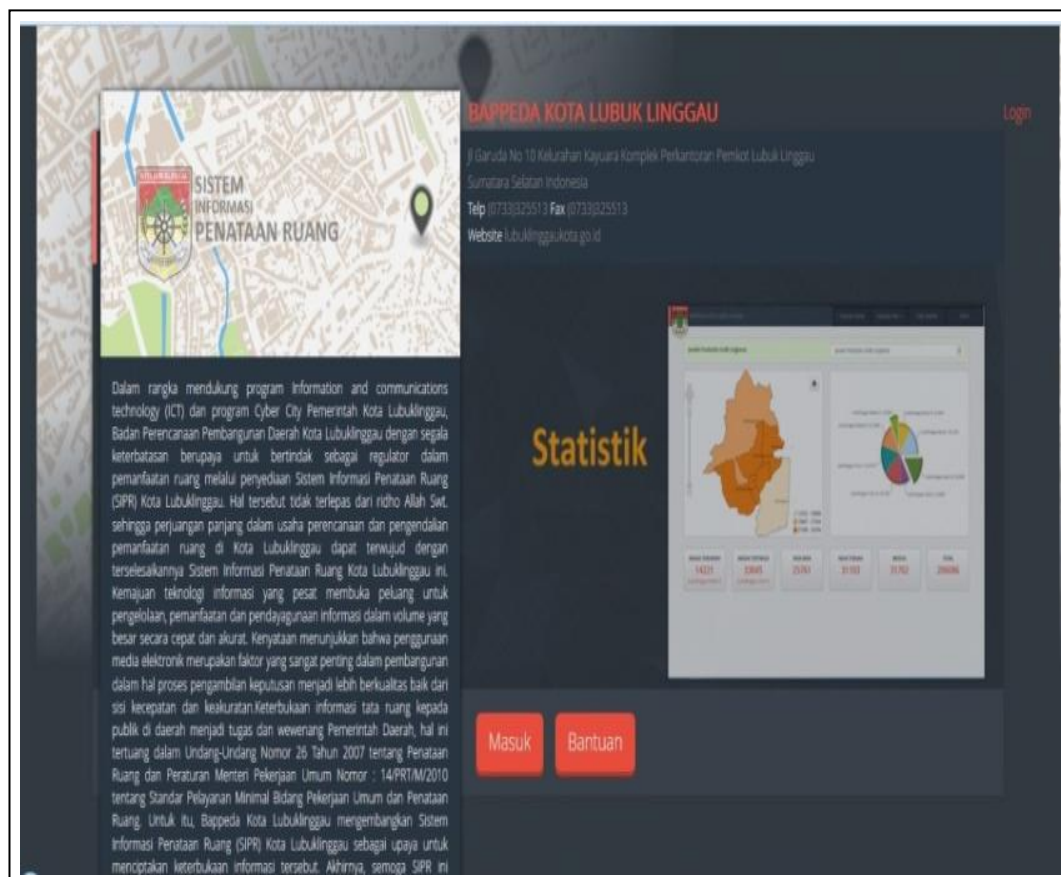
Pada tahapan ini survey dilakukan secara random semua kabupaten di Sumatera Selatan jatuh pada objek tempat yaitu BAPPEDA dan Layanan Pengadaan Secara Elektronik (LPSE) Kota Lubuk Linggau.

5.2. Hasil Diagnosa

Untuk menghasilkan *diagnosing* yang meliputi *information gathering* dan scanning yang dilakukan pada tahap awal ini, peneliti menetapkan tiga jenis tool untuk *vulnerability* yaitu, *Whois Domain Tools*, *Builtwith Tools* dan *Nmap Tools* Maka pada tahap ini peneliti akan mencoba melakukan *information gathering* (pengumpulan informasi) terhadap *website* target dan analisa *vulnerability* tersebut sebagai berikut:

5.2.1. Website Sistem Informasi Penataan Ruang Kota Lubuklinggau

Website <http://sipr.lubuklinggaukota.go.id> dengan *interface* yang dapat dilihat pada **Gambar 5.1** di bawah ini.



Gambar 5.1 Website Sistem Informasi Penataan Ruang

5.2.1.1. Information Gathering Menggunakan Whois Domain Tools

Whois domain tools merupakan tools yang digunakan secara online dengan cara menginputkan `http://sipr.lubuklinggaukota.go.id` pada *dialog search* yang tersedia pada tools tersebut. Maka didapatlah informasi seperti pada **Gambar 5.2** berikut ini.

Whois & Quick Stats	
Email	neknang@gmail.com
Dates	Created on 2013-03-14 - Expires on 2015-03-14 - Updated on 2015-01-14
IP Address	116.213.48.66 - 113 other sites hosted on this server
IP Location	- Jakarta Raya - Jakarta - Rumahweb
ASN	AS58487 RUMAHWEB-AS-ID Rumahweb Indonesia CV. (registered Dec 21, 2011)
Whois History	13 records have been archived since 2013-04-03
Whois Server	whois.pandi.or.id
Website	
Website Title	Website Title
Server Type	Apache/2.2.29 (Unix) mod_ssl/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/1.4 mod_fcgid/2.3.9
Response Code	200
SEO Score	51%

Gambar 5.2 Informasi yang didapat setelah menggunakan *Whois Domain Tools*

5.2.1.2. Information Gathering Menggunakan Builtwith Tools

Builtwith Tools merupakan tools yang digunakan secara online dengan cara menginputkan `http://sipr.lubuklinggaukota.go.id` pada *dialog search* yang tersedia pada tools tersebut. Maka didapatlah informasi seperti pada **Gambar 5.3** di bawah ini..

SIPR.LUBUKLINGGAUKOTA.GO.ID

Technology Profile

Web Server

[View Global Trends](#)

Apache

[Apache Usage Statistics - Websites using Apache](#)

Apache has been the most popular web server on the Internet since April 1996.

Apache 2.2

[Apache 2.2 Usage Statistics - Websites using Apache 2.2](#)

Frameworks

[View Global Trends](#)

CodeIgniter

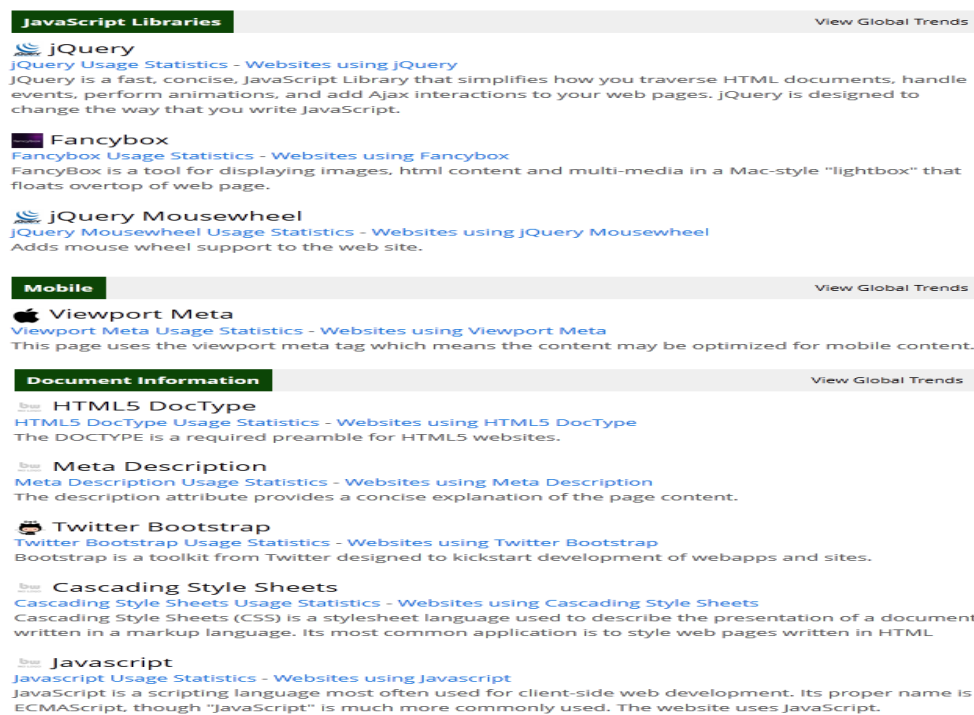
[CodeIgniter Usage Statistics - Websites using CodeIgniter](#)

CodeIgniter is a powerful PHP framework with a very small footprint.

PHP

[PHP Usage Statistics - Websites using PHP](#)

PHP is a widely-used general-purpose scripting language that is especially suited for Web development and can be embedded into HTML.



Gambar 5.3 Informasi yang didapat setelah menggunakan *Builtwith Tools*

5.2.1.3. Information Gathering Menggunakan Nmap Tools

Nmap digunakan untuk melakukan analisis atau penguraian untuk mengetahui *port* apa saja yang terbuka pada website yang telah menjadi target, hasil dari *Nmap tools* dapat dilihat pada **Gambar 5.4** di bawah ini.

```

root@ins:~# nmap 121.100.29.14
Starting Nmap 6.25 ( http://nmap.org ) at 2015-02-07 07:47 WIT
Nmap scan report for 121.100.29.14
Host is up (0.14s latency).
Not shown: 974 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
53/tcp    open  domain
80/tcp    open  http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
443/tcp   open  https
445/tcp   filtered microsoft-ds
465/tcp   filtered smtps
593/tcp   filtered http-rpc-epmap
1024/tcp  filtered kdm
1025/tcp  filtered NFS-or-IIS
1026/tcp  filtered LSA-or-nterm
1027/tcp  filtered IIS
1028/tcp  filtered unknown
1029/tcp  filtered ms-lsa
1030/tcp  filtered iadl
1080/tcp  filtered socks
1433/tcp  filtered ms-sql-s
1434/tcp  filtered ms-sql-m
3128/tcp  filtered squid-http
4444/tcp  filtered krb524
5432/tcp  open  postgresql
8080/tcp  open  http-proxy
9898/tcp  filtered monkeycom
12345/tcp filtered netbus
Nmap done: 1 IP address (1 host up) scanned in 36.12 seconds

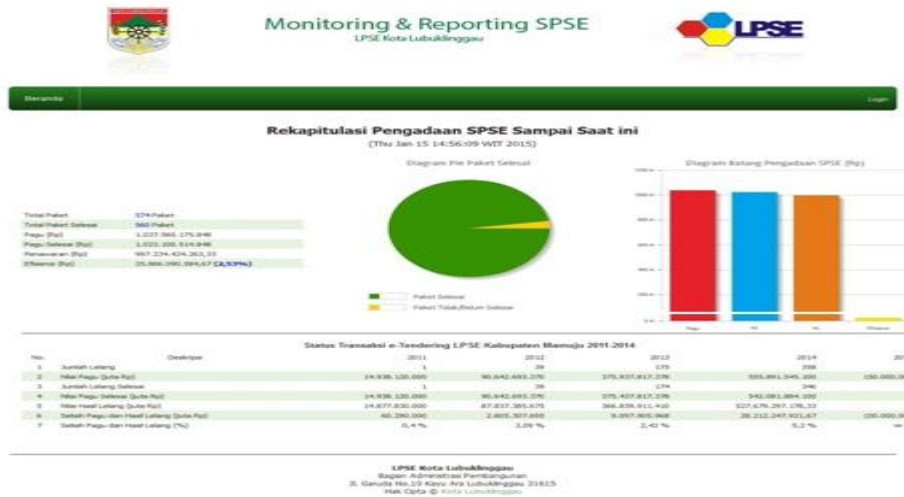
```

Gambar 5.4 Informasi yang didapat setelah Nmap Tools

Dari gambar di atas maka didapatkan informasi mengenai port yang terbuka pada website report.lpse.lubuklinggaukota.net.

5.2.2. Website Monitoring & Reporting SPSE LPSE Kota Lubuklinggau.

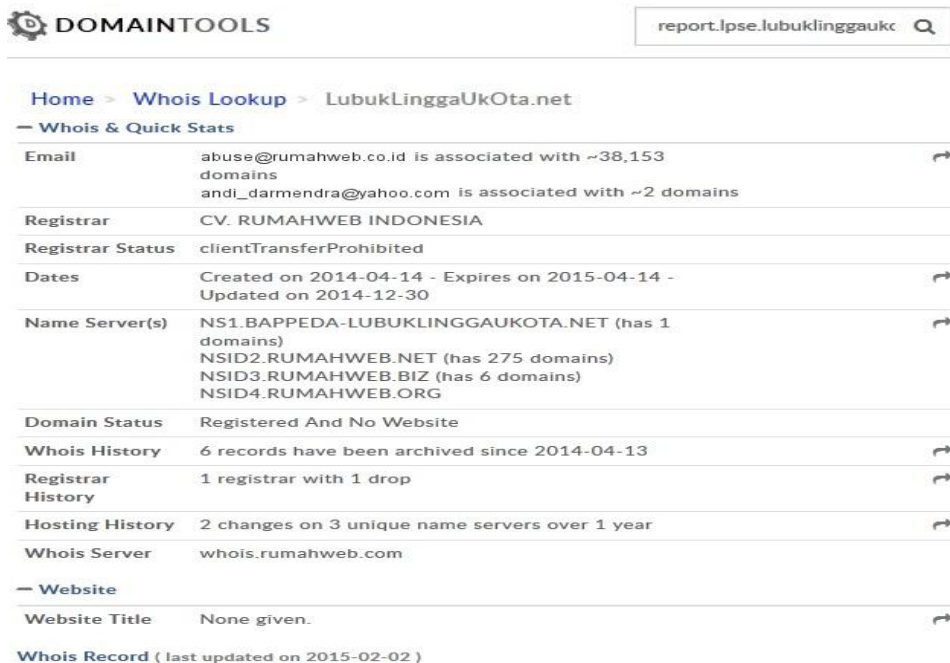
website <http://report.lpse.lubuklinggaukota.go.id> dengan interface yang dapat dilihat pada Gambar 5.5 berikut:



Gambar 5.5 Interface Website Monitoring & Reporting SPSE LPSE Kota Lubuklinggau

5.2.2.1. Information Gathering Menggunakan Whois Domain Tools

Whois domain tools merupakan tools yang digunakan secara online dengan cara menginputkan <http://report.lpse.lubuklinggaukota.net> pada dialog search yang tersedia pada tools tersebut. Maka didapatkan informasi seperti pada Gambar 5.6 di bawah ini.



```
Domain Name: LUBUKLINGGAUKOTA.NET
Registry Domain ID:
Registrar WHOIS Server: whois.rumahweb.com
Registrar URL: https://www.rumahweb.com
Creation Date: 2015-04-14T01:54:55+07:00
Registrar Registration Expiration Date: 2015-04-14T01:54:55+07:00
Registrar: CV. Rumahweb Indonesia
Registrar IANA ID: 1675
Registrar Abuse Contact Email: abuse@rumahweb.co.id
Registrar Abuse Contact Phone: +62.274882257
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: Hadi Sanjaya
Registrant Organization: appedaotaubuklinggau
Registrant Street: Jl. Garuda No. 10 Kelurahan Kayuara
Registrant City: Lubuklinggau
Registrant State/Province: Sumatera Selatan
Registrant Postal Code: 31616
Registrant Country: ID
Registrant Phone: +62.000000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: andi_darmendra@yahoo.com
Registry Admin ID:
```

Gambar 5.6 Informasi yang didapat setelah menggunakan Whois Domain

5.2.2.2. Information Gathering Menggunakan Builtwith Tools.

Builtwith Tools merupakan tools yang digunakan secara online dengan cara menginputkan http://report.lpse.lubuklinggaukota.net pada dialog search yang tersedia pada tools tersebut. Maka didapatkanlah informasi seperti pada Gambar 5.7 berikut:

Gambar 5.7 Informasi yang didapat setelah menggunakan *Builtwith Tools*

5.2.2.3. Information Gathering Menggunakan Nmap Tools

Nmap digunakan untuk melakukan analisis atau penguraian untuk mengetahui *port* apa saja yang terbuka pada website yang telah menjadi target, hasil dari *Nmap tools* dapat dilihat pada **Gambar 5.8** berikut.

```
root@Ins:~# nmap 121.100.28.196

Starting Nmap 6.25 ( http://nmap.org ) at 2015-02-07 08:06 WIT
Nmap scan report for 121.100.28.196
Host is up (0.18s latency).
Not shown: 965 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    filtered smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open  imap
443/tcp   open  https
445/tcp   filtered microsoft-ds
465/tcp   filtered smtps
593/tcp   filtered http-rpc-epmap
631/tcp   open  ipp
666/tcp   filtered doom
993/tcp   open  imaps
995/tcp   open  pop3s
1024/tcp  filtered kdm
1025/tcp  filtered NFS-or-IIS
1026/tcp  filtered LSA-or-nterm
1027/tcp  filtered IIS
1028/tcp  filtered unknown
1029/tcp  filtered ms-lsa
1030/tcp  filtered iadl
1080/tcp  filtered socks
3128/tcp  filtered squid-http
4444/tcp  filtered krb524
5061/tcp  filtered sip-tls
8000/tcp  open  http-alt
8080/tcp  open  http-proxy
8888/tcp  open  sun-answerbook
9898/tcp  filtered monkeycom
10000/tcp filtered snet-sensor-mgmt
12345/tcp filtered netbus
20000/tcp open  dnp

Nmap done: 1 IP address (1 host up) scanned in 29.61 seconds
root@Ins:~#
```

Gambar 5.8 Informasi yang didapat setelah menggunakan *Nmap Tools*

5.3. Analisis Data Vulnerability, Hasil Scanning dan information gatehering

Pada tahapan ini dapat dilakukan analisis vulnerability dengan data awal berupa report hasil dari scanning vulnerability pada portal website BAPPEDA Kota LubukLinggau yang dapat dilihat pada table 5.1.

Tabel 5.1. Data Hasil Scanning Vulnerability pada Portal WEB BAPPEDA Kota LubukLinggau

No	WEB Target	Tools			Hasil Scanning/ Information Gathering
		Whois domain	Builtwith	Nmap	
1	http://sipr.lubuklinggaukota.go.id	√			1. Domain Name : LUBUKLINGGAUKOTA.GO.ID 2. IP Location : Jakarta Raya – Jakarta – Rumahweb 3. ASN : AS58487 RUMAHWEB-AS-ID Rumahweb Indonesia CV. 4. Server Type : Apache/2.2.29 OpenSSL/1.0.1e-fips mod_bwlimited/14 mod. 5. Admin ID : baidil-65833 6. Admin Name : Baidillah Sangkut 7. Admin Organization : Pemerintah Kota Lubuklinggau 8. Admin Street1 : Jl Garuda No. 10 9. Admin Street2 : Jl Agung No. 31 10. Admin City : Lubuklinggau 11. Admin State / Province : Sumatera Selatan 12. Admin Postal Code : 31615 13. Admin Phone : +62.73332258 14. Admin Email : neknang@gmail.com
			√		1. Server Type : Apache 2.2 2. Frameworks : CodeIgniter, PHP 3. JavaScript Libraries : jQuery, Fancybox, jQuery Mousewheel 4. Mobile : Viewport Meta 5. Document Information :HTML5 DocType, Meta Description, Twitter, Bootstrap, Cascading Styke Sheets, Javascript 6. Encoding : UTF-8 7. Server Information : Ubuntu.

				√	1. 22/tcp (SSH) 2. 53/tcp (Domain) 3. 80/tcp (Http) 4. 443/tcp (Https) 5. 5432/tcp (Postgresql) 6. 8080/tcp (http-proxy)
2	http://report.lpse.lubuklinggaukota.go.id	√			a. <i>Registrar</i> : CV RUMAHWEB INDONESIA b. <i>Name Server(s)</i> : NS1.BAPPEDA LUBUKLINGGAU.NET (has 1 domains) NSID2.RUMAWEB.NET (has 275 domains) NSID3.RUMAHWEB.BIZ 9has 6 domains) NSID4.RUMAHWEB.ORG c. <i>Domain Name</i> : LUBUKLINGGAUKOTA.NET d. <i>Registrant Abuse Contact Email</i> : abuse@rumahweb.co.id e. <i>Registrant Abuse Contact Phone</i> : +62.274882257 f. <i>Admin Name</i> : Hadi Sanjaya g. <i>Admin Organization</i> : appedaotaubuklinggau h. <i>Admin City</i> : Jl. Garuda No. 10 Kelurahan Kayuara i. <i>Admin City</i> : Lubuklinggau j. <i>Admin State / Province</i> : Sumatera Selatan k. <i>Admin Postal Code</i> : 31616 l. <i>Admin Email</i> : andi_darmendra@yahoo.com
a. <i>Frameworks</i> : <i>Play Frameworks.</i> b. <i>JavaScript Libraries</i> : <i>JQuery 1.6.2, JQuery UI dan jqPlot.</i> c. <i>Document Informatio</i> : <i>HTML5 DocType, Cascading Style</i> <i>Sheets, Javascript.</i>					
a. 21/tcp (ftp) b. 22/tcp (SSH) c. 52/tcp (Domain) d. 80/tcp (http)					

					e. 110/tcp (POP3) f. 143/tcp (imap) g. 443/tcp (https) h. 631/tcp (ipp) i. 993/tcp (imaps) j. 995/tcp (POP3s)
--	--	--	--	--	--

5.4 Pembahasan (Evaluasi)

Dari hasil *scanning vulnerability* pada *portal website Monitoring dan Reporting SPSE LPSE dan Sistem Informasi Penataan Ruang (SIPR)* terdapat kerentanan yang di timbulkan karena adanya *Software Error, Security Error dan Human Error* sebagai berikut :

Tabel 6.1. Tabel perbandingan *vulnerability* pada portal website Monitoring dan Reporting SPSE LPSE dan Sistem Informasi Penataan Ruang (SIPR) di sebabkan *Software Error*

No	Jenis Kerentanan	Level	SPSE	SIPR
			Keterangan	Keterangan
1	Insecure Cross-Origin Resource Access Control	High	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/print_proxy/canvas.php , tehnik yang umum digunakan para attacker ialah dengan merubah coding header pada laman website guna menambahkan cross domain sebagai phishing site.

2	SQL Injection	High	http://121.100.28.196/report/application/login, dengan menggunakan tools Sqlmap pada kali linux atau Havij pada windows. Attacker dapat melakukan eksploitasi database serta remote server untuk mengambil hak akses penuh.	Tidak ditemukan kerentanan.
3	Cross Side Scripting	High	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/map/do_print, dengan menggunakan tools XSSER. Attacker dapat melakukan eksploitasi pada laman website untuk membuat phishing site login bagi administrator.
4	Session Cookie Without HttpOnly Flag	High	http://121.100.28.196/report, dengan memanfaatkan Java Script. Attacker dapat melakukan phishing site untuk mendapatkan user dan password administrator.	http://sipr.lubuklinggaukota.go.id, dengan memanfaatkan Java Script. Attacker dapat melakukan phishing site untuk mendapatkan user dan password administrator.
5	Session Cookie Without Secure Flag	High	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id, untuk dapat memanfaatkan kerentanan ini di butuhkan teknik dan pengalaman dari attacker pada umumnya attacker dapat memanfaatkan coding script pada website untuk di gunakan sebagai phishing site atau lainnya untuk mendapatkan user dan password administrator.
6	Application Error Massage	Medium	http://121.100.28.196/report/application/login, tidak terdapat tools maupun teknik yang pasti untuk kerentanan ini tergantung dari pengalaman attacker.	http://sipr.lubuklinggaukota.go.id/contact/save_form, tidak terdapat tools maupun teknik yang pasti untuk kerentanan ini tergantung dari pengalaman attacker.

7	Application Error Disclosure	Medium	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/map/do_print , tidak terdapat tools maupun teknik yang pasti untuk kerentanan ini tergantung dari pengalaman attacker.
8	X-content-type-options header missing	Low	http://121.100.28.196/report/public/javascripts/akunting.js , dengan memanfaatkan tools MIME-Sniffing attacker dapat menangkap packet data yang berjalan untuk akses login pada website.	http://sipr.lubuklinggaukota.go.id/contact/form_fill , dengan memanfaatkan tools MIME-Sniffing attacker dapat menangkap packet data yang berjalan untuk akses login pada website.
9	User credentials are sent in clear text	Low	http://121.100.28.196/report/application/loginpage , dengan memanfaatkan tools metasploit, ettercap attacker dapat melakukan teknik sniffing attack untuk masuk kedalam web server.	http://sipr.lubuklinggaukota.go.id/manage/auth/login , dengan memanfaatkan tools metasploit, ettercap attacker dapat melakukan teknik sniffing attack untuk masuk kedalam web server.

Tabel 6.2. Tabel perbandingan *vulnerability* pada portal website Monitoring dan Reporting SPSE LPSE dan Sistem Informasi Penataan Ruang (SIPR) di sebabkan *Security Error*

No	Jenis Kerentanan	Level	SPSE	SIPR
			Keterangan	Keterangan
1	Cleartext password over http	High	http://121.100.28.196/report/application/loginpage , Dengan menggunakan tools sniffing attack yang terdapat pada kali linux seperti metasploit. Attacker dapat menangkap aliran packet data yang sedang berjalan guna melakukan otentikasi login pada website.	http://sipr.lubuklinggaukota.go.id/manage/auth/login , Dengan menggunakan tools sniffing attack yang terdapat pada kali linux seperti metasploit. Attacker dapat menangkap aliran packet data yang sedang berjalan guna melakukan otentikasi login pada website.

2	From password field with autocomplete enabled	Medium	http://121.100.28.196/report/application/loginpage , masih dengan menggunakan teknik sniffing guna mendapatkan informasi sebagai otentikasi login attacker kedalam website.	http://sipr.lubuklinggaukota.go.id/manage/auth/login , masih dengan menggunakan teknik sniffing guna mendapatkan informasi sebagai otentikasi login attacker kedalam website.
3	Local filesystem paths found	Medium	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/info , untuk memanfaatkan kerentanan ini di butuhkan pengalaman serta kemampuan attacker. Kerentanan ini umumnya menampilkan layout filesystem root.
4	Backup files	Medium	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/map/show/10.000 , dibutuhkan pengalaman serta kemampuan lebih bagi attacker untuk melakukan eksekusi pada kerentanan ini. Umumnya kerentanan ini menampilkan backup file yang terdapat pada web server.
5	Source code disclosure	Medium	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/manage/auth/login , di butuhkan pengalaman serta kemampuan lebih attacker untuk memanfaatkan kerentanan ini. Umumnya kerentanan ini menampilkan informasi sensitif seperti string database dan logika aplikasi yang berjalan pada website.

6	Password autocomplete in browser	Low	http://121.100.28.196/report/application/loginpage , pada umumnya kerentanan ini dapat di eksekusi dengan serangan sniffing attack guna menangkap informasi sensitif seperti username dan password administrator.	http://sipr.lubuklinggaukota.go.id/manage/auth/login , pada umumnya kerentanan ini dapat di eksekusi dengan serangan sniffing attack guna menangkap informasi sensitif seperti username dan password administrator.
7	Directory listing detected	Low	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/print_proxy/ , umumnya dengan menggunakan tools Dirbuster attacker dapat melakukan serangan pada directory website guna mendapatkan data-data penting website.

Tabel 6.3. Tabel perbandingan *vulnerability* pada portal website Monitoring dan Reporting SPSE LPSE dan Sistem Informasi Penataan Ruang (SIPR) di sebabkan *Human Error*

No	Jenis Kerentanan	Level	SPSE	SIPR
			Keterangan	Keterangan
1	SVN respository found	Medium	Tidak ditemukan kerentanan.	http://sipr.lubuklinggaukota.go.id/themes/default_admin/setting , untuk memanfaatkan kerentanan ini di butuhkan kemampuan dan pengalaman lebih attacker guna menampilkan informasi subversi pada folder direktori.

2	Web browser xss protection not enabled	Low	<p>http://121.100.28.196/report/public/javascripts/akunting.js, dengan memanfaatkan kode java script seperti cookie stealing, url redirection attacker dapat mengambil informasi sensitif website.</p>	<p>http://sipr.lubuklinggaukota.go.id/assets/ico/favicon.png, dengan memanfaatkan kode java script seperti cookie stealing, url redirection attacker dapat mengambil informasi sensitif website.</p>
3	Apache mod_negotiation filename bruteforcing	Low	<p>tidak terdapat tools maupun teknik khusus untuk melakukan teknik eksploitasi pada kertanan ini. Umumnya data informasi yang di hasilkan berupa file direktori, backup maupun bruteforcing yang terdapat pada web server.</p>	<p>tidak terdapat tools maupun teknik khusus untuk melakukan teknik eksploitasi pada kertanan ini. Umumnya data informasi yang di hasilkan berupa file direktori, backup maupun bruteforcing yang terdapat pada web server.</p>
4	Login page password-guessing attack	Low	<p>http://121.100.28.196/report/application/login, dengan menggunakan tools brutus attacker dapat melakukan serangan bruteforce untuk mendapatkan informasi username dan password pada website.</p>	<p>http://sipr.lubuklinggaukota.go.id/manage/auth/proc_login, dengan menggunakan tools brutus attacker dapat melakukan serangan bruteforce untuk mendapatkan informasi username dan password pada website.</p>
5	Possible sensitive directories	Low	<p>Tidak ditemukan kerentanan.</p>	<p>http://sipr.lubuklinggaukota.go.id/phpmyadmin, umumnya teknik yang di pakai attacker dapat merubah source code pada website guna membuat phising login site bagi user dan administrator.</p>

BAB VI RENCANA TAHAPAN BERIKUTNYA

Adapun rencana tahapan berikutnya adalah akan melakukan pengujian yang sama terhadap beberapa portal yang digunakan pada semua Kabupaten dan Kotamadya yang ada di Provinsi Sumatera Selatan. Pada penelitian ini memang belum didapat hasil yang maksimal menurut peneliti dikarenakan ada beberapa factor yang mempengaruhi terlaksananya pengujian misalnya tools yang digunakan hanya beberapa tools saja. Dari permasalahan ini peneliti akan menambahkan beberapa tools lagi sebagai alat pengujian, yang mungkin nantinya dapat menghasilkan hasil yang lebih maksimal.

BAB VII SIMPULAN DAN SARAN

7.1 Kesimpulan

1. Setelah melalui serangkaian proses *penetration testing* terhadap *vulnerability* yang ada dengan menggunakan beberapa *tools*. Namun hasil yang didapat belum begitu maksimal, dikarenakan ada beberapa faktor yang mempengaruhi *vulnerability* tersebut seperti, pada *HTTP Request*.

7.2 Saran

Beberapa yang harus dihindari dari hal yang tidak diinginkan terhadap *web server* pada saat melakukan *penetration testing*, diantaranya:

1. Mengontrol *HTTP Request* dengan memfilter atau menyembunyikan metode *PUT* dan *DELETE* dari *user* tanpa autentikasi.
2. Melakukan perbaikan terhadap *Script Connection* pada *form* yang terdapat dalam *website*.
3. Mengaktifkan *SSL* pada *form login* guna melindungi *password* yang diinputkan pada *form login website*.

DAFTAR PUSTAKA

- Santoso, Hanif dkk. *Analisis Vulnerability Aplikasi iFace IT Telkom bandung*. paper UAS CS4633 Keamanan Sistem. Bandung.
- Priandoyo, Anjar. (2006). *Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi*. Jurnal Sistem Informasi. Vol. 1, No. 2, pp.73-83.
- Lumy, Gildas Deograt. *Ilusi Test Penetrasi Bagian 1*, InfoKomputer, April 2010.
- GOV-CSIRT. 2012. *Methodology Vulnerability Assessment*. Diakses pada 1 Desember 2013, <<http://govcsirt.kominfo.go.id/254/>>.
- Indrajit, Richardus Eko. *Aneka Ragam Serangan Dunia Maya*. ID-SIRTII.
- Davison, R. M., Martinsons, M. G., Kock N., 2004, *Journal : Information Systems Journal : Principles of Canonical Action Research*
- Simson Garfinkel, “*PGP: Pretty Good Privacy*,” : O’Reilly & Associates, Inc., 1995.)
- Menurut W. Stallings [William Stallings, “*Network and Internetwork Security*,” Prentice Hall, 1995.]
- “introduction to network security” - <http://www.interhack.net/pubs/network-security/networksecurity>.
- Jill H. Ellsworth; Matthew V. Ellsworth. 1994, *Using Computer Serve*, Que Corporation, Amerika. (<http://ns1.cic.ac.id/~eboo/ebook/adm/myebook/0028.pdf>)

Lampiran. Biodata Tim Peneliti

1.1 Biodata Ketua Peneliti

A. Identitas Diri

1	Nama	Irwansyah, M.M., M.Kom.
2	Jabatan Fungsional	Asisten Ahli Madya
3	Jabatan Struktural	-
4	NIP	0400110210
5	NIDN	0211117401
6	Tempat/Tgl. Lahir	Palembang, 11 November 1974
7	Alamat Rumah	Jl. Ramakasih II No.661 RT.07 Kel.Duku Palembang
8	Nomor Telepon/Faks/HP	081367531115
9	Fakultas/Jurusan	Ilmu Komputer / Teknik Komputer
10	Alamat Kantor	Jl. Jendral A.Yani No.12 Plaju Palembang
11	Nomor Telepon/Faks	0711-515679
12	E-Mail	Irwansyah@mail.binadarma.ac.id
14	Mata Kuliah yang Diampu	1. Jaringan Komputer 2. Komunikasi Data 3. Keamanan Jaringan Komputer

B. Riwayat Pendidikan

Jenjang	S1	S2
Perguruan Tinggi	Universitas Bina Darma Palembang	Universitas Bina Darma Palembang
Bidang Ilmu	Teknik Komputer	- Manajemen Sistem Informasi - Magister Teknik Informatika
Tahun Masuk-Lulus	1995-2001	2005 - 2007 2009-2011
Judul Skripsi/Tesis/Desertasi	Simulasi Gerak Lengan Robot dengan Menggunakan Motor DC.	- Analisis Tingkat Pendidikan, Pelatihan dan Pengalaman Terhadap Kemampuan Dalam Membuat Sistem Informasi. - Analisis Penerapan <i>Access Control List Router</i> dengan Pendekatan Metode <i>Quality Of Service (QoS)</i> (Studi kasus pada Jaringan Universitas Bina Darma
	1.	

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan
----	-------	------------------	-----------

			Sumber	Jml (Juta Rp)
1	2008	PERANCANGAN APLIKASI KAMUS ONLINE BAHASA PRANCIS YANG BERBASIS WAP (WIRELESS APLICATION PROTOCOL)	Mandiri	
2	2009	PERANCANGAN NETWORK ADDRESS TRANSLATION (NAT) ROUTER CISCO 2600 SERIES DENGAN MENGGUNAKAN SIMULATOR PAKET TRACER 4.11	Mandiri	
3	2011	PENERAPAN TRANSPARENT PROXY DAN BANDWIDTH MANAGEMENT UNTUK MENINGKATKAN KINERJA SERVER INTERNET MENGGUNAKAN MIKROTIK ROUTER OS	Mandiri	
4	2012	APLIKASI PENENTUAN WARIS PADA PERANGKAT MOBILE MENGGUNAKAN JAVA (J2ME)	Univ. Bina Darma	5 Jt
5	2013	ANALISA KEAMANAN JARINGAN TERHADAP ANCAMAN DATA FLOODING PADA BPBD PROV. SUMSEL	Univ. Bina Darma	5 Jt
6	2013	Analisis Log Router Untuk Meningkatkan Keamanan Jaringan Komputer pada Universitas Bina Darma	LPPM Universitas Bina Darma	6

D. Pengalaman Pengabdian Kepada Masyarakat Dalam 5 Tahun Terakhir

No.	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah (Juta Rp)
1	2010	Tim Penguji Ujian Nasional Praktek Kejuruan di SMK Negeri 1 Indralaya Selatan	SMK Negeri 1 Indralaya Selatan	
2	2011	Tim Penguji Ujian Nasional Praktek Kejuruan di SMK Negeri 1 Indralaya Selatan	SMK Negeri 1 Indralaya Selatan	
3	2011	Pelatihan Petugas Operator Komputer Sistem Informasi Manajemen Prov. Sumsel	Bappeda Prov. Sumsel	
4	2012	Tim Penguji Ujian Nasional Praktek Kejuruan di SMK Negeri 1 Indralaya Selatan	SMK Negeri 1 Indralaya Selatan	
5	2012	Relawan TIK Kota Palembang	Inforkom Kota Palembang	
6	2012	TIM Juri Lomba Kompetensi Siswa SMK Tingkat Provinsi Sumsel	Diknas Kota Palembang	
7	2013	TIM Juri Lomba Kompetensi Siswa SMK Tingkat Provinsi	Diknas Kota Palembang	

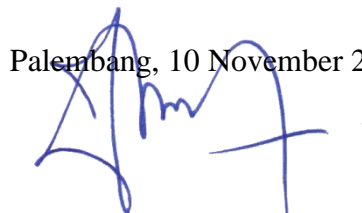
		Sumsel		
--	--	--------	--	--

E. Pengalaman Publikasi Ilmiah Dalam 5 Tahun Terakhir

No.	Tahun	Judul Artikel Ilmiah	Nama Jurnal
1	2008	PERANCANGAN APLIKASI KAMUS ONLINE BAHASA PRANCIS YANG BERBASIS WAP (WIRELESS APLICATION PROTOCOL)	<i>Matrik, ISSN:1411-1624</i>
2	2009	PERANCANGAN NETWORK ADDRESS TRANSLATION (NAT) ROUTER CISCO 2600 SERIES DENGAN MENGGUNAKAN SIMULATOR PAKET TRACER 4.11	<i>Matrik, ISSN:1411-1624</i>
3	2011	PENERAPAN TRANSPARENT PROXY DAN BANDWIDTH MANAGEMENT UNTUK MENINGKATKAN KINERJA SERVER INTERNET MENGGUNAKAN MIKROTIK ROUTER OS	<i>Matrik, ISSN:1411-1624</i>
4	2012	APLIKASI PENENTUAN WARIS PADA PERANGKAT MOBILE MENGGUNAKAN JAVA (J2ME)	<i>Snif2012</i>
5	2013	ANALISA KEAMANAN JARINGAN TERHADAP ANCAMAN DATA FLOODING PADA BPBD PROV. SUMSEL	<i>DISC2013</i>

Demikianlah Biodata ini dibuat dengan sebenar-benarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Penelitian Dosen Pemula dan dapat dipertanggungjawabkan secara hukum.

Palembang, 10 November 2015



(Irwansyah, M.M., M.Kom.)
NIP. 0400110210

1.2 Biodata Anggota Peneliti

A. Identitas Diri

1	Nama	Timur Dali Purwanto, M.Kom.
2	Jabatan Fungsional	-
3	Jabatan Struktural	-
4	NIP	130209378
5	NIDN	0203108505
6	Tempat/Tgl. Lahir	Palembang, 03Oktober1985
7	Alamat Rumah	Jl. PertahananLr. Kelapa 3 No.2096 RT.53RW.12

		Palembang
8	Nomor Telepon/Faks/HP	087897708339
9	Fakultas/Jurusan	Ilmu Komputer / Teknik Komputer
10	Alamat Kantor	Jl. Jendral A. Yani No.12 Plaju Palembang
11	Nomor Telepon/Faks	0711-515679
12	E-Mail	timur@mail.binadarma.ac.id
14	Mata Kuliah yang Diampu	1. Jaringan Komputer
		2. Fundamental TCP/IP
		3. Administrasi Linux
		4. Designing Security Windows Server
		5. Pemrograman

B. Riwayat Pendidikan

Jenjang	S1	S2
Perguruan Tinggi	Universitas Bina Darma Palembang	Universitas Bina Darma Palembang
Bidang Ilmu	Teknik Informatika	- Magister Teknik Informatika
Tahun Masuk-Lulus	2007-2010	2010-2011
Judul Skripsi/Tesis/Desertasi	Analisis Kinerja Jaringan Internet Universitas Bina Darma	Analisa kinerja wireless radius server pada perangkat access point 802.11g (studi kasus di universitas Bina Darma)

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No.	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jml (Juta Rp)
1	2014	Analisis Penerapan Metode Link Layer Pada Radius Server Untuk Meningkatkan Kinerja Jaringan WLAN (Studi Kasus Perusahaan)	LPPM Universitas Bina Darma	13.500.000

		Pengguna Radius Server/Hotspot)		
--	--	---------------------------------	--	--

D. Pengalaman Pengabdian Kepada Masyarakat Dalam 5 Tahun Terakhir

No.	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah (Juta Rp)
1	2014	Tim Penguji Ujian Nasional Praktek Kejuruan di SMK Negeri 1 Indralaya Selatan	SMK Negeri 1 Indralaya Selatan	Rp.1.500.000
2	2013	Pengenalan Komputer 'Kismart IBM' sebagai Pelengkap Perpustakaan Anak di Perpustakaan Daerah Sumatera Selatan	Perpustakaan Daerah Sumatera Selatan	Rp.1.000.000

E. Pengalaman Publikasi Ilmiah Dalam 5 Tahun Terakhir

No.	Tahun	Judul Artikel Ilmiah	Nama Jurnal
1	2013	PENERAPAN ANALISA KINERJA WIRELESS RADIUS SERVER PADA PERANGKAT ACCESS POINT 802.11G (STUDI KASUS DI UNIVERSITAS BINA DARMA)	<i>ISSN</i>
2	2014	PERANCANGAN JARINGAN VPN ROUTER DENGAN METODE LINK STATE ROUTING PROTOCOLS	<i>ISSN</i>

Demikianlah Biodata ini dibuat dengan sebenar-benarnya untuk memenuhi salah satu persyaratan dalam pengajuan Hibah Penelitian Dosen Pemula dan dapat dipertanggungjawabkan secara hukum.

Palembang, 29 April 2014


(Timur Dali P, M.Kom.)
NIP. 130209378