Vulnerability Testing pada Sistem Administrasi Rumah Sakit X

David Harjowinoto[1], Agustinus Noertjahyana[2], Justinus Andjarwirawan [3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131, Surabaya 60236
Telp (031) – 2983455, Fax. (031) - 8417658
davidharjowinoto@gmail.com[1], agust@petra.ac.id[2], justin@petra.ac.id [3]

ABSTRAK

Perkembangan Rumah Sakit X semakin besar dan memiliki berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya. Rumah Sakit X sendiri telah memiliki *server* untuk mendukung kegiatan operasionalnya, terutama sistem administrasi yang berisi mengenai data-data pasien. Dengan adanya ketersediaan jaringan di Rumah Sakit X, baik melalui *WiFi* maupun kabel *Ethernet*, maka perlu diperhatikan keterkaitannya antara jaringan dengan *server* dan para *hacker*. Oleh karena adanya permasalahan tersebut maka kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan pemantauan pada sistem administrasi dan melakukan *vulnerability testing.*

Berdasarkan latar belakang permasalahan itu, maka dibutuhkan evaluasi dengan menggunakan metode *vulnerability*/*penetration testing.* Selain itu, penelitian ini juga menggunakan pedoman dari modul *CEH (Certified Ethical Hacker), Acunetix, dan CISSP (Certified Information Systems Security Professional)*. Pengujian skripsi ini adalah bertujuan untuk menemukan kelemahan sistem administrasi pada Rumah Sakit X yang ada. Beberapa masalah yang ditemukan setelah pengujian, cukup banyak dimana setiap kelemahan yang ada mempunyai penanganan yang berbeda, keamanan fisik server yang lemah, dan *port* yang seharusnya tidak terbuka menjadi terbuka.

Solusi yang diberikan untuk mengatasi permasalahan tersebut antara lain*:* penggunaan standar acunetix dan *CISSP* sebagai solusi terhadap kelemahan yang ada, melakukan *maintenance* secara berkala terhadap hardware, software, maupun jaringan, melakukan *filter port* yang ada, meningkatkan tingkat keamanan *server*, dan melakukan pengujian keamanan secara rutin dan berkala, baik dengan berkonsultasi kepada bidang terkait maupun menggunakan suatu panduan (seperti acunetix, CEH, CISSP).

Kata Kunci: *Penetration Testing, Vulnerability Testing, Certified Ethical Hacker, Sistem Administrasi, Rumah Sakit*

ABSTRACT

The development and growth of Hospital X is getting bigger and bigger, and has information system in running their operational activities. Hospital X itself has a server to support its activities, especially the administration system which contains data about their patients. With the availability of the network at the Hospital X, either through Wi-Fi or an Ethernet cable, therefore it should be noted the bonds between networks and servers. Furthermore it is an important need nowadays to help minimize and anticipate the hacking crimes of the existing servers. One of the things that can be done is to monitor the administration and conduct vulnerability testing.

Based on the background of the problem, it is necessary to evaluate server and network security using the vulnerability / penetration testing. In addition, this study also uses the guidelines of the CEH (Certified Ethical Hacker), Acunetix, and CISSP (Certified Information Systems Security Professional) modules. The testing of this thesis aims to find weaknesses in the administration system at Hospital X. Some problems were discovered after testing, which each of the weaknesses has different handling or treatment, physical security server weak, and unused opened ports that should not be open.

The solution offered to solve these problems, are: the use of Acunetix and CISSP as a standard network security as the solution to anticipate weaknesses, to perform maintenance on a regular basis for the hardware, software, and network, to filter the existing port, to increase the level of security of the server, and to test security regularly and periodically, either through consultation with the related field experts or using a guide (like Acunetix, CEH, and CISSP).

Keywords: *Penetration Testing, Vulnerability Testing, Certified Ethical Hacker, Administration System, Hospital.*

1. PENDAHULUAN

Rumah Sakit merupakan institusi untuk merawat orang yang sakit, yang pelayanannya disediakan oleh dokter, perawat, dan tenaga ahli kesehatan lainnya. Saat ini telah banyak rumah sakit yang menggunakan teknologi dan sistem informasi yang telah berkembang, khususnya media penyimpanan maupun pusat data, atau disebut sebagai *server* dalam kegiatan sehari-hari. Namun seiring dengan perkembangan teknologi tersebut, keamanan merupakan aspek yang perlu diwaspadai oleh setiap pihak yang memiliki skema sistem terpusat, karena pembobolan, manipulasi, maupun kehilangan data dapat terjadi jika dilakukan oleh para *hacker* yang memang berniat mengambil data sensitif dari sebuah instansi, terutama dalam hal ini rumah sakit.

Perkembangan Rumah Sakit X semakin besar dan memiliki berbagai macam sistem informasi dalam menjalankan kegiatan operasionalnya. Rumah Sakit X sendiri telah memiliki *server* untuk mendukung kegiatan operasionalnya, terutama sistem administrasi yang berisi mengenai data-data pasien. Dengan adanya ketersediaan jaringan di Rumah Sakit X, baik melalui *Wi-Fi* maupun kabel *Ethernet*, maka perlu diperhatikan keterkaitannya antara jaringan dan *server* dari para *hacker*.

Oleh karena adanya permasalahan tersebut maka kebutuhan yang penting saat ini adalah membantu meminimalisir dan mengantisipasi *server* yang ada dari kejahatan *hacking*. Salah satu hal yang dapat dilakukan adalah dengan melakukan pemantauan pada sistem administrasi dan melakukan *vulnerability testing*.

2. LANDASAN TEORI

2.1 Keamanan *Server*

Tidak ada *server* komputer yang benar-benar aman. Sebuah *server* membutuhkan sistem jaringan untuk berkomunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan dapat disalahgunakan. Sistem keamanan membantu mengamankan *server* dan jaringannya tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus. Selain itu, pastikan bahwa *user* dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang dibuat. Jika tidak memahami hal tersebut, maka harus menciptakan suatu lubang (*hole*) keamanan pada jaringan yang ada.

Keamanan komputer, dalam hal ini *server* meliputi beberapa aspek antara lain [3]:

1. *Confidentiality. Confidentiality attack* adalah pencegahan dalam menjaga informasi dari orang yang tidak berhak dan tidak berkepentingan untuk mengakses.
2. *Integrity. Integrity* adalah upaya pencegahan terhadap informasi yang tidak boleh diubah dan dihapus tanpa seijin pemilik informasi.
3. *Availability. Availability* adalah upaya pencegahan ditahannya informasi atau sumber daya terkait oleh mereka yang tidak berhak dimana berhubungan dengan ketersediaan informasi ketika dibutuhkan.
4. Non-*repudiation. Non-repudiation* merupakan hal yang yang bersangkutan dengan pengirim yang melakukan transaksi dan penerima. Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi
5. *Authentication. Authentication* adalah suatu langkah untuk menentukan atau mengonfirmasi bahwa pengirim suatu informasi yang ada dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu. Melakukan autentikasi terhadap sebuah objek adalah melakukan konfirmasi terhadap kebenarannya, sedangkan melakukan autentikasi terhadap seseorang biasanya adalah untuk memverifikasi identitasnya, dengan kata lain informasi tersebut benar-benar dari orang yang dikehendaki

2.2 *Hacking*

Pada dasarnya ada tiga jenis *hacker* tergantung pada *domain* dari pekerjaan seseorang. Adapun beberapa *hacker* itu antara lain [3]:

1. *White hat hacker*, merupakan orang yang menulusuri atau memecah sistem keamanan komputer untuk tujuan yang tidak berbahaya. Tujuan-tujuan ini berkisar pada pengujian sistem keamanan untuk menemukan celah besar dalam jaringan. Orang-orang seperti biasanya mengikuti cara yang sah dan bekerja dalam wilayah hukum *cyber*.
2. *Black hat hacker*. *Black hat hacker* umumnya menumbangkan keamanan komputer tanpa otorisasi dengan bantuan berbagai *virus* dan *hacking tools* lainnya. *Hacker* ini menggunakan teknologi untuk penipuan vandalisme, kartu kredit, atau pencurian identitas.
3. *Grey hat hacker*. *Grey hat hacker* merupakan bagian pertengahan jalan antara *black hat hacker* dan *white hat hacker*.

2.3 *Vulnerability Testing/Penetration Testing*

Vulnerability Testing merupakan metode untuk mengevaluasi keamanan sistem komputer atau jaringan dengan mensimulasikan serangan dari sumber yang berbahaya. Hal ini dapat diberikan contoh seperti serangan yang dilakukan oleh *black hat hacker*, *cracker*, *defacer*, dan sebagainya.

Tujuan *vulnerability testing* adalah untuk menentukan dan mengetahui serangan-serangan yang bisa terjadi terhadap kerentanan yang ada pada sistem, mengetahui dampak bisnis yang diakibatkan dari hasil ekpoitasi yang dilakukan oleh penyerang.

Tipe untuk melakukan suatu *vulnerability testing* ada 2 macam [8]. Kedua macam itu antara lain:

1. *External Testing. External Testing* adalah *testing* dengan melakukan analisa terhadap informasi *public* yang tersedia, *network enumeration phase*, dan analisa keamanan *devices* yang digunakan.
2. *Internal Testing. Internal Testing* adalah *testing* yang akan menampilkan jumlah *network access points* yang mewakili beberapa *logical* dan *physical segment*.

Ada beberapa metode untuk melakukan *Vulnerability testing* yang bisa digunakan [8], antara lain:

1. *Passive Vulnerability testing*. Dalam hal ini yang dilakukan adalah melakukan pemetaan dan pengujian terhadap kontrol yang ada didalam *web application*, *login*, dan konfigurasinya, sehingga dapat memetakan target sistem.
2. *Active Vulnerability testing. Active Vulnerability testing* merupakan melakukan kegiatan aktif dalam pengujian terhadap keamanan sistem dengan melakukan manipulasi *input*, pengambilan hak akses, dan melakukan pengujian terhadap *vulnerability* yang sudah ada.
3. *Aggressive Vulnerability testing. Aggressive Vulnerability testing* adalah melakukan eksploitasi terhadap *vulnerability*, melakukan *reverse enginering* terhadap *software* dan *system*, menanamkan *backdoor*, mengunduh *code*, dan mencoba mengambil alih finansial dan informasi yang ada di *server*.

Pada Tabel 1 dapat dilihat langkah-langkah *penetration testing*/*vulnerability testing* yang dilakukan dalam skripsi ini. Langkah-langkah ini juga dilengkapi dengan *objective* dan metodologi atau teknik apa yang digunakan dari setiap *step* yang ada.

Tabel 1. Langkah-langkah penetration testing

NO.	***STEP***	***OBJECTIVE***
1	***Footprinting***	*Gather target information*
2	***Enumeration and Scanning Networks***	*Identification valid user accounts.*
3	***System Hacking***	*Hacking the system*

2.4 *CISSP (Certified Information System Security Professional)*

CISSP merupakan sertifikasi professional di bidang keamanan sistem informasi yang tidak mengacu kepada produk tertentu (*neutral vendor*) dan mencakup seluruh aspek keamanan mulai dari manajemen keamanan informasi, keamanan fisik hingga yang sangat teknis seperti cara kerja protokol jaringan dan algoritma enkripsi *asynchronous* [2].

2.5 *CEH (Certified Ethical Hacker)*

CEH merupakan salah satu sertifikasi *IT Security*, dimana seseorang yang memegang sertifikat tersebut bertanggung jawab seumur hidup terhadap ilmu yang sudah dia miliki. Masing-masing pemegang sertifikat mempunyai *unique number* yang sudah terdaftar atas namanya. Seorang *CEH certified* biasanya dipercaya untuk mengelola jaringan atau sistem komputer menggunakan metode yang sama dengan metode seorang *hacker*.

2.6 *Angry IP Scanner*

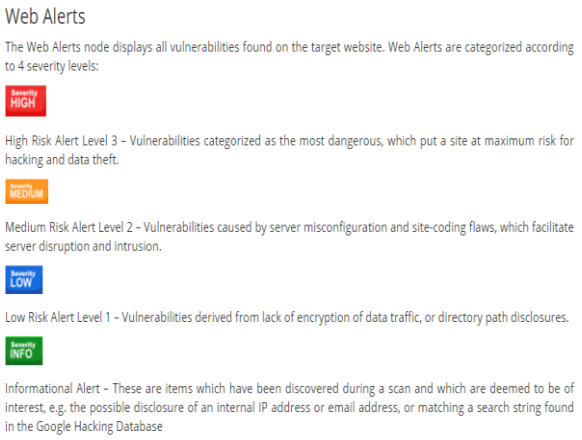
Angry IP Scanner adalah *software* yang berfungsi untuk mendeteksi, melacak dan memonitor alamat *ip* dalam sebuah jaringan. Dengan *Angry IP Scanner*, *user* dapat mengetahui alamat *ip, pingtime, hostname, TTL, MAC address, NetBIOS info*.

2.7 *Acunetix*

Keamanan *website* mungkin aspek yang paling diabaikan saat ini. Padahal mengamankan perusahaan harus menjadi prioritas utama dalam setiap organisasi. *Hacker* berkonsentrasi mengusahakan upaya mereka pada aplikasi berbasis *web* (seperti *shopping cart*, *forms*, *login page*). *Web applications* dapat diakses 24 jam sehari, 7 hari seminggu dan bertugas untuk mengontrol data berharga karena *web applications* mempunyai akses langsung, seperti *database* pelanggan. *Web application* sering dibuat namun kurang dilakukan pengujian sehingga lebih mungkin mempunyai kerentanan yang kurang diperhatikan. Acunetix Web Vulnerability Scanner otomatis memeriksa *web application* terhadap *SQL Injection , XSS*, dan kerentanan *web* lainnya.

Tool Acunetix Web Vulnerability Scanner 9.5 yang digunakan pada skripsi ini juga dapat menampilkan level dari hasil *scanning* [1].

Pada Gambar 1 dapat dilihat *severity levels* dari acunetix yang akan menjelaskan tingkat keamanan dari *URL* atau *IP address* yang di-*scan.*



Gambar 1 Level *tool* Acunetix [1]

3. ANALISA DAN DESAIN SISTEM

3.1 Analisa Permasalahan

Vulnerability testing server sistem administrasi Rumah Sakit X ini memang diperlukan. Hal ini dikarenakan *server* sistem administrasi tersebut memegang peranan yang sangat penting di Rumah Sakit X.

Vulnerability testing server ini dilakukan dengan tujuan untuk mengetahui *vulnerability* yang ada. Dari *range IP address* yang di-*scanning*, nantinya akan diketahui *IP address* yang mempunyai *NetBIOS info* dan yang tidak mempunyai *NetBIOS info*. Setelah itu, dari *NetBIOS info* yang ada, dapat diketahui *IP address* server Rumah Sakit X. Selanjutnya, *IP address* tersebut akan di-*scanning* lagi dengan *tools* berbeda untuk melihat kelemahan yang dimiliki. Hasil dari *scanning* ini akan ditembus. Laporan ini nantinya dapat memberikan evaluasi kepada pengelola jaringan komputer Rumah Sakit X untuk lebih waspada lagi terhadap kelemahan yang ada.

3.2 Analisa Sistem

Dalam skripsi ini, program aplikasi (*tool*) yang digunakan adalah program yang sesuai dengan langkah *penetration testing*. *Tool* yang digunakan ada yang didapatkan melalui cara *download* dari *internet* maupun dari buku *CEH* (*Certified Ethical Hacker*) sendiri. Pada Tabel 2 dapat dilihat sistem (*tool*) yang digunakan untuk *penetration testing* dalam pengerjaan skripsi.

Tabel 2 Tabel *tool* yang digunakan untuk skripsi

NO.	*STEP*	*TOOLS*
1	***Footprinting*** [4]	Angry IP Scanner
2	***Enumeration and Scanning Networks*** [5] [6]	Acunetix Web Vulnerability Scanner 9.5
3	***System Hacking*** [7]	Windows Explorer, Microsoft SQL Server Management Studio 2012, dan program SIMRS X

3.3 Metodologi *Vulnerability Testing*

Pada skripsi ini digunakan beberapa metodologi *vulnerability testing* [8]. Adapun beberapa metodologi yang digunakan dalam skripsi ini adalah sebagai berikut:

1. *Information Gathering. Information gathering* merupakan salah satu dari langkah utama dalam melakukan *vulnerability testing.* Metodologi ini merupakan fase pertama dalam melakukan *vulnerability testing* dan dilakukan dengan menggunakan berbagai macam *tools, scanners, online resource*, mengirim *http* sederhana, dan lain-lain.

2. *Vulnerability Analysis. Vulnerability Analysis* merupakan metode untuk mengidentifikasi *vulnerability* dalam suatu *network*. Metodologi ini menyediakan ringkasan dari beberapa celah atau *flaw* dari sistem atau *network.*

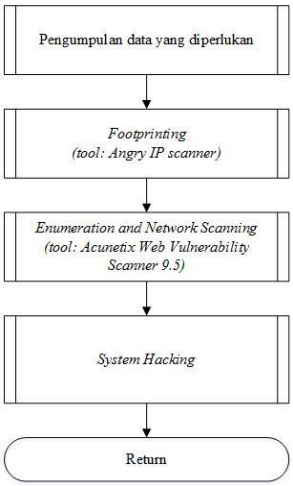
3. *External Vulnerability/Penetration Testing. External vulnerability* testing dijalankan untuk mengetahui apakah *external network* tersebut aman atau tidak. Di dalam *external*

vulnerability testing, hacking dilakukan dengan cara yang sama dengan seseorang yang melakukan *attack* tetapi sama sekali tidak membahayakan *network.*

4. *Social Engineering. Social Engineering* adalah sebuah metode serangan yang digunakan oleh penyerang untuk mendapatkan informasi krusial dari sebuah perusahaan, biasanya dengan kontak langsung dengan target, secara verbal, maupun informasi mengenai target yang ditemukan dimanapun.

3.4 Alur Pengujian

Pada Gambar 2 dapat dilihat *flowchart* pengerjaan jurnal. Pertama, *user* harus melakukan koneksi dengan *WiFi* dan melakukan autentikasi. Selanjutnya *user* dapat melakukan *vulnerability testing* untuk melakukan pengumpulan data.



Gambar 2 Langkah-langkah pengerjaan *vulnerability testing*

4. PENGUJIAN SISTEM

4.1 *Footprinting*

Footprinting merupakan metode untuk mendapatkan informasi sebanyak mungkin mengenai target.

4.1.1 Physical (Environmental) Security

Setiap *vulnerability* diberikan solusi sebagai berikut [2]:

1. Pintu ruang *server* yang selalu terbuka. Pintu di ruang *server* harus ditutup dengan tujuan agar hanya orang yang berkepentingan yang dapat keluar masuk ruang *server.*
2. Terdapat barang-barang selain *server* sistem administrasi Rumah Sakit X. Barang-barang yang tidak berhubungan dengan *server* sistem administrasi diletakkan di tempat sesuai dengan fungsinya
3. *Air conditioner* yang mengalami kebocoran. Dilakukan *maintenance* terhadap *Air conditioner* sesuai dengan periode tertentu yang ditentukan oleh pihak Rumah Sakit X.
4. Hanya terdapat *smoke detector*, namun tidak ada alat pemadam api. Seharusnya di sebuah ruangan *server* diberi fasilitas pemadam api, seperti *water sprinkler*, atau penyemprot karbondioksida supaya api dapat sesegera mungkin terdeteksi dan dapat dipadamkan secara cepat sehingga *server* tidak mengalami kerusakan.

4.1.2 Angry IP Scanner

Setelah melakukan autentikasi koneksi *WiFi* dengan menggunakan *IP static* dan mengetahui topologi *network* Rumah Sakit X, langkah selanjutnya yang dilakukan yaitu melakukan *scan IP address* yang memiliki *range* 192.168.20.0 sampai 192.168.20.255 dengan menggunakan *Angry ip Scanner* untuk mengetahui detail siapa saja yang terkoneksi dalam jaringan sesuai dengan topologi *network* Rumah Sakit X.

Berikut hasil *scanning range ip* 192.168.20.0 sampai dengan 192.168.20.255 seperti yang tertera pada Tabel 2.

Table 2. Tabel *tool yang digunakan untuk skripsi*

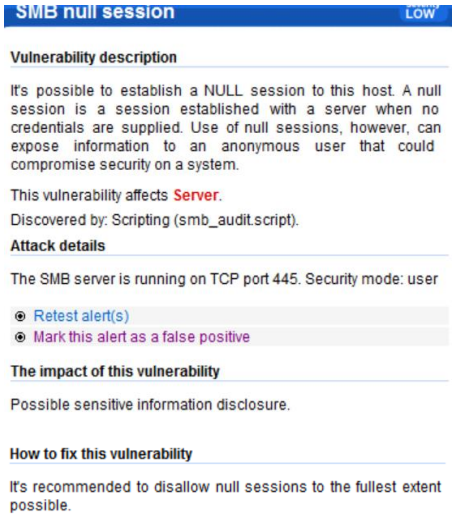
No.	*IP*	*NetBIOS Info*
1	*192.168.20.10*	*SERVERSOTH0\FO-SOTH*
2	*192.168.20.11*	*SERVERSOTH0\OPERATOR-SOTH*
3	*192.168.20.15*	*SERVERSOTH0\LABORAT-SOTH*
4	*192.168.20.16*	*SERVERSOTH0\KASIR_RJ-SOTH*
5	*192.168.20.17*	*SERVERSOTH0\FARMASI-SOTH*
6	*192.168.20.19*	*SERVERSOTH0\LOGISTIK-SOTH*
7	*192.168.20.22*	*SERVERSOTH0\NSTATIONRJ-SOTH*
8	*192.168.20.23*	*SERVERSOTH0\KEUANGAN-SOTH*
9	*192.168.20.25*	*SERVERSOTH0\ADMINLOGISTIK-S*
10	*192.168.20.71*	*SERVERSOTH0\OPERASI-SOTH*
11	*192.168.20.73*	*SERVERSOTH0\SEKRETARIS-SOTH*
12	*192.168.20.74*	*SERVERSOTH0\KEUANGAN4-SOTH*
13	*192.168.20.77*	*SERVERSOTH0\DIKLAT-SOTH*
14	*192.168.20.78*	*SERVERSOTH0\HRD_2-SOTH*
15	*192.168.20.79*	*SERVERSOTH0\JOHN-PC*
16	*192.168.20.80*	*SERVERSOTH0\HRD-SOTH*
17	*192.168.20.83*	*SERVERSOTH0\KEUANGAN2-SOTH*
18	*192.168.20.85*	*SERVERSOTH0\DIRUT-SOTH*
19	*192.168.20.86*	*SERVERSOTH0\KASIRRI-SOTH*
20	*192.168.20.89*	*SERVERSOTH0\KASIR-SOTH*
21	*192.168.20.101*	*WORKGROUP\SIRS-PC*
22	*192.168.20.103*	*WORKGROUP\ADIT*
23	*192.168.20.116*	*WORKGROUP\DAVE*

No.	IP	NetBIOS Info
24	192.168.20.119	SERVERSOTH0\RADIOLOGI-SOTH
25	192.168.20.210	WORKGROUP\WEBSERVER
26	192.168.20.212	WORKGROUP\SMIKROTIK
27	192.168.20.215	SERVERSOTH0\SERVERSOTH

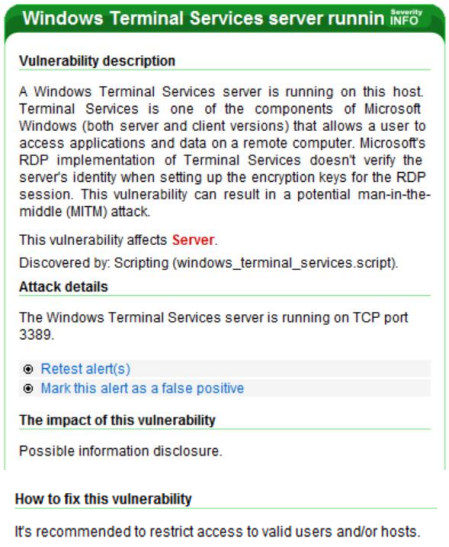
4.2 *Enumeration and Scanning Networks*

4.2.1 Acunetix Web Vulnerability Scanner 9.5

Gambar 3 dan 4 menunjukkan solusi yang diberikan *Acunetix* untuk hasil pemindaian celah *ip address* 192.168.20.210 yang memiliki *threat level 1: low* dengan 1 peringatan tingkat rendah, 1 peringatan informasi, dan 8 *port* yang terbuka akan di bahas pada bagian *system hacking.*



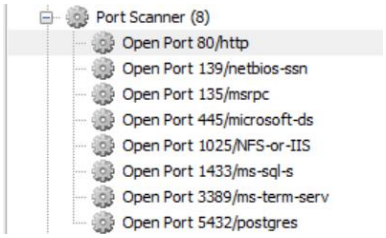
Gambar 3 Peringatan Tingkat Rendah



Gambar 4 Peringatan Tingkat Informasional

4.3 *System Hacking*

Dari kelemahan-kelemahan yang telah ditemukan pada langkah sebelumnya, yaitu *enumeration and scanning networks*,akan digunakan untuk masuk ke dalam *server* [7] dan dibahas kelemahan-kelemahan yang ditemukan. Kelamahan-kelemahan tersebut ditemukan karena adanya *port-port* yang terbuka seperti yang ditampilkan pada Gambar 5.



Gambar 5 *Port* yang Terbuka

4.3.1 Windows File Explorer

Pada langkah *footprinting* didapatkan *list ip address* yang sedang aktif seperti yang terlihat pada Tabel 5.1. Dari tabel tersebut didapatkan *ip address server*, yaitu 192.168.20.210 dan *IP address* komputer SIRS (Sistem Informasi Rumah Sakit) PC, yaitu 192.168.20.101. *Windows Explorer* di dalam langkah ini digunakan untuk masuk ke dalam *file sharing* komputer-komputer tersebut, yang memanfaatkan *port 139* dan *port 445*.

IP 192.168.20.210 tidak dapat ditembus dan sudah aman. *IP* 192.168.20.101 dapat ditembus dan diambillah program SIMRS(Sistem Informasi Manajemen Rumah Sakit) X.

4.3.2 Microsoft SQL Server Management Studio 2012

Microsoft SQL Server Management Studio 2012 digunakan untuk masuk ke dalam *database* sistem administrasi Rumah Sakit X menggunakan *port 1433/ms-sql-s* untuk mendapatkan *credential username* dan password pada program SIMRS X.

Untuk masuk kedalam *database* dilakukan *social engineering attack* untuk mendapatkan *username* dan *password SQL Server Management Studio 2012.*

Setelah masuk, ditemukan tabel User_Login yang dapat mengakses program SIMRS. Kemudian dilakukan query untuk melihat isi tabel tersebut. *SELECT TOP 1000 [Kode_UserLogin],[Username],[Password],[KPassword],[Jabatan],[Department] FROM [SOTH].[dbo].[User_Login]*

Dapat dilihat pada Gambar 6 tampilan isi table *User_Login*

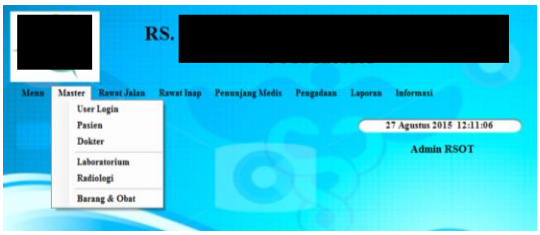
Gambar 6 Tampilan isi Tabel *User_Login*

Dari kelemahan yang ditemukan, solusi yang diberikan yaitu terhadap *Social Engineering attack*, berupa penemuan kertas yang berisikan *credential* untuk masuk ke dalam *Microsoft SQL Server Management Studio.* Solusi dari celah tersebut yaitu menyimpan *credential administrator* di tempat yang aman, letakkan di tempat dimana karyawan lain tidak dapat melihat *credential* tersebut.

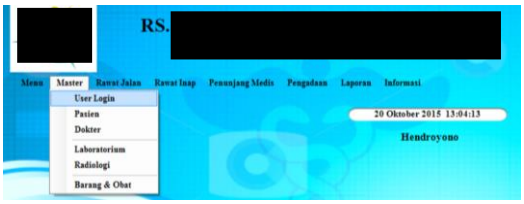
4.3.3 Program SIMRS X

Credential user yang ditemukan, digunakan untuk masuk ke dalam Program SIMRS X untuk menemukan vulnerability pada hak akses *user-user*nya.

Tampak pada Gambar 7 dan Gambar 8 *Privilege* akses *Staff IT* sama dengan *Administrator*.



Gambar 7 Tampilan Hak Akses Administrator



Gambar 8 Tampilan Hak Akses *Staff IT*

Dari beberapa hak akses *user* yang ditemukan, terdapat permasalahan dimana hak akses *user staff IT* sama dengan *administrator*. *Chapter2 Domain 2: Access Control* [2] dalam keamanan komputer pada bagian *Accountability*, setiap user diberikan *policy least privilege and need to know*. Dalam kelemahan ini, *access control* lemah pada bagian administratif.

Solusi dari kelemahan ini yaitu dengan melakukan *limit access control* terhadap beberapa *user* sesuai dengan kebutuhan dan kapasitas kerja dan melakukan tindakan *corrective control*, yaitu membenahi sistem yang sudah ada.

4.3.4 Solusi Unused Opened Ports

Langkah *system hacking* yang telah dilakukan adalah dengan menggunakan *port-port* yang terbuka. Berdasarkan *Chapter 7 Domain 7: Telecommunications and Network Security* [2], *port* dibuka agar dapat terjadi komunikasi. Namun membuka semua *port* bukan jalan yang tepat untuk menghasilkan komunikasi yang bagus, tetapi dengan melakukan *filter port* yang ada dengan tujuan hanya *port-port* yang digunakan saja yang dapat diakses. Selain melakukan *filter port* perlu dilakukan *authentication protocol*

5. KESIMPULAN

Berdasarkan dari semua yang telah dilakukan selama pengerjaan skripsi, dapat disimpulkan beberapa hal, antara lain:

1. Kelemahan *physical security* yang ditemukan tidak direkomendasikan untuk sebuah ruangan *server* karena rentan terhadap orang luar yang masuk ke dalam ruang server dan mengambil perangkat keras yang ada, serta rentan terhadap *disaster* seperti kebakaran dan terkena air.
2. *Vulnerability testing* dengan menggunakan *Acunetix Web Vulnerability Scanner 9.5* menghasilkan kelemahan dan dijelaskan dengan detail. Selain itu juga dibagi berdasarkan tingkat level kelemahannya. Berikut level kelemahan yang terbagi pada Acunetix.
   - *Low* : *SMB Null Session*
   - *Informatioal* :*Terminal Services server running*
3. Tidak ditemukannya kelemahannya *SQL Injection* menandakan bahwa database server sistem administrasi Rumah Sakit X aman terhadap serangan SQL injection yang berdampak pada diambilnya data-data, terutama data pasien yang ada pada Rumah Sakit X.
4. Terbukanya beberapa *port* yang tidak sesuai dengan fungsinya. Hal ini dapat menyebabkan adanya celah yang dapat dimanfatkan untuk diserang.
5. Rumah Sakit X masih rentan terhadap serangan *social engineering* yang mengakibatkan didapatkannya informasi-informasi yang dapat digunakan oleh *hacker* untuk masuk ke dalam sistem.
6. Tidak adanya proteksi *credentials user* pada fitur *network file sharing* yang dapat diakses oleh umum.
7. Beberapa hak akses *user* terhadap program SIMRS X tidak sesuai pada kapasitas kerja karyawan tersebut.

6. DAFTAR PUSTAKA

[1] Acunetix. 2015. *Analyzing the Scan Results*. URI= http://www.acunetix.com/support/docs/wvs/analyzing-scan-results/

[2] Conrad, E. 2011. *Eleventh Hour CISSP Study Guide*. Amerika: SYNGRESS

[3] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 01 *Introduction to Ethical Hacking*. Amerika: EC-Council.

[4] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 02 *Footprinting and Reconnaissance*. Amerika: EC-Council

[5] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 03 *Scanning Networks*. Amerika: EC-Council.

[6] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 04 *Enumeration*. Amerika: EC-Council.

[7] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 05 *System Hacking*. Amerika: EC-Council.

[8] EC-Council. 2012. *Certified Ethical Hacker* v8: *Module* 20 *Penetration Testing*. Amerika: EC-Council.