**PROPOSAL SKRIPSI**

**VULNERABILITY ASSESMENT PADA WEB SERVER WWW.BINADARMA.AC.ID**

**I. PENDAHULUAN**

* 1. **Latar Belakang**

Sistem Informasi memiliki peranan besar di semua perusahaan atau institusi agar dapat menghasilkan keuntungan semaksimal mungkin dengan cara mengiklankan, menjual, mengadministrasi, dan mewujudkan produk baru. Perusahaan dipaksa untuk menciptakan dan memikirkan inovasi baru agar dapat bersaing dan bertahan hidup di dalam persaingan bisnis yang ketat. (ibisa, 2011:1)

Menurut Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika dan Kementerian Komunikasi dan Informatika tahun 2011. Saat ini *website* merupakan salah satu layanan informasi yang banyak diakses oleh pengguna internet di dunia. Sebagai salah satu layanan informasi maka perlu dibangun *website* yang mampu menangani permintaan (*request*) dari banyak pengguna dengan baik (*reliable*). Pada dasarnya terdapat 4 (empat) elemen dasar dari sebuah *website* yaitu: *browser, server, URL,* dan *pages. Web server* berisi *web pages*, yang di dalamnya mengandung informasi atau dokumen yang ingin disebarluaskan atau diperlukan oleh para pengguna. Perkembangan teknologi membuat *website* menjadi alat berbagi informasi secara global. *Website* sendiri terhubung ke *web server*. Sejak beberapa tahun terakhir ini keamanan merupakan pokok persoalan utama. Banyak diberitakan mengenai penyusupan di *website* dan perusahaan atau perusakan dan penghilangan aset perusahaan yang dalam bentuk digital. *Web Server* seringkali menjadi target dari berbagai jenis serangan baik yang sifatnya minor maupun major sehingga berakibat fatal.Akan tetapi adakalanya *website* dijadikan pintu oleh peretas (hacker) untuk menembus *web server* bahkan sampai ke *root* untuk kesenangan bahkan dengan sengaja menyerang *website* tersebut. Oleh karena itu, untuk menghindari kejadian tersebut, banyak perusahaan keamanan komputer memberikan solusi dan penawaran perangkat penangkalannya baik berupa hardware maupun software dan jasa.

Meskipun umumnya serangan yang terjadi hanya menimbulkan kesan negatif, memalukan atau ketidaknyamanan (seperti *defacing*), seperti situs www.presidensby.info pada rabu 1 september 2012 sempat di *deface* peretas. Pelaku meninggalkan jejak dengan menuliskan diri sebagai *Jember Hacker Team*.Namun tidak tertutup kemungkinan penyerang dapat membuat masalah yang lebih serius atau bahkan sangat merugikan.

Dari pada orang lain yang tidak bertanggung jawab yang menemukan pintu masuk atau celah ke web *server www.binadarma.ac.id*, lebih baik saya dahulu yang menemukan dan melaporkan ke admin *web server www.binadarma.ac.id*.

* 1. **Perumusan Masalah**

Berdasarkan latar belakang di atas, maka perumusan masalah dalam penelitian ini yaitu bagaimana menganalisa serta menemukan kelemahan pada *web server www.binadarma.ac.id* untuk meningkatkan keamanan dan kenyamanan pada layanan *website www.binadarma.ac.id.* Dan dapat memberikan rekomendasi perbaikan.

* 1. **Batasan Masalah**

Agar penelitian tidak menyimpang dan tetap terarah diperlukan adanya batasan masalah.Batasan masalah dalam penelitian ini adalah *web server* yang di analisa adalah *web server www.binadarma.ac.id* dan hanya sebatas pengujian saja.

* 1. **Tujuan dan Manfaat Penelitian**
		1. **Tujuan Penelitian**

Penelitian ini bertujuan untuk :

1. Mengkaji kontrol keamanan *Internal* maupun *External* sistem dengan mengidentifikasi ancaman yang dapat menimbulkan masalah serius terhadap aset organisasi.
2. Serta diharapkan dapat membantu administrator dalam mengidentifikasi celah keamanan dan menutupnya sebelum diketahui dan dimanfaatkan oleh pengguna yang tidak bertanggung jawab.
	* 1. **Manfaat Penelitian**

Manfaat dari penelitian ini adalah :

1. Meningkatkan keamanan pada layanan *website.*
2. Bagi pihak Universitas Bina Darma tidak perlu mengeluarkan biaya untuk menyewa suatu perusahaan yang menjual jasa keamanan.
3. Bagi penulis dapat menambah pengetahuan dan pemahaman tentang keamanan sistem terutama pada *web server.*
4. Bagi mahasiswa penelitian ini bermanfaat untuk keamanan dan kenyamanan dalam menggunakan layanan pada *website www.binadarma.ac.id.*
5. **TINJAUAN PUSTAKA**
	1. **Objek Penelitian**

**2.1.1 Universitas Bina Darma**

UBD berdiri atas penggabungan 3 (tiga) Sekolah Tinggi  berdasarkan Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia Nomor : 112/D/0/2002 tanggal 7 Juni 2002 yaitu **STMIK Bina Darma** (Surat Keputusan Mendikbud RI. Nomor : 027/D/O/1994, tanggal 18 Mei 1994), **STIE Bina Darma** (SK. Mendikbud RI. Nomor : 046/D/O/1994, tanggal 7 Juli 1994), dan **STBA Bina Darma** (Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia nomor : 143/D/0/2001 tanggal 27 Agustus 2001).

Universitas Bina Darma adalah Perguruan Tinggi Swasta (PTS) yang mengasuh dan mengembangkan ilmu dan keahlian profesional pada 7 (tujuh) fakultas (Fakultas Ilmu Komputer, Fakultas Ekonomi, Fakultas Bahasa dan Sastra, Fakultas Teknik, Fakultas Psikologi, Fakultas Ilmu Komunikasi, dan Fakultas Keguruan dan Ilmu Pendidikan) dengan program studi unggulan tiap fakultas yang berada di Sumatera Selatan. Universitas Bina Darma mempunyai komitmen untuk menciptakan lulusan yang siap kerja dan dapat diterima di masyarakat. Untuk itulah Universitas Bina Darma mengusahakan Sertifikasi dari International *Organization for Standarization* ( ISO 9001:2000 ), dan pada tanggal 7 Juli 2003 telah memperoleh Sertifikasi dengan nomor Registrasi 04100. 30981. Dengan telah ditetapkan sistem manajemen mutu ISO 9001 : 2000 di Universitas Bina Darma maka setiap aktivitas dilaksanakan dengan terencana dan hasilnya dapat diukur secara objektif. Hal ini berarti proses belajar mengajar di Universitas Bina Darma telah sesuai dengan persyaratan dan peraturan yang berlaku, sehingga lulusannya sesuai dengan apa yang diharapkan oleh masyarakat. UBD secara aktif mengembangkan kerja sama di dalam maupun luar negeri yang saat ini tercatat memiliki perjanjian dengan UBD diantaranya adalah: *University of Industri Selangor* (UNISEL) Malaysia, Sun Microsystem, Barring Edu Training Sdn Bhd-Malaysia, Pearson VUE Authorised Center-India, NIIT Antilles NV – Neteherlands, Planet Edupro Indonesia (University of Cambridge English for Speakers of Other languages (ESOL) Authorised Main Center), Cisco Networking Academy, Stichting Hogeschool Zeeland (HZ)-Holland, dan NPO International Japanese Education Center.

**2.1.2 Web Server**

Menurut Direktorat Keamanan Informasi, Direktorat jenderal Aplikasi Informatika, dan Kementrian komunikasi dan Informatika tahun 2011 Web server adalah suatu komputer yang menyediakan layanan *World Wide Web* (WWW) pada internet, yang mencakup perangkat keras, sistem operasi, perangkat lunak Web server tersebut digunakan secara internal dan tidak oleh public, maka dikenal sebagai suatu “*server intranet”.*

Setiap kali sebuah web browser berhubungan dengan suatu situs web, sebetulnya ia berhubungan dengan sebuah *web server*.server tersebut mendengarkan (*listen*) request pada jaringan dan memberikan jawaban berupa data tertentu kepada client atau pengirim permintaan. Web server atau HTTP adalah sebuah program yang melayani koneksi HTTP (*Hyper Text Transfer Protocol*) yang bekerja di port 80 (secara default, namun kita bias rubah sesuai keinginan). Web server bekerja berdasarkan *request-response*, yaitu ketika HTTP client (web browser) membangun koneksi dengan mengirimkan request (permintaan) kepada server, maka server akan merespon dengan mengelola permintaan tersebut kemudian mengirimkan data sesuai yang diminta oleh HTTP Client. HTTP merupakan protocol yang bekerja pada lapisan aplikasi (application layer) dan secara sederhana dapat didefinisikan sebagai sekumpulan aturan untuk tukar menukar data pada *World Wide Web* (WWW). (Abdul Rohman, 2010)

* 1. **Landasan Teori**
		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* bias 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)

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

 Dijelaskan pula oleh Anjar Priandoyo tahun 2006 *Vulnerability assessment* (VA) adalah salah satu cara untuk pengukuran terhadap kemanan sistem. VAmerupakan salah satu bagian pengendalian preventif dalam keseluruhan rangkaian pengendalian TI, disamping berbagai metode pengendalian terhadap keamanan yang lain seperti detektif dengan IDS (*Instrusion Detection System),* atau preventif dengan firewall dan antivirus dan pengendalian akan keamanan informasi dalam perusahaan.

Proses VA bias diselenggarakan oleh internal departemen TI ataupun oleh pihak ketiga seperti firma audit TI atau konsultan TI. Dapat diselenggarakan dengan dana terbatas ataupun dengan spesialis dalam jumlah besar. Pelaksanaan VA disesuaikan dengan kondisi perusahaan, jenis industri hingga kebutuhan perusahaan tersebut.

Pada prakteknya di industri, permintaan akan VA umumnya datang setelah terjadi proses pemeriksaan TI yang kemudian berlanjut pada pemeriksaan kemanan data. VA seringkali merupakan tindak lanjut dari proses perencanaan strategi kemanan informasi, kelengkapan standar industry hingga faktor regulasi. Di Indonesia sebagian besar permintaan VA data dari indsutri yang memiliki ketergantungan tinggi pada TI seperti industry perbankan atau telekomunikasi atau pun dari industri yang sudah matang dalam pengelolaan TI-nya.

 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).

* + 1. **Penetration Testing**

 Ali dan Heriyanto (2011:39-40) menjelaskan bahwaPenetration test adalah proses melakukan eksplorasi dan eksploitasi lebih jauh ke dalam sistem target setelah megetahui *bug* atau *security hole* yang di report pada proses *vulnerability assesment*. Pada proses ini aktivitas *gainingaccess* coba di lakukan oleh *attacker*. *Attacker*akan mencoba mengeksploitasi celah keamanan sehingga berhasil mendapatkan akses ke dalam system target. Aktivitas *penetrationtest* bisa dikatakan sebagai aktivitas *gainingaccess* yang lebih spesifik dibandingkan dengan *vulnerabilityassessment*, karena pada proses ini *attacker* sudah terlebih dahulu mengetahui kondisi target. Selain itu pada proses *penetrationtest* sudah tidak ada lagi *falsepositive* karena *attacker* sudah mengetahui dengan benar kondisi target. Setelah melakukan analisa kerentanan sistem, pada proses ini peneliti berusaha untuk mendapatkan akses pada mesin target dengan melakukan *exploitasi.*

* + 1. **Tipe-tipe ancaman kemanan terhadap web server**

 Pada e-book yang diterbitkan oleh Direktorat kemanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kementrian Komunikasi dan Informatika tahun 2011 bahwa *web server* seringkali merupakan *host* yang paling banyak menjadi sasaran dan diserang di lingkup jaringan suatu organisasi.Akibatnya, mengamankan web server dan infrastruktur jaringan yang mendukungnya merupakan hal yang perlu dilakukan. Ancaman keamanan secara spesifik terhadap *web server* umumnya terbagi menjadi beberapa kategori :

1. Entitas *malicious* dapat mengeksploitasi *bug*  perangkat lunak dalam *web server*, sistem operasi *web server*, atau *active content* untuk memperoleh akses ilegal ke dalam *web server.*
2. Serangan *deniel of service* (DoS) yang diarahkan pada *web server* atau infrastruktur jaringan pendukungnya, sehingga dapat menolak atau menghalangi para pengguna sah yang akan memanfaatkan layanannya.
3. Informasi sensitive pada *web server*  yang memungkinkan untuk dibaca atau dimodifikasi tanpa otoritsasi.
4. Informasi sensitif di database penyangga yang digunakan untuk mendukung elemen interaktif dari suatu aplikasi *web injection,* misalnya injeksi *Structured Query Languange* (SQL), injeksi *Lightweight Direktory Access Protocol* (LDAP)*, cross-site scripting* (XSS).
5. Informasi sensitive yang ditransmisikan tanpa dienkripsi antara *web server* dan *browser* yang dapat disadap dan terbaca dengan jelas.
6. Informasi pada *web server* dapat diubah untuk tujuan jahat. *Defacement* (penggantian tampilan) situs web merupakan contoh yang umumnya dilaporkan untuk ancaman ini.
7. Entitas *malicious* yang berhasil mendapatkan akses illegal terhadap sumber daya di tempat lain dalam jaringan organisasi melalui suatu serangan terhadap *web server.*
8. Entitas *malicious* yang menyerang organisasi internal setelah membobol suatu *host web server*. serangan tersebut dapat dilancarkan secara langsung, misalnya dari  *host* yang bobol terhadap suatu server internal atau secara tidak langsung misalnya dengan menempatkan konten *malicious* pada web dalam *browser web* dari para pengguna yang mengunjungi situs tersebut.
9. Server yang dapat digunakan sebagai suatu titik distribusi perangkat serangan, pornografi, atau perangkat lunak yang dicopy secara ilegal.

Tipe serangan tak langsung terhadap *Web server* bertujuan mendapatkan informasi dari para penggunanya. Sebagai contoh, pengguna dibujuk atau secara otomatis diarahkan untuk mengunjungi situs Web *malicious*  tampak tidak mencurigakan (karena menyerupai website aslinya, dsb). Melalui aktivitas yang dilakukan pengguna pada website *malicious* tersebut, didapat

informasi penting pengguna sepeti *username*, *password*, dll. Hasil perolehan tersebut dapat disalahgunakan untuk mengakses *website* aslinya secara sah atau dengan kata lain merupakan salah satu upaya pencurian identitas. Serangan yang berhasil mampu membobol rahasia sumber daya situs Web atau merusak gambaran atau profil mengenai organisasi. Serangan tidak langsung ini dapat berbentuk:

1. *Phishing ,* dimana para penyerang menggunakan *social engineering* (rekayasa social untuk memperdaya para pengguna agar melakukan *logging* ke suatu situs palsu.
2. *Pharming,* dimana server DNS atau *file host* para pengguna dibobol sehingga para pengguna diarahkan ke suatu situs *malicious* pengganti situs yang sah.

Open Web Application Security Project (OWASP) adalah project open source yang dibangun untuk menemukan penyebab dari tidak amannya sebuah software dan menemukan cara menanganinya. Pada tahun 2013 ini OWASP menerbitkan *e-book* “The Ten Most Critical Web Application Security Risks”.Dan dijelaskan pula ada 10 celah keamanan aplikasi web yang ditemukan dan direkomendasi mereka tentang menanganinya sebagai standard keamanan minimal dari aplikasi web.

Berikut ini adalah 10 celah tersebut:

1. *Injection,* Injeksi kelemahan, seperti SQL, OS dan injeksi Lightweight Directory Access Protocol (LDAP) terjadi ketika data yang tidak dipercayadikirim ke penerjemah sebagai bagian dari suatu perintah atau query.Data yang dikirim penyerang dapat mengelabui penerjemah dalam menjalankan perintah yang tidak disengaja atau mengakses data yang tidak sah.
2. *Broken Authentication and Session Management,* Fungsi aplikasi yang berhubungan dengan pembuktian dan pembahasan manajemen seringkali tidak diterapkan dengan benar, sehingga memungkinkan penyerang membahayakan *password*, kunci, sesi token atau mengeksploitasi kelemahan implementasi lainnya untuk memperoleh identitas pengguna lain.
3. *Cross-Site Scripting* (XSS)**,** Kelemahan XSS terjadi ketika aplikasi mengambil data yang tidak dipercaya dan mengirimkannya ke web browser tanpa validasi atau pengesahan yang tepat atau tanpa jalan keluar.XSS memungkinkan penyerangan untuk mengeksekusi naskah atau tulisan dalam membaca korbannya yang mana dapat membajak sesi pengguna, merusak situs web, atau mengarahkan pengguna ke situs berbahaya.
4. *Insecure Direct Object References***,** Sebuah referensi objek langsung terjadi ketika pengembang mengekspos referensi ke suatu objek dalam implementasi, seperti file, petunjuk, atau tombol *database*. Tanpa pemeriksaan kontrol akses atau perlindungan lainnya atau penyerang dapat memanipulasi referensi-referensi ini untuk mengakses data yang tidak sah.
5. *Security Misconfiguration,* Keamanan yang baik membutuhkan adanya konfigurasi keamanan didefinisikan dan digunakan untuk aplikasi, kerangka kerja*,* aplikasi server, *web server,database server,* dan*platform.*Semua pengaturan ini harus didefinisikan,diimplementasikan dan dipelihara karena banyak yang tidak disertakan bersama konfigurasi *default* yang aman.Ini termasuk menjaga semua perangkat lunak *up to date.*
6. *Sensitive Data Exposure***,** Banyak aplikasi web tidak benar dalam melindungi data yang sensitive, seperti kartu kredit, id pajak dan pembuktian surat-surat berharga atau mandate.Penyerang dapat mencuri atau memodifikasi data yang lemah dilindungi tersebut untuk melakukan pencurian identitas, penipuan kartu kredit, atau kejahatan lainnya. Data sensitif layak mendapatkan perlindungan ekstra seperti enkripsi saat istirahat atau transit, serta tindakan pencegahan khusus bila ditukar dengan browser.
7. *Missing Function Level Access Control*, Hampir semua aplikasi web memverifikasi fungsi tingkat hak akses sebelum membuat fngsi 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.
8. *Cross-Site Request Forgery*, Sebuah serangan CSRF memaksa masuk ke browser korban untuk mengirim permintaan HTTP palsu, termasuk sesi *cookie* korban dan disertakan informasi otentikasi otomatislainnya. Untuk sebuah aplikasi web yang rentan.Ini memungkinkan penyerang untuk memaksa browser korban untuk menghasilkan serangan aplikasi yang menurutnya permintaan itu sah dari korban.
9. *Using Components with Known Vulnerabilities*, Komponen yang rentan, seperti *libraries, frameworks* dan modul perangkat lunak lain hampir selalu berjalan dengan hak penuh. Jadi, jika dimanfaatkan, mereka dapat menyebabkan hilangnya data yang serius maupun pengambilalihan server. Aplikasi yang menggunakan komponen-komponen yang rentan dapat merusak pertahanan mereka dan memungkinkan berbagai serangan dan dampak yang buruk.
10. *Unvalidated Redirects and Forwards*, Aplikasi web sering mengarahkan dan meneruskan pengguna ke situs halaman lain dan menggunakan data tidak dipercaya untuk menentukan halaman tujuan. Tanpa validasi yang tepat, penyerang dapat mengarahkan korban ke *phising* atau *malware sites*.Atau meneruskan untuk mengakses halaman yang tidak sah.

Dari penjelasan kedua *e-book* tersebut dapat kita lihat dari 2011 – 2013 ada beberapa perubahan tipe serangan dan teradapat beberapa ancaman dan tipe serangan terhadap *web server*. Dengan menggunakan beberapa tipe-tipe ancaman inilah peneliti akan melakukan analisa kerentanan pada *web server www.binadarma.ac.id.*

* + 1. **Resiko Keamanan Aplikasi**

Penyerang berpotensi menggunakan beragam cara melalui aplikasi anda untuk membahayakan bisnis atau organisasi anda. Masing-masing jalur ini merupakan risiko yang mungkin, atau tidak mungkin, cukup serius untuk memperoleh perhatian.



**Gambar 2.1** alur serangan pada aplikasi

Terkadang, jalur ini mudah untuk ditemukan dan mengeksploitasi dan terkadang juga sangat sulit ditemukan.Demikian pula bahaya yang diakibatkan dapat berkisar dari tidak ada sampai sangat merugikan.Untuk menentukan risiko organisasi, kita dapat mengevaluasi kemungkinan yang terkait dengan setiap agen ancaman, vector serangan, dan kelemahan keamanan dan menggabungkannya dengan memperkirakan dampak teknis dan bisnis untuk organisasi.Semua faktor-faktor ini menentukan keseluruhan risiko.

* + 1. **Hasil Pantauan Trafik dari Indonesia – *Security Incident Response Team on Information Infrastructure* (ID-SIRTII)**



Sumber: Pusat Layanan Informasi Keamanan Internet Nasional

 **Gambar 2.2** Trafik data di internet nasional, ID-SIRTII Januari 2013



Sumber : Pusat Layanan Informasi Keamanan internet Nasional

 **Gambar 2.3** Trafik data di internet nasional, ID-SIRTII Februari 2013



Sumber : Pusat Layanan Informasi Keamanan Internet Nasional

**Gambar 2.4** Trafik data di internet nasional, ID-SIRTII Maret 2013

Dari gambar tersebut dapat kita lihat variasi dari ancaman keamanan di internet nasional. Pada bulan Januari (Gambar 2.2), terlihat data SQL yang memiliki trafik yang sangat tinggi. Menjelaskan bahwa teknik *SQL injection* dilakukan oleh kelompok atau individu tertentu untuk melakukan serangan terhadap korban mereka. Bulan Februari (Gambar 2.3), SQL masih pada trafik tertinggi. Maka dari itu dalam bulan januari dan februari trafik data SQL masih digunakan peretas untuk menyerang target mereka. Setelah itu pada bulan Maret (Gambar 2.4), Malware-CNC menggeser SQL dari peringkat trafik tertinggi. Menjelaskan bahwa lalu lintas Malware-CNC pada bulan tersebut sering dilakukan oleh individu atau kelompok tertentu.

**III. METODOLOGI PENELITIAN**

* 1. **Waktu Penelitian**

Waktu pelaksanaan penelitian dilakukan selama kurang lebih 1 bulan dimulai pada bulan Mei 2013 sampai dengan Agustus 2013.

* 1. **Kebutuhan Perangkat**

 Alat dan bahan yang digunakan dalam proses penelitian ini meliputi perangkat *hardware* dan *software* yang diantaranya sebagai berikut :

1. *Hardware* : satu unit *Personal Computer* atau *Laptop* bertindak sebagai *attacker.*
2. *Software* : Sistem Operasi Backtrack sebagai *attacker,* serta software dan tools lainnya sebagai pendukung peneliti untuk mengumpulkan informasi.
	1. **Metode Penelitian**
		1. **Metode penelitian tindakan (*action research*)**

Metode penelitian yang digunakan dalam penelitian ini menggunakan metode penelitan tindakan atau action research, ada lima tahapan dalam penelitian yang merupakan siklus dari *action research*, yaitu :

1. Melakukan diagnosa (*Diagnosing*)

 Pada tahapan ini peneliti akan melakukan identifikasi masalah-masalah yaitu diagnosa sistem keamanan pada *web server www.binadarma.ac.id*.

1. Membuat rencana tindakan (*Action Planning*)

 Tahapan ini peneliti melakukan pemahaman pokok masalah yang ada dan menyusun rencana tindakan yang tepat untuk menyelesaikan masalah yang ada.Peneliti akan mulai menyusun rencana pengujian yang akan dilakukan pada *web server www.binadarma.ac.id.*

1. Melakukan tindakan (*Action Taking*)

 Mengimplementasikan rencana tindakan yang telah disusun. Pada langkah ini peneliti mulai melakukan tahapan-tahapan investigasi guna mendapatkan informasi kelemahan sistem dan mengujinya secara langsung dengan menggunakan tipe-tipe ancaman terhadap *web server* dan objeknya adalah *www.binadarma.ac.id.*

1. Melakukan evaluasi (*Evaluating*)

 Setelah tahapan *Action Taking* dilaksanakan peneliti mulai melakukan evaluasi pada hasil dari implementasi sebelumnya dan mulai menyimpulkan hasil dari langkah sebelumnya.

1. Pembelajaran (*Learning*)

 Langkah ini merupakan tahap akhir dari penelitian yaitu melakukan review terhadap hasil dari tahapan-tahapan yang telah dilalui.

* + 1. **Metode Pengumpulan Data**

 Dalam penyusunan penelitian ini penulis mengumpulkan data yang dibutuhkan dalam pengujian penetrasi menggunakan metode pengumpulan data sebagai berikut :

1. Pengamatan (*Observation*)

Peneliti melakukan peninjauan langsung ke Universitas Bina Darma khususnya di bagian unit pelaksanaan teknis (UPT-SIM) yang merupakan bagian teknis system informasi di Universitas Bina Darma dengan pemilihan, pengubahan, pencatatan dan pengkodean serangkaian perilaku dan suasana berkenaan dengan objek penelitian

1. Wawancara (*Interview*)

Demi mendapatkan informasi dan data-data yang berhubungan dengan penelitian ini maka penulis mengajukan beberapa pertanyaan dan diskusi kepada ketua unit satuan kerja TI Universitas Bina Darma serta jajarannya guna untuk mendapatkan informasi gambaran jaringan *web server* serta sistem keamanan*web server* untuk mempermudah penelitian.

1. Studi kepustakaan (*Literature*)

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

* + 1. **Metode Deskriptif**

 Menurut Nasir (2003:54) bahwa metode deskriptif adalah suatu metode dalam meneliti status sekelompok manusia, suatu objek, suatu set kondisi, suatu sistem pemikiran, ataupun suatu kelas peristiwa pada masa sekarang. Tujuan dari penelitian deskriptif ini adalah untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat mengenai fakta-fakta, sifat-sifat serta hubungan antarafenomena yang diselidiki.

* 1. **Penelitian Sebelumnnya**

Penelitian sebelumnya digunakan untuk dapat dijadikan sebagai bahan pertimbangan dan diharapkan dapat membantu dalam penelitian.

 Menurut penelitian Hanif Santoso, dkk dengan judul penelitian “Analisis *Vulnerability* Aplikasi iFace IT Telkom Bandung”. Menjelaskan bahwa dari sisi dalam aplikasi, dengan bantuan *tools* backtrack 5 di Linux, terlihat masih banyak terdapat celah keamanan yang cukup banyak untuk dilakukan *SQL injection*  pada aplikasi web iFace. Lalu menghindari *brute force attack*  dengan memberikan batasan sebanyak 3 atau 5 kali untuk kesalahan ataupun kegagalan login aplikasi. Dan mengganti sisi penggunaan HTTP ke HTTPS yang dimana penggunaan protokol HTTPS yang dinilai lebih *secure* agar apabila terdapat hacker yang ingin melakukan *sniffing*  terhadap data seperti *password* dan *username* menjadi lebih sulit dan terhambat.

 Lalu pada penelitian selanjutnya artikel ilmiah yang ditulis oleh Ir. Kodrat Iman Satoto, MT (2009), dengan judul “ Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Dipenogoro”. Pada penelitian ini dinyatakan bahwa :

1. Data kata sandi pada sistem login tidak dienkripsi sebelum dikirim ke server,
2. Penggunaan kata sandi *default* sama dengan nama pengguna (*username*) menjadikan sistem rawan penyusup,
3. Data sesi yang dikirim dari perambanan ke *server*  tidak terenkripsi,
4. Penyerangan dengan teknik *SQL Injection*  tidak dapat dilakukan pada sistem login maupun *query string*  pada baris alamat,
5. Jejak nama pengguna dan kata sandi dapat dilihat pada pengelola kata sandi peramban Firefox sebagai teks tidak terenkripsi.

**Jadwal Penelitian**

|  |  |  |
| --- | --- | --- |
| No | Jenis kegiatan | Bulan |
| Mei | Juni | Juli | Agustus |
| Minggu ke |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 |
| 1 | ***Diagnosing* (diagnosa)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Identifikasi sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 2 | ***Action Planning* (rencanan tindakan)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mengumpulkan informasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mencari kelemahan sistem |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 3 | ***Action Taking* (tindakan)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Uji penetrasi |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | ***Evaluating* (evaluasi)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Evaluasi hasil |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 5 | ***Learning* (pembelajaran)** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Dokumentasi dan *Repoting* |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Menyimpulkan |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | **Konsultasi, Penulisan dan Penyusunan Skripsi** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Keterangan : Telah dilaksanakan Belum dilaksanakan

**DAFTAR PUSTAKA**

Ali, Shakel., Heriyanto, Tedy. 2011. *Backtrack 4: Assuring Security by Penetration Testing*. Birmingham-Mumbai: PACK Publishing Open Source.

Direktorat Keamanan Informasi, Direktorat Jendral Aplikasi Informatika, Kementerian Komunikasi dan Informatika Republik Indonesia. 2011. E-Book: *Panduan Keamanan Web Server.*

GOV-CSIRT. 2012. *Methodology VulnerabilityAssessment.*

Diakses pada 12 april 2013, <http://govcsirt.kominfo.go.id/254/>.

IBISA.(2011). *Keamanan Sistem Informasi.*Yogyakarta: Andi

Kusmandani, Syaful. (2013). *Kisah Hacker Pembobol Situs Presiden SBY*. Diakses pada 12 april 2013, <http://inet.detik.com/read/2013/01/29/130724/2155140/323/kisah-hacker-pembobol-situs-presiden-sby>.

Nasir, Moh PH.D. 2003. Metode Penelitian. Jakarta: Ghalia Indonesia

OWASP. (2013). *The Ten Most Critical Web Application Security Risk*. E-book.Edisi ke-2.

Priandoyo, Anjar. (2006). *Vulnerablity Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi*. Jurnal Sistem Informasi. Vol. 1, No. 2, pp.73-83.

Rohman, Abdul. (2010). *Membangun DNS Server Dan Web Server Dengan Debian Linux*.ICT SMK Muhammadiyah 5 babat.

Santoso, Hanif. *Analisis Vulnerability Aplikasi iFace IT Telkom bandung*. paper UAS CS4633 Keamanan Sistem. Bandung.

Satoto, Kodrat Iman. (2009).  *Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Dipenogoro*. Artikel Ilmiah. Yogyakarta: Universitas Dipenogoro.

Sejarah Universitas Bina Darma. Diakses pada 12 april 2013,

<http://www.binadarma.ac.id/content/27/4/Sejarah.html>