SK42
Sistem Maklumat Pengujian Keselamatan Teknologi Maklumat Berasaskan OSSTMM

Firkhan Ali Hamid Ali[1] & M. Tarmizi Abd. Wahab[2]

[1,2]Fakulti Teknologi Maklumat dan Multimedia, UTHM, Parit Raja, Johor
[1]firkhan@uthm.edu.my

Abstrak: Sistem Maklumat Pengujian Keselamatan Teknologi Maklumat ini dibangunkan berasaskan kepada modul-modul manual yang terdapat dalam *Open Source Security Testing Methodology Manual* (OSSTMM). OSSTMM menggunakan borang-borang secara manual untuk memasukkan maklumat-maklumat hasil pengujian dan pemerhatian keselamatan bagi sesebuah infrastruktur teknologi maklumat. Sistem maklumat berkomputer ini akan memudahkan pengguna untuk memasukkan, mengedit dan melihat data-data dan maklumat-maklumat yang telah diperolehi daripada sistem pengujian keselamatan teknologi maklumat tersebut.

Kata kunci: Sistem maklumat, teknologi maklumat, keselamatan, OSSTMM

1. Pengenalan

Isu keselamatan dalam dunia teknologi maklumat merupakan satu perkara yang sangat penting dan ia sering dibincangkan oleh pakar-pakar teknologi maklumat seluruh dunia (Firkhan, 2006). Oleh itu, satu proses pengujian tahap keselamatan bagi sesuatu implementasi teknologi maklumat perlu dilakukan agar ia memenuhi piawaian keselamatan yang ditetapkan sekurang-kurangnya pada tahap yang minimum (Blaha, 2001).

Oleh yang demikian, sebuah organisasi yang tidak berasaskan keuntungan iaitu *Institute for Security and Open Methodology* (ISECOM) telah mengambil satu usaha yang baik dengan membangunkan sebuah manual piawaian pengujian tahap keselamatan dalam implementasi teknologi maklumat. Manual tersebut dikenali sebagai *Open Source Security Testing Methodology Manual* (OSSTMM) (Herzog, 2006).

OSSTMM merupakan sebuah manual penilaian untuk menguji tahap keselamatan bagi sesebuah implementasi teknologi maklumat terutama dalam infrastruktur fizikalnya (Herzog, 2006). Ia mengandungi panduan terperinci berkenaan dengan praktikal pengujian dan penilaian laporan keputusan pengujian.

Manual OSSTMM ini adalah dalam bentuk borang-borang dan panduan-panduan yang boleh dicetak atau digunakan secara digital. Perlaksanaan pengujian keselamatan implementasi teknologi maklumat boleh dibuat berdasarkan kepada panduan-panduan yang terdapat di dalamnya (Gollmann, 2006). Kemudian terdapat borang-borang yang boleh digunakan untuk mencatat dan menyimpan maklumat-maklumat berkenaan dengan hasil pengujian-pengujian yang telah dibuat.

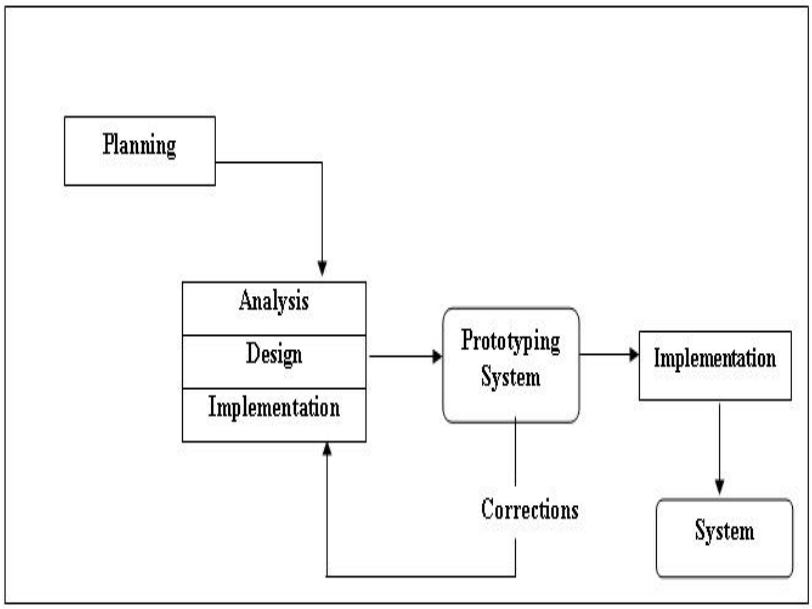
Sistem yang dibangunkan adalah Sistem Maklumat Pengujian Keselamatan Teknologi Maklumat berasaskan OSSTMM yang boleh diakses menerusi pelayar web dan mempunyai pangkalan datanya yang tersendiri untuk menyimpan maklumat-maklumat hasil pengujian keselamatan yang telah dibuat.

OSSTMM dipilih sebagai metodologi pengujian keselamatan teknologi maklumat kerana ia adalah berasaskan sumber terbuka dan masih dalam bentuk manual.

2. Metodologi

Pembangunan sistem maklumat ini dibuat menggunakan metodologi Kitar Hayat Pembangunan Sistem atau *System Development Life Cycle* (SDLC). Penggunaan SDLC dapat memastikan sistem yang dibangunkan untuk sesebuah organisasi berupaya memenuhi objektif-objektif yang ditetapkan dan mematuhi keperluan semasa yang dirancang (Usdoj, 2006).

Model prototaip digunakan dalam pembangunan sistem ini seperti yang ditunjukan dalam Rajah 1. Model prototaip ini mempunyai lima fasa perlaksanaan iaitu perancangan, analisis, reka bentuk, implementasi dan prototaip dan; implementasi dan pengujian.



Source: (Denis, 2006)

Rajah 1: Model Pembangunan Prototaip

2.1 Fasa Perancangan

Dalam fasa ini, sistem manual yang terdapat dalam pengujian keselamatan teknologi maklumat OSSTMM perlu dikaji dengan lebih teliti dan terperinci. Jadual perancangan juga dibangunkan bagi memudahkan fasa-fasa yang seterusnya dilaksanakan sehinggalah sistem maklumat ini berjaya dibangunkan.

Disamping itu, keperluan-keperluan seperti perkakasan, perisian, sumber kerja dan sebagainya perlu ditentukan dengan segera dan tepat. Ia perlulah mengikut kehendak persekitaran teknologi maklumat sesebuah organisasi tersebut. Dalam projek ini, sebuah makmal di Fakulti Teknologi Maklumat dan Multimedia, UTHM telah dikenal pasti untuk implementasi projek ini.

2.2 Fasa Analisis

Segala maklumat berkenaan dengan sistem maklumat yang dibangunkan dikumpul dan dianalisis dengan lebih terperinci. Strategi pembangunan sistem maklumat juga dikaji dengan teliti agar ia bersesuaian dengan sistem manual OSSTMM. Kesemua keperluan perkakasan dan perisian diperincikan dengan lebih teliti.

Di samping itu, keperluan dalam sistem maklumat OSSTMM juga dikenal pasti agar ia dibangunkan bersesuaian dengan keperluan pengguna dan manual OSSTMM. Ia juga melibatkan proses-proses dalam mengenal pasti bahasa pengaturcaraan yang digunakan, modul-modul untuk pengguna dan keperluan sistem dalam perlaksanaan proses-proses OSSTMM.

2.3 Fasa Reka Bentuk

Keseluruhan reka bentuk sistem maklumat OSSTMM ini dihasilkan berdasarkan kepada hasil analisa terperinci keperluan sistem dan pengguna dalam fasa analisis. Ia melibatkan proses-proses mereka bentuk paparan pengguna seperti antara muka pengguna sistem, struktur-struktur asas sistem, reka bentuk output dan pengenalpastian kod-kod aturcara untuk antara muka sistem.

2.4 Fasa Protaip dan Implementasi

Dalam fasa ini, segala proses pengaturcaraan kod-kod dilaksanakan berdasarkan kepada fasa-fasa yang sebelumnya. Seterusnya, sebuah prototaip sistem maklumat OSSTMM akan dihasilkan. Namun begitu, pada fasa ini, sekiranya ada keperluan atau kelemahan, ia akan berulang kembali kepada fasa analisis dan reka bentuk sehinggalah sistem maklumat OSSTMM itu berupaya berfungsi dengan baik dan diterima oleh pengguna.

Pangkalan data yang telah direka bentuk dalam fasa sebelum ini akan dibangunkan berserta dengan antara muka sistem maklumat yang telah dikenal pasti. Proses pengulangan kepada fasa-fasa yang sebelum ini akan berlaku setelah prototaip sistem maklumat OSSTMM ini diuji oleh pembangun dan para pengguna.

2.5 Fasa Pengujian dan Implementasi

Dalam fasa ini, model prototaip sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM telahh diubah kepada satu sistem maklumat yang sedia untuk diimplementasikan secara sepenuhnya dan diterima pakai secara nyata. Modul-modul dalam sistem maklumat OSSTMM telah diuji lari dengan baik dalam fasa ini. Seterusnya adalah pengujian penerimaan oleh pengguna bagi memastikan ia bertepatan dengan kehendak dan keperluan pengguna yang akan menggunakannya.

Pengujian secara sepenuhnya akan dilakukan kepada sistem maklumat OSSTMM ini untuk yang terkahirnya sebelum ia boleh diguna pakai oleh pengguna. Sekiranya berjaya diujilarikan tanpa ralat dan memenuhi kehendak dan keperluan pengguna, ia akan diimplementasikan di tempat yang telah dicadangkan penggunaannya.

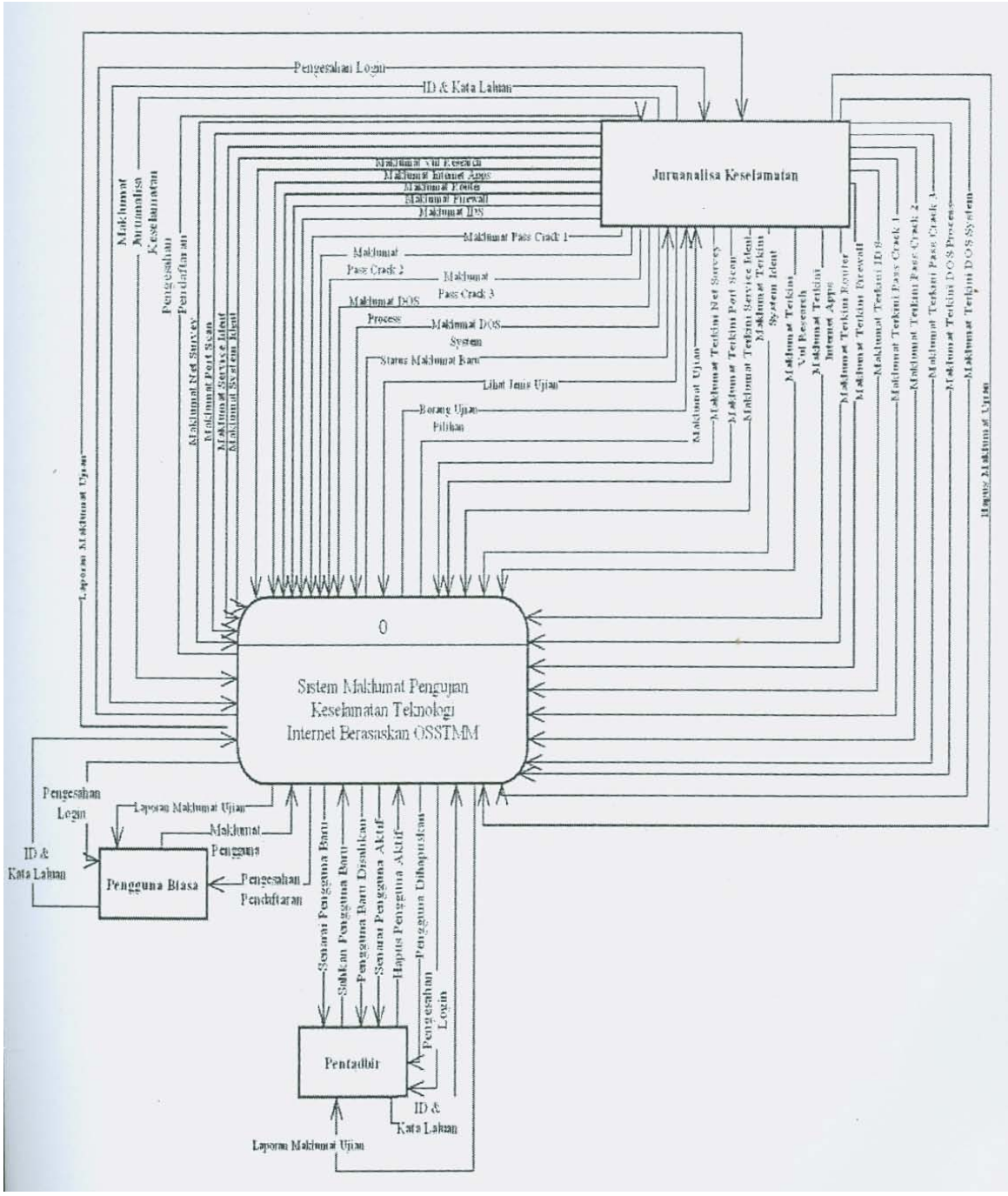
3. Arkitektur dan Reka Bentuk Sistem

Sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM ini telah dibangunkan berasaskan kepada aplikasi berasaskan web yang memerlukan pelayan web disamping pengkalan data untuk menjalankannya. Ia memudahkan pengguna untuk mengakses ke dalam sistem ini kerana ia boleh diakses menerusi mana-mana pelayar web dalam mana-mana sistem pengoperasian dan di mana-mana menerusi rangkaian dan Internet (Norton, 1999).

Diagram konteks seperti dalam Rajah 2 dibangunkan untuk menunjukkan bagaimana sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM yang dibangunkan ini berinteraksi dengan pengguna akhir dan pentadbir sistem. Ia merupakan gambaran umum bagi keseluruhan sistem maklumat OSSTMM dan menunjukkan hubungan antara entiti dengan sistem dan input dengan output.

Terdapat tiga entiti yang berinteraksi dengan sistem maklumat OSSTMM ini iaitu pengguna biasa, juruanalisa keselamatan dan pentadbir sistem. Pengguna biasa adalah seperti pihak atasan atau yang tertentu yang memerlukan akses hanya kepada laporan hasil pengujian keselamatan yang telah dibuat. Juruanalisa keselamatan pula menggunakannya untuk melihat panduan-panduan dalam perlaksanaan pengujian keselamatan, memasukkan maklumat hasil pengujian, kemas kini maklumat dan melihat laporan hasil-hasil pengujian keselamatan yang telah dibuat (Scambray, 2001).

Manakala pentadbir sistem pula bertindak sebagai koordinator kepada sistem maklumat OSSTMM ini seperti mengesahkan status pengguna, penambahan item-item atau atribut-atribut ke dalam sistem, penyelenggaraan sistem dan sebagainya. Kesemua pengguna perlu mendapatkan pengesahan pentadbir sistem terlebih dahulu sebelum dapat menggunakan sistem maklumat OSSTM ini.



Rajah 2: Diagram Konteks Sistem

4. Modul-Modul Sistem Maklumat OSSTMM

Sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM ini telah dibangunkan dalam kajian ini memberikan fokus utamanya dalam membangunkan aspek automasi sistem maklumat berkomputer daripada sistem manual borang bagi pengujian keselamatan teknologi maklumat berasaskan OSSTMM. Antara fungsinya adalah untuk mengisi, mencapai dan mengemas kini maklumat-maklumat hasil pengujian keselamatan teknologi maklumat berasaskan kaedah OSSTMM.

Terdapat beberapa modul yang telah dibangunkan dalam sistem ini seperti yang terdapat dalam Jadual 1.

Jadual 1: Modul-Modul dalam Sistem Maklumat OSSTMM

Indek	Modul Sistem	Pengguna	Keterangan
1	Pendaftaran	Semua pengguna	Pendaftaran pengguna baru dengan maklumat peribadi termasuk kata laluan dan lain-lain
2	Pengesahan Pendaftaran	Pentadbir Sistem	Pengesahan pengunan-pengguna dan tahap capaiannya dalam sistem.
3	Kemasukkan dan kemaskini maklumat pengujian dan hasil pengujian keselamatan	Juruanalisa keselematan sahaja	Proses kemasukkan maklumat pengujian dan hasil pengujian keselamatan. Kemas kini data.
4	Laporan	Semua pengguna	Melihat laporan bagi maklumat pengujian dan hasil pengujian yang telah dilakukan.

Berikut adalah beberapa jenis pengujian keselamatan teknologi maklumat yang boleh dilaksanakan oleh juruanalisa keselamatan dalam sistem maklumat OSSTMM berdasarkan kepada manual pengujian OSSTMM.

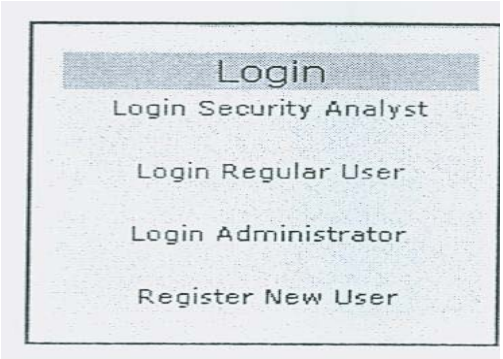
1. Pencarian maklumat rangkaian semasa.
2. Pengimbasan port.
3. Pengenalpastian servis-servis yang berjalan.
4. Pengenalpastian sistem yang digunakan.
5. Pengkajian dan pengecaman entiti-entiti tidak selamat atau *vulnerabalities*.
6. Pengujian aplikasi Internet.
7. Pengujian Router.
8. Pengujian Firewall.
9. Pengujian IDS.
10. Pemecahan kata laluan.
11. Pengujian DoS.

Panduan perlaksanaan pengujian-pengujian keselamatan teknologi maklumat seperti yang dinyatakan sebelum ini boleh diakses menerusi sistem maklumat OSSTMM oleh para juruanalisa keselamatan. Maklumat-maklumat pengujian dan hasil pengujian juga boleh dimasukkan, dicapai dan dikemaskini dengan lebih baik dan teratur menerusi sistem maklumat OSSTMM ini.

5. Implementasi Sistem Maklumat OSSTMM

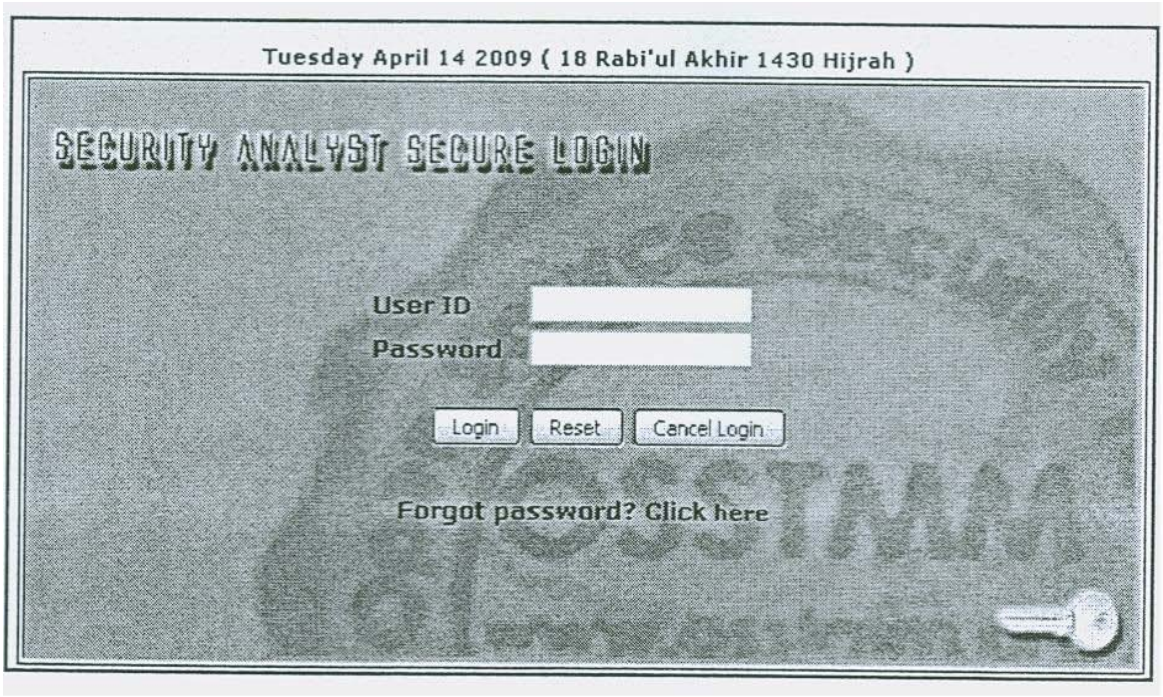
Sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM ini telah dibangunkan dalam kajian ini memberikan fokus utamanya dalam membangunkan aspek automasi sistem maklumat berkomputer daripada sistem manual borang bagi pengujian keselamatan teknologi maklumat berasaskan OSSTMM. Antara fungsinya adalah untuk mengisi, mencapai dan mengemas kini maklumat-maklumat hasil pengujian keselamatan teknologi maklumat berasaskan kaedah OSSTMM.

Pengguna sistem ini perlu mendaftarkan diri terlebih dahulu menerusi borang yang disediakan seperti di laman web yang disediakan. Maklumat-maklumat diri seperti yang diperlukan perlu didaftarkan terlebih dahulu. Di samping itu, kata laluan yang didaftarkan akan dienkripsi untuk keselamatan. Dalam Rajah 3 ditunjukkan menu kemasukan ke dalam sistem iaitu pendaftaran dan kemasukan untuk pengguna biasa, pentadbir atau penganalisa sekuriti.



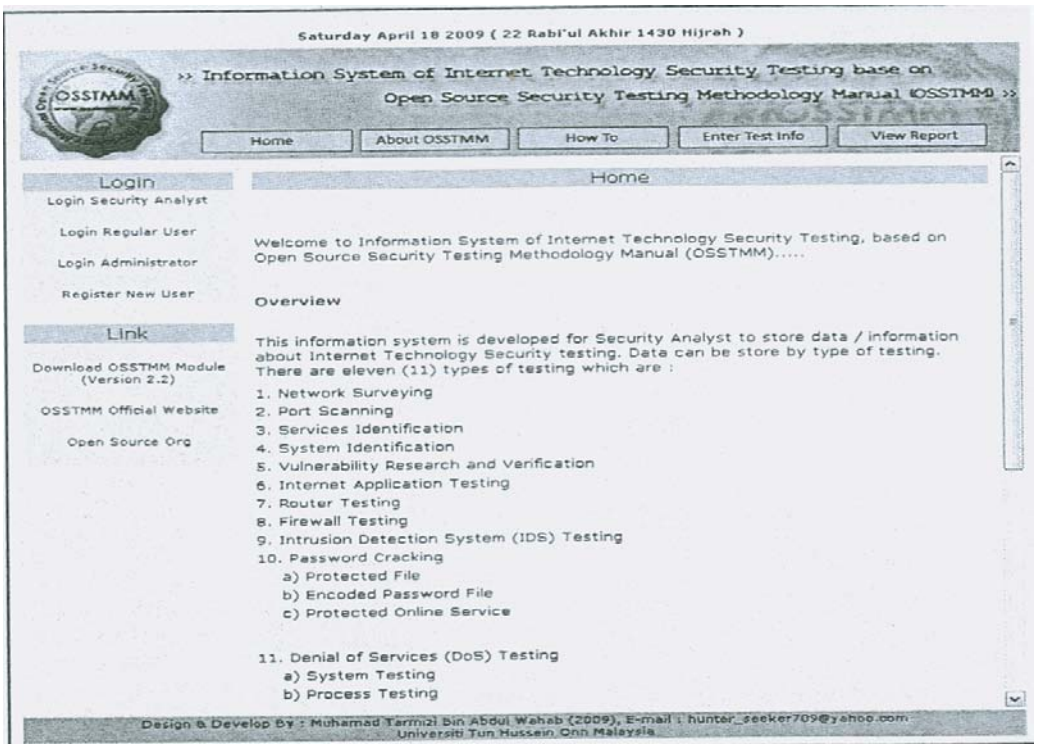
Rajah 3: Menu Kemasukan

Setelah pendaftaran berjaya, pengguna boleh masuk ke dalam sistem seperti yang ditunjukkan dalam Rajah 4.



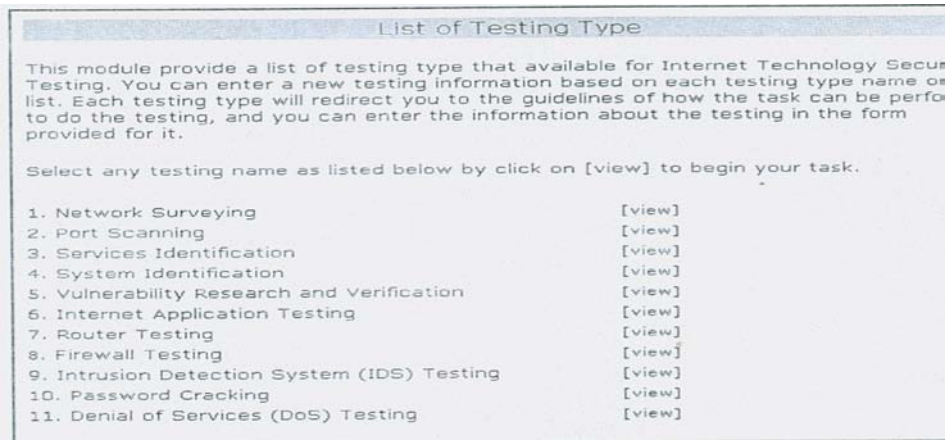
Rajah 4: Login dan kata laluan

Seterusnya adalah muka utama bagi sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM seperti yang terdapat dalam Rajah 5.



Rajah 5: Muka utama sistem maklumat pengujian keselamatan OSSTMM

Rajah 6 adalah laman muka untuk juru analisa keselamatan untuk memilih jenis pengujian yang akan dibuat.

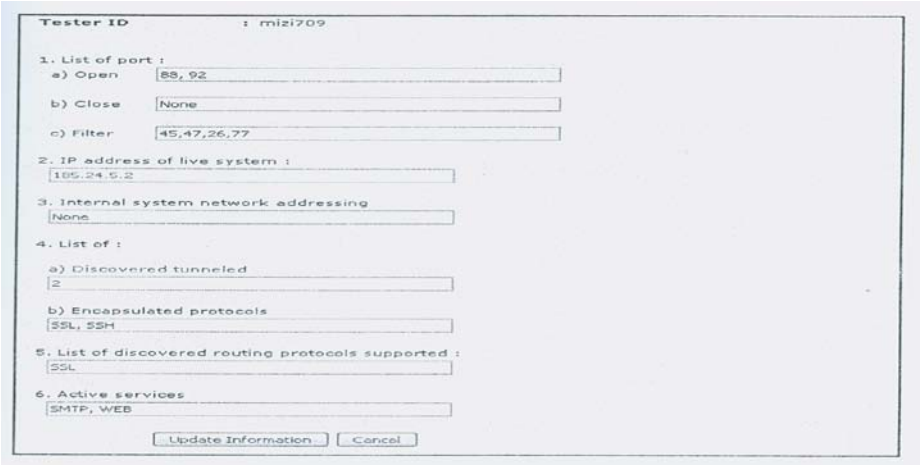


Rajah 6: Jenis-jenis pengujian keselamatan

Rajah 7 adalah laman sistem berkenaan dengan salah satu borang untuk memasukkan maklumat-maklumat berkenaan sesuatu jenis pengujian yang telah dibuat.

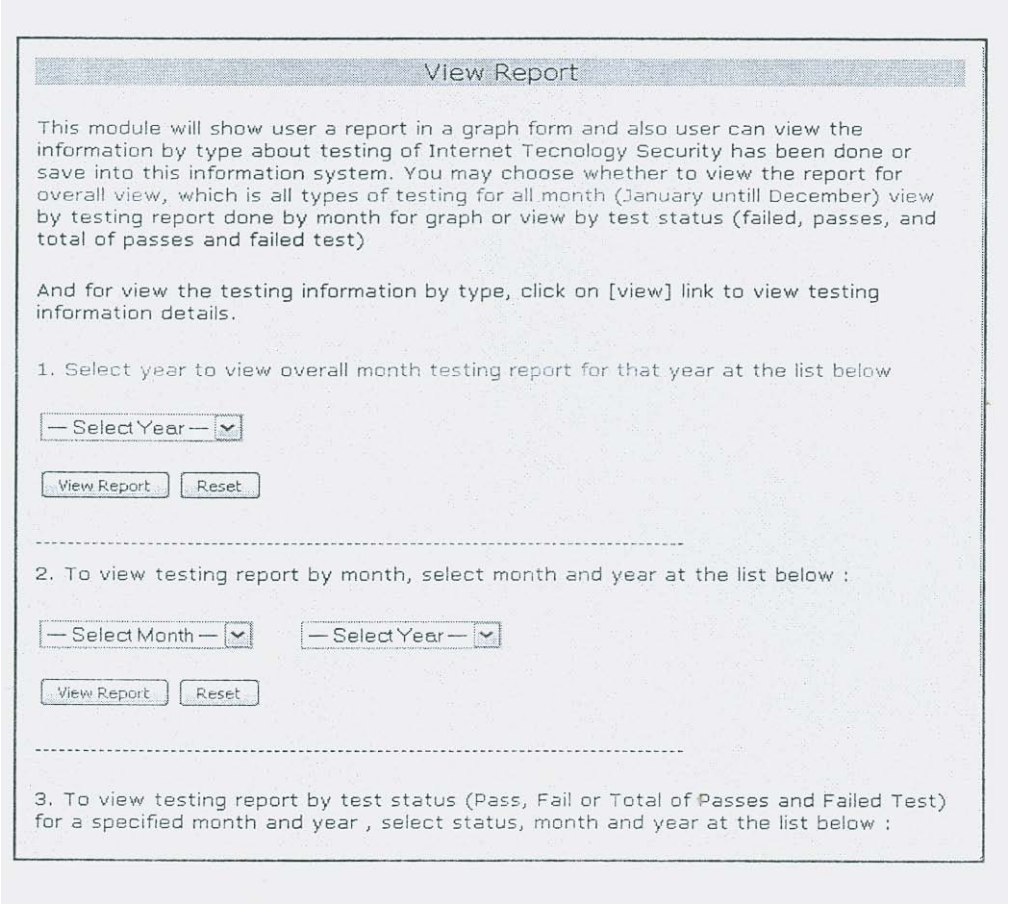
Rajah 7: Contoh borang isian maklumat pengujian

Rajah 8 pula menunjukkan contoh maklumat-maklumat pengujian keselamatan teknologi maklumat yang telah dimasukkan dan sedia untuk dikemas kini sekiranya perlu.



Rajah 8: Contoh maklumat hasil pengujian

Rajah 9 pula menunjukkan contoh laman sistem untuk penjanaan laporan hasil-hasil pengujian yang telah dijalankan dalam sistem maklumat yang telah dibangunkan.



Rajah 9: Contoh borang janaan laporan hasil pengujian

Itulah hasil implementasi yang telah dibangunkan sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM yang telah dikomputerkan daripada borang-borang manual pengujian OSSTMM.

6. Kesimpulan

Pembangunan sistem maklumat pengujian keselamatan teknologi maklumat OSSTMM ini adalah untuk memudahkan proses penyelengaraan dan pengurusan maklumat-maklumat pengujian dan hasil pengujian keselamatan teknologi maklumat yang telah dibuat (Firkhan, 2006). Ia memudahkan proses capaian, masukkan dan kemas kini maklumat yang berkaitan dengan cepat, teratur dan mudah. Kaedah pengujian OSSTMM ini diambil kerana ia telah melalui proses penilaian yang matang oleh pakar-pakar keselamatan teknologi maklumat menerusi organisasi ISECOM dan ia merupakan teknik pengujian yang berasaskan sumber terbuka.

Namun begitu skop perlaksanaannya adalah kecil dalam implementasi sistem maklumat ini iaitu sebuah makmal di Fakulti Teknologi Maklumat dan Multimedia (FTMM), Universiti Tun Hussein Onn Malaysia (UTHM). Ini adalah disebabkan kekangan masa dan usaha dalam pembangunan sistem maklumat ini. Modul janaan dalam laporan secara automatik dalam bentuk graf memudahkan pihak pengurusan sesebuah organisasi melihat maklumat-maklumat yang diperlukan secara kolektif dan terancang dalam untuk membuat seseuatu keputusan.

Begitu juga dengan sistem yang dibangunkan berasaskan web membolehkan ia diakses secara mudah dan pelbagai platfom menerusi pelayar web. Namun begitu, terdapat beberapa pelayar web yang memaparkan antara mukanya dalam bentuk yang tidak kemas tetapi fungsi-fungsinya dapat beroperasi dengan baik.

Akhir kata, sistem maklumat pengujian keselamatan teknologi maklumat berasaskan teknik OSSTMM ini dapat memudahkan pakar keselamatan teknologi maklumat dalam pengendalian maklumat pengujian

dan maklumat hasil pengujian untuk kepentingan sesebuah syarikat atau organisasi agar berupaya beroperasi dengan lebih baik.

Penghargaan

Jutaan terima kasih kepada pihak pengurusan FTMM dan UTHM kerana membiayai penerbitan kertas kerja ini. Terima kasih juga diucapkan kepada semua yang terlibat secara langsung dan tidak langsung dalam menghasilkan penulisan kertas kerja ini.

Rujukan

Blaha, K. D. & Murphy, L. C. (2001). Targeting assessment: how to hit the bull's eye. *Journal of Computing Sciences in Colleges.* Vol.17 , No. 2.

Denis, A., Wixom, B.H. & Roth, R.M. (2006). *System Analysis and Design*. 3rd Ed. John Wiley & Son, USA.

Firkhan Ali, H. A. (2006). Isu Keselamatan Terhadap Teknologi Maklumat dan Komunikasi : Aktiviti Penggodaman Terhadap Rangkaian Komputer . In *Proceedings of the Seminar IT di Malaysia 2006*. Primula Beach Resort, Kuala Terengganu.

Firkhan Ali, H. A. & Maziah Na'aman (2006). Vulnerabality Assessment on the Network Security. In *Proceedings of the International Conference on Science and Technology 2006*. PWTC, Kuala Lumpur.

Gollmann, D. (2006). *Computer Security*. 2nd Ed. John Wiley & Son, England.

Herzog, P. (2006). Open Source Security Testing Security Methodology. Security Focus. http://www.securityfocus.com/columnists/395. (Date of access: 20 July 2008).

Herzog, P. (2006). OSSTMM – Open Source Security Testing Methodology Manual. http://www.isecom.info/mirror/osstmm.en.2.2.pdf. (Date of access: 20 July 2008).

Norton, P. & Stockman, M. (1999). *Peter Norton's Network Security Fundamentals*. SAMS Publishing.

Scambray, J., Mcclure, S. & Kurtz, G. (2001) *Hacking Exposed: Network Security and Solutions.* Osborne/McGraw-Hill.

Usdoj (2006). DOJ System Development Life Cycle Guiddance Chapter 1. http://www.usdoj.gov/jmd/irm/lifecycle/ch1.htm#para1.4 (Date of access: 13 September 2008).