SATU ANALISA KE ATAS KELEMAHAN-KELEMAHAN YANG MEMBOLEHKAN BERLAKUNYA KOMPROMI DI DALAM KESELAMATAN RANGKAIAN KOMPUTER

Firkhan Ali Hamid Ali, [1]Khairul Amin Mohd Sukri, [2]Mohamad Aizi Salamat & [3]Norsalina Monhadi
[1,2]Fakulti Teknologi Maklumat dan Multimedia,
Kolej Universiti Teknologi Tun Hussein Onn,
Beg Berkunci 101, 86400 Parit Raja,
Johor Darul Takzim.
firkhan@kuittho.edu.my, [1]khairulm@kuittho.edu.my, [2]aizi@kuittho.edu.my

[3]Sek.Men.Keb.Tun Aminah,
Jln Kluang, 83007 Batu Pahat,
Johor Darul Takzim
finfosecure@yahoo.co.uk

ABSTRAK
Kemungkinan wujudnya kompromi di dalam keselamatan rangkaian komputer boleh berlaku daripada kelemahan-kelemahan yang terdapat pada setiap nod di dalam sistem tersebut. Biasanya kelemahan-kelemahan ini wujud tanpa disedari kehadirannya secara nyata.Kelemahan-kelemahan ini boleh dikesan dan dianalisa terlebih dahulu sebelum ia dipergunakan oleh pihak yang tidak bertanggung jawab untuk menyerang sistem rangkaian komputer.Proses '*vulnerability scanning*' telah dilaksanakan di Fakulti Teknologi Maklumat dan Multimedia (FTMM), Kolej Univerisiti Teknologi Tun Hussein Onn (KUiTTHO) untuk mengenalpasti dan menganalisa kelemahan-kelemahan yang terdapat pada sistem rangkaian komputer [2]. Hasil daripada kajian tersebut, kelemahan-kelemahan yang wujud telah dianalisa dari segi jenis-jenis kemungkinan serangan, jenis-jenis data atau maklumat yang berkemungkinan rosak atau hilang dan jenis – jenis kelemahan yang merujuk kepada pengkompromian terhadap sistem rangkaian komputer tersebut terutama di FTMM, KUiTTHO.

PENGENALAN
Dewasa ini, kebanyakan organisasi di Malaysia termasuk di FTMM, KUiTTHO menghadapi suasana persekitaran digital yang amat sukar dari segi masalah keselamatan rangkaian komputer. Ianya berasaskan kepada berita, maklumat,laporan dan statistik yang telah disediakan oleh Kumpulan Reaksi Kecemasan Komputer Malaysia atau lebih dikenali sebagai MyCERT bagi masalah-masalah tersebut yang telah berlaku di Malaysia. Laporan tersebut juga boleh diperolehi menerusi halaman web MyCERT di www.mycert.org.my (Awas, 2004; DFCST, 2004)

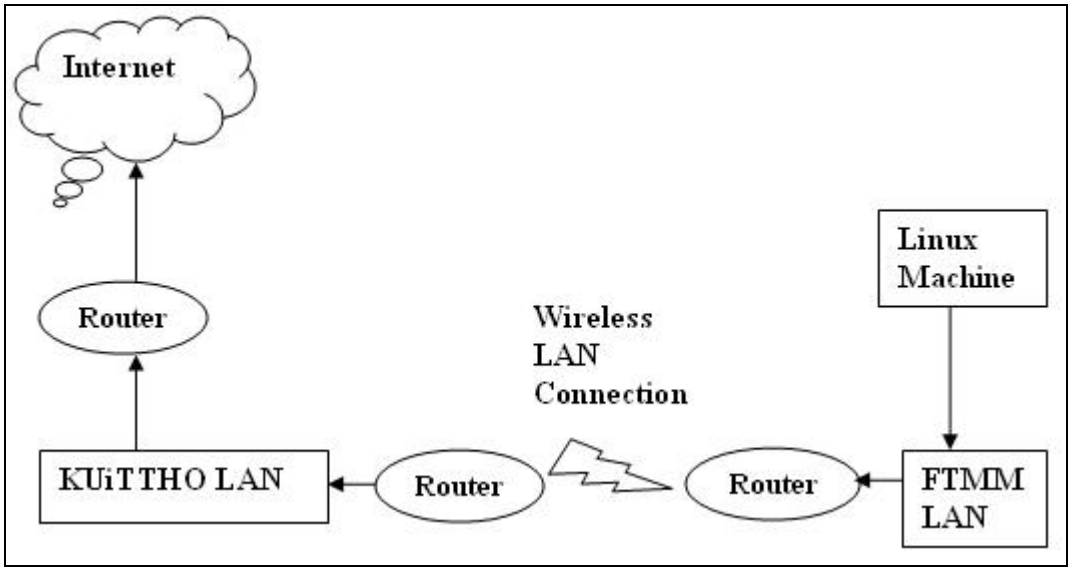
Di dalam keadaan kekalutan keselamatan di persekitaran digital ini menyebabkan prasarana teknologi maklumat dan perhubungan yang sedia ada dan diperlukan tidak dapat digunakan secara sepenuhnya atau sekiranya ia dapat digunakan hanya pada tahap yang paling minimum (O'Brien, 1998). Berlarutan daripada kesan ini juga boleh meyebabkan sesuatu proses kerja itu dilaksanakan di dalam keadaan yang amat perlahan dan kurang cekap. Seterusnya menyebabkan kualiti dan kuantiti yang diperlukan oleh organisasi pada tahap optimum akan menurun atau terganggu. Secara tidak langsung perkara ini akan meyebabkan ketidakjayaan strategi perniagaan bagi sesuatu organisasi tersebut. Kepentingan kajian ini sangat perlu di mana laporan daripada kajian ini digunakan sebagai asas yang kukuh untuk meyediakan panduan berguna secara meyeluruh bagi keselamatan di dalam sistem rangkaian komputer bagi sesebuah organisasi (Firkhan, 2005).

Dengan adanya panduan ini, kelemahan-kelemahan tersebut yang menyebabkan kemungkinan berlakunya kompromi di dalam keselamatan sistem rangkaian komputer dapat diurus dengan baik dan ianya berupaya dikurangkan ke tahap yang paling minimum. Di samping itu, secara khususnya, disediakan juga laporan analisa dari segi jemis-jenis kelemahan, jenis-jenis kemungkinan serangan dan jenis-jenis kemungkinan data atau informasi hilang. Perkara-perkara ini dibincangkan bertujuan untuk mengenalpasti potensi-potensi yang mewujudkan kemungkinan wujudnya kompromi di dalam sistem rangkaian komputer tersebut dengan lebih menyeluruh.

KAEDAH PERLAKSANAAN DAN PERKAKASAN

Perkaksasan yang diperlukan di dalam menjalankan kajian ini adalah satu stesen kerja atau satu set komputer bersama dengan perisian sistem pengoperasian Linux. Stesen kerja ini juga perlu dan telah dihubungkan di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Stesen kerja tersebut juga perlu digunakan sebagai tapak bagi melarikan perisian Nessus yang digunakan bagi melaksanakan tugas mengenalpasti kelemahan-kelemahan yang wujud di dalam sistem rangkaian komputer di FTMM,KUiTTHO (Introduction, 2004). Perisian Nessus merupakan perisian sumber terbuka dan perisian pelayan-pelanggan yang sangat terkenal di dalam melaksanakan proses 'vulnerability scanning' dengan baik dan cekap. Ia dipakejkan bersama dengan dua jenis perisian iaitu yang pertama digunakan sebagai perisian pelayan dan yang kedua digunakan sebagai perisian pelanggan (Northcutt, et al., 2003).

Jadi, perisian-perisian ini telah ditempatkan bersama di dalam stesen kerja komputer Linux tersebut. Pada mulanya, perisian pelayan Nessus perlu dan telah dilarikan terlebih dahulu secara berterusan bagi tujuan untuk mengenalpasti status keselamatan dan kehadiran kelemahan-kelemahan yang sedia ada di dalam sistem rangkaian komputer di FTMM, KUiTTHO tersebut (Demonstrations, 2004; Documentation, 2004). Bagi mendapatkan gambaran yang lebih jelas berkenaan dengan lokasi fizikal bagi perkakasan-perkakasan yang telah digunakan di dalam sistem rangkaian komputer tersebut, sila rujuk di dalam Rajah 1.

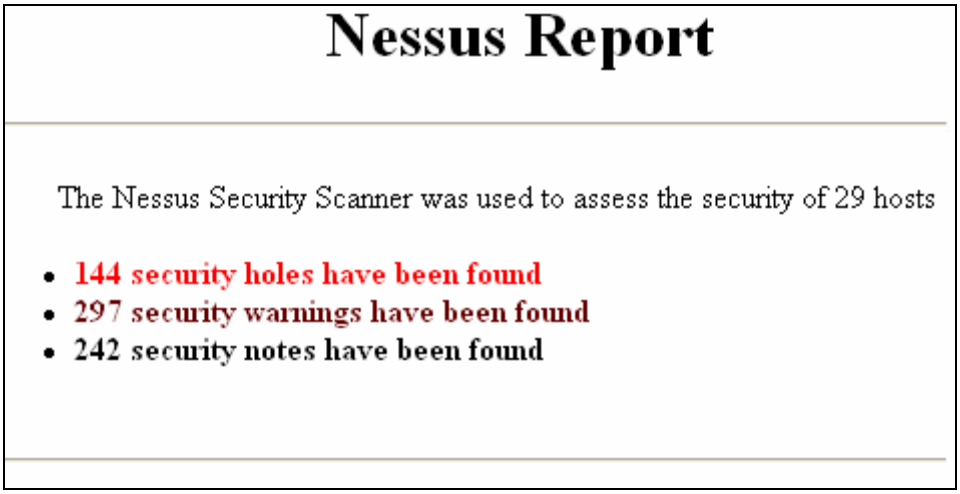


Rajah 1: Sistem rangkaian komputer di FTMM

Kemudian, selepas beberapa hari perisian pelayan Nessus dilarikan, perisian pelanggan Nessus pula telah dilarikan ke atas 255 buah alamat protokol Internet atau alamat IP yang wujud dan dipilih di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Setelah itu, apabila selesai sahaja perisisan Nessus melaksanakan proses mengenalpasti kelemahan-kelemahan yang terdapat di dalam setiap nod di dalam sistem rangkaian komputer ini, ia memaparkan satu laporan secara menyeluruh berkenaan dengan keputusan kelemahan-kelemahan yang wujud berserta dengan status tahap bahayanya di dalam sistem rangkaian komputer di FTMM, KUiTTHO.

ANALISA DAN HASIL KAJIAN

Hasil laporan dan keputusan yang diperolehi setelah melaksanakan 'vulnerability scanning' menggunakan perisian Nessus boleh dibahagikan kepada dua jenis laporan iaitu yang pertama, laporan berkenaan ditumpukan secara keseluruhan bagi semua nod di dalam sistem rangkaian komputer tersebut dan yang kedua, laporan berkenaan ditumpukan secara yang lebih fokus dan spesifik kepada setiap nod di dalam sistem rangkaian komputer tersebut. Bagi perlaksanaan tujuan kajian ini, laporan keputusan bagi keseluruhan sistem rangkaian komputer tersebut lebih banyak diperlukan dan digunakan untuk dianalisa. Laporan keputusan secara keseluruhan untuk kesemua nod yang aktif di dalam sistem rangkaian komputer tersebut boleh dirujuk kepada Rajah 2.



Rajah 2: Laporan oleh Nessus bagi keseluruhan sistem rangkaian komputer

Rajah 2 menunjukkan laporan berkenaan dengan tahap keselamatan nod-nod yang dipilih dan aktif di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Berdasarkan kepada Rajah 2, terdapat 29 buah nod yang aktif daripada 255 buah alamat protokol Internet atau alamat IP yang telah dikenalpasti oleh perisian Nessus. Kemudian, daripada 29 buah nod tersebut, terdapat sebanyak 144 kelemahan – kelemahan yang telah wujud atau 'security holes' di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Di samping itu, terdapat juga sebanyak 297 amaran keselamatan dan sebanyak 242 nota keselamatan bagi keseluruhan 29 buah nod yang aktif tersebut. Kelemahan-kelemahan yang telah wujud atau 'security holes' merupakan satu keadaan di mana kelemahan-kelemahan itu boleh digunapakai terus oleh pihak yang tidak bertanggung jawab untuk mengkrompomi keselamatan di dalam sistem rangkaian komputer. Amaran keselamatan pula merujuk kepada situasi keselamtan nod tersebut yang berkemungkinan boleh menjadi kelemahan-kelemahan yang boleh digunapakai terus di dalam menyerang sistem rangkaian komputer tersebut. Nota keselamatan adalah merupakan maklumat berkaitan dengan situasi bagi nod tersebut seperti maklumat berkenaan dengan port yang terbuka, perkhidmatan yang wujud dan lain-lain.

Aktiviti mengenalpasti kelemahan-kelemahan ini oleh perisian Nessus melibatkan port-port yang terbuka bersama dengan perkhidmatan-perkhidmatan dan aplikasi-aplikasi yang wujud bagi setiap nod yang aktif di dalam sistem rangkaian komputer tersebut (Scambray et al., 2001; Stallings, 2000). Kelemahan-kelemahan ini adalah merupakan agen penting yang membolehkan berlakunya kompromi ke atas keselamatan di dalam sistem rangkaian komputer (Norton & Stockman, 1999). Berdasarkan kepada perkara tersebut, kajian ini lebih fokus dan menumpukan kepada analisa terhadap kelemahan-kelemahan itu sendiri yang meliputi sebanyak 144 kelemahan bagi keseluruhan 27 nod yang aktif di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Bagi mengenalpasti kewujudan kelemahan-kelemahan ini bagi setiap nod di dalam rangkaian komputer, perisian pelayan Nessus mengandungi lebih daripada 7 000 jenis percontohan yang merujuk kepada jenis kelemahan-kelemahan yang lebih spesifik di dalamnya (Plugins, 2005).Terdapat 33 jenis kumpulan kelemahan-kelemahan yang ditakrifkan secara lebih umum seperti Windows, 'Gain root Remotely' dan lain-lain bagi keseluruhan, lebih daripada 7 000 jenis percontohan tersebut.

Berdasarkan kepada keputusan yang telah diperolehi, terdapat 47 jenis kelemahan yang lebih spesifik daripada 144 kelemahan yang telah dijumpai bagi keseluruhan nod di dalam sistem rangkaian komputer tersebut. Sekiranya ia merujuk kepada jenis kumpulan yang lebih umum pula, lebih daripada 80 peratus kelemahan-kelmahan ini adalah berada di dalam kumpulan jenis Window dan selebihnya pula adalah 'Gain Root Remotely', 'CGI Abuses' dan pelbagai (Top 20 Exploits, 2004).

Jenis Kemungkinan Serangan

Bagi kesemua 144 kelemahan yang telah dijumpai, ianya boleh disalahgunakan oleh pelbagai pihak yang tidak bertanggung jawab dengan menggunakan kelemahan-kelemahan ini dengan tujuan untuk mengkompromi keselamatan di dalam sistem rangkaian komputer. Jadi, serangan ke atas sistem rangkaian komputer ini berkemungkinan boleh berlaku secara serangan dari dalam, serangan dari luar atau kedua-duanya sekali.

Apabila berlaku serangan dari dalam, ianya bermaksud kelemahan tersebut boleh disalahgunakan dari dalam sistem rangkaian komputer tersebut sahaja berbanding dengan serangan dari luar yang bermaksud kelemahan tersebut hanya boleh disalahgunakan dari luar sistem rangkaian komputer tersebut. Namun begitu, sekiranya kelemahan-kelemahan ini boleh disalahgunakan untuk tujuan serangan dari luar, berkemungkinan besar ianya boleh digunakan untuk tujuan serangan dari dalam. Kemudian, sekiranya berlaku satu keadaan seperti di mana si penyerang menggunakan perkhidmatan telnet untuk memasuki secara sah atau tidak sah ke dalam nod tersebut dan seterusnya memulakan serangannya menerusi perkhidmatan telnet tersebut, ia dikategorikan sebagai serangan dari dalam kerana serangan tersebut tidak secara terus kepada nod atau sistem rangkaian komputer tersebut tetapi ia memasuki sistem itu terlebih dahulu sebagai pengguna.

Jadi, menerusi Jadual 1 yang berikut didapati bahawa sebanyak 78 kelemahan yang melibatkan kemungkinan serangan dari luar, sebanyak 17 kelemahan yang melibatkan kemungkinan serangan dari dalam dan sebanyak 49 kelemahan yang melibatkan kedua-dua jenis kemungkinan serangan tersebut daripada 144 kelemahan yang telah diperolehi, Dengan ini, keterdedahan yang melibatkan kemungkinan serangan dari luar adalah lebih tinggi berbanding yang lain.

Jadual 1: Jenis kemungkinan serangan

Jenis Serangan	Bilangan Kelemahan
Serangan dari Luar	78
Serangan dari Dalam	17
Serangan dari Dalam dan Luar	49

Jenis Kemungkinan Keselamatan Rangkaian Komputer Dikompromi

Jenis kemungkinan keselamatan rangkaian komputer boleh dikompromi bagi keseluruhan 144 kelemahan yang diperolehi berserta dengan bilangan kelemahan yang terlibat boleh dirujuk kepada Jadual 2 yang berikut:

Jadual 2: Jenis kemungkinan keselamatan rangkaian komputer dikompromi

Jenis Pengkompromian Keselamatan	Bilangan Kelemahan
Perihal ada	30
Kerahsiaan	7
Kesempurnaan	52
Perlindungan Keselamatan/Kebenaran	55

Berdasarkan kepada Jadual 2, elemen kerahsiaan tidak melibatkan jumlah kelemahan yang tinggi berbanding dengan elemen lain seperti perihal ada, kesempurnaan dan perlindungan keselamatan/kebenaran. Seterusnya di dalam elemen kerahsiaan dan kesempurnaan, ia melibatkan sesuatu perkara atau situasi di mana bagaimana untuk mendapatkan atau megubahsuaikan maklumat atau data yang diperolehi menerusi pengkompromian tersebut. Manakala bagi elemen perihal ada dan perlindungan keselamatan/kebenaran pula, ia melibatkan situasi di mana bagiamana untuk mendapatkan maklumat/data tersebut atau penghalanagan terus kebolehcapaian maklumat/data tersebut.

Pendedahan Terhadap Sistem Komponen

Kajian ini menunjukkan bahawa terdapat beberapa jenis sistem komponen yang terlibat sebagai tempat kepada 144 kelemahan ini bertapak dan ia boleh dirujuk kepada Jadual 3 seperti yang dipaparkan berikutnya:

Jadual 3: Jenis sistem komponen yang mengandungi kelemahan

Jenis Sistem Komponen	Bilangan Kelemahan
Sistem Pengoperasian	40
Protokol Timbunan Rangkaian	9
Aplikasi Pelayan	4
Aplikasi Bukan Pelayan	33
Perkakasan	13
Protokol Komunikasi	44
Modul enkripsi	1
Lain-lain	0

Berdasarkan kepada maklumat yang diperolehi daripada Jadual 3, kebanyakan kelemahan ini wujud dengan kadar kuantiti yang besar di dalam komponen sistem pengoperasian, protokol komunikasi dan

aplikasi bukan pelayan. Daipada pemerhatian yang dijalankan pula, terdapat lebih 80 peratus sistem komponen ini adalah merujuk kepada kelemahan bagi persekitaran Windows atau berfungsi di dalam persekitaran tersebut. Bagi komponen aplikasi bukan pelayan pula, ia ljuga didapati lebih merujuk kepada perisian yang digunakan oleh pengguna biasa seperti Internet Explorer, Macromedia Flash, Microsoft Visual Basic dan lain-lain yang juga turut digunakan di dalam persekitaran Windows di mana ia mempunyai tahap keselamatan yang amat rendah. Jadi, proses pemasangan dan perlaksanaan bagi setiap perisian bukan pelayan tersebut perlu dilaksanakan dengan lebih teliti terutama dari segi aspek keselamatan seperti konfigurasi perisian, penampungan perisian dan lain-lain [16].

CADANGAN

Berdasarkan kepada pemerhatian yang telah dibuat daripada kajian tersebut terutama menerusi laporan yang telah disediakan oleh persian Nessus, terdapat beberapa langkah yang perlu dilaksanakan sama ada tindakan tersebut diambil secara aktif atau proaktif. Bagi tindakan yang aktif, semua cadangan yang telah dikemukakan oleh perisian Nessus perlu di ambil kira, dianalisa dan dilaksanakan secepat yang mungkin berdasarkan kepada keutamaannya. Kemudian, tindakan secara proaktif pula sangat penting untuk dilaksanakan bagi mewujudkan kesinambungan di dalam perlaksanaan yang baik dan cekap untuk keselamatan sistem rangkaian komputer tersebut (Lindholm, 2001).

Antara amalan secara umum yang perlu dilaksanakan bagi memastikan keselamatan rangkaian komputer berada di dalam keadaan yang baik adalah seperti (1) menyediakan polisi keselamatan rangkaian komputer yang baik dan teliti di dalam organisasi, (2) proses pemasangan aplikasi perlu dilaksana dengan baik dengan mengambilkira penampalannya, pepijat dan pembaiki keselamatan, (3) tutup kesemua port dan perkhidmatan yang tidak diperlukan bagi setiap nod di dalam sistem rangkaian komputer tersebut, (4) proses pemasangan dan konfigurasi sistem pengoperasian dan perkakasan seperti firewall, router dan lain-lain perlu dilaksana dengan baik dengan mengambilkira penampalannya, pepijat dan pembaiki keselamatan. Elakkan daripada pemasangan secara 'default', (5) sentiasa melaksanakan pengauditan dan penilaian di dalam keselamatan rangkaian komputer dan (6) sentiasa melaksanakan kemaskini penampalan, pepijat dan pembaiki keselamatan bagi mana-mana perisian, sistem pengoperasian, komponen-komponen di dalam rangkaian dan sebagainya.

KESIMPULAN

Keselamatan di dalam sistem rangkaian komputer telah dan akan terus menghadapi situasi-situasi yang amat mencabar pada masa akan datang. Kesemuanya memerlukan titik pertemuan dan penyelesaian yang sangat mantap bagi menghadapi setiap jenis risiko dan kekangan yang diterima. Walaubagaimanapun, kunci utama bagi kejayaan perlaksanaan keselamatan di dalam sistem rangkaian komputer ini adalah sangat bergantung kepada kesesuaian dan keserasian dengan misi, objektif, polisi dan amalan di dalam organisasi tersebut (Reynolds, 2003). Menerusi keputusan kajian yang telah dijalankan didapati terdapat 47 jenis kelemahan yang berjumlah 144 bagi kesemuanya yang telah dijumpai di dalam 27 nod yang aktif di dalam sistem rangkaian komputer di FTMM, KUiTTHO. Dengan ini, keputusan tersebut boleh dinisbahkan dengan satu nod mengandungi 5 kelemahan ataupun 1:5.

Penggunaan perisian Nessus di dalam kajian ini telah menghasilkan satu keputusan yang sangat bernilai bagi menganalisa tahap keselamatan di dalam sistem rangkaian komputer. Ini disebabkan oleh situasi kelemahan-kelemahn ini adalah sama dengan situasi di mana pintu dan tingkap sesuatu rumah itu ditutup dan dikunci dengan tidak sempurna. Situasi ini boleh mengundang pelbagai anasir luar yang tidak sihat untuk cuba memasuki rumah tersebut. Begitulah andaian yang dibuat kepada kelemahan-kelemahan yang wujud di dalam perlaksanaan elemen keselamatan di dalam sistem rangkaian komputer. Perlaksanaan kajian telah dijalankan di dalam julat yang dipilih dan tertentu sahaja disebabkan oleh keterbatasan dari segi waktu dan sumber tenaga. Namun begitu, hasil daripada kajian ini adalah sangat penting dan bernilai untuk dilaksanakan bagi meningkatkan lagi tahap sensitiviti masyarakat di FTMM, KUiTTHO terhadap elemen keselamatan di dalam sistem rangkaian komputer. Dengan ini ia boleh dilaksanakan secara meyeluruh dan berterusan di masa hadapan sama ada di peringkat fakulti atau universiti dengan tahap pengetahuan dan kesedaran yang tinggi di kalangan kakitangan KUiTTHO.

RUJUKAN

Awas (2004). Awas! Pencerobohan laman web besar-besaran. http://www.mycert.org.my/news/2004_01_28_01.html

Amit Klein, 'Ethical Hacking Techniques to Audit and Secure Web-Enabled Applications http://www.SanctumInc.com/pdf/Ethical_Hacking_Technique.pdf

DFCST. 2004. Definition for Common Security Terms. http://www.mycert.org.my/securityterm.html

Demonstrations. (2004). http://www.nessus.org/demo/index.html
Documentation. (2004). http://www.nessus.org/decomentation.html
Firkhan Ali B. Hamid Ali. (2005). An Analysis of Possible Network Security Compromises in the Computer Network: A Case Study of FTMM,KUiTTHO Paper presented at the ICKM 2005 Conference, PWTC, 7-9 Julai.
Introduction. (2004). http://www.nessus.org/intro.html
Kane, J., Lindholm, C. (2001). *Cisco Networking Academy Program: First Year Companion Guide*. (2nd Edition), Cisco Press.
Norton, P and Stockman, M. (1999). *Peter Norton's Network Security Fundamentals*. SAMS Publishing.
Northcutt, S., Zeltser, L., Winters, S., Frederick, K.K. and Ritchey, R.W. (2003*). Inside Network Perimeter Security: The Definitive Guide to Firewalls*,. VPNs, Routers and Intrusion Detection Systems, New Riders.
O'Brien, J.A. (1998). *Managing Information Systems*. (4th Edition), Mc Graw-Hill.
Plugins. (2005). http://www.nessus.org//plugins/plugins.html
Reynolds,G (2003). *Ethics in Information Technology*. Boston: Thompson Course Technology
Scambray, J., Mcclure, S. & Kurtz G. (2001). *Hacking Exposed: Network Security and Solutions*. Osborne/McGraw-Hill.
Stallings, W. (2000) *Network Security Essentials: Application and Standards*. Prentice Hall.
Tipton, H.F. and Krause, M. (2000) *Information Security Management Handbook.* (4th Edition), Auerbach Publications.
Top 20 Exploits. (2004). http://www.sans.org/top20/index.php