

ANALISIS VULNERABILITAS HOST PADA KEAMANAN JARINGAN KOMPUTER DI PT. SUMEKS TIVI PALEMBANG (PALTV) MENGGUNAKAN ROUTER BERBASIS UNIX

Zaid Amin
STMIK PalComTech Palembang

Abstract

Network security is one of the important and fundamental in the utilization of a system. a weakness (vulnerability) in a computer network system is often ruled out, until the event of an attack or logic physic that damage to the system, the impact will be more bad and very costly, cost recovery it will become bloated beyond previous estimates. Analysis vulnerability in the form of audit reports, which in turn serve as benchmark for the design implementation of computer network security more secure the preventive measures are systematic, and installation and maintenance costs are low, because operating system, and tools based on open source.

Keywords : Vulnerability, Network Security, Audit Reports.

PENDAHULUAN

Keamanan jaringan komputer merupakan salah satu hal penting dan mendasar dalam pemanfaatan sebuah sistem. Suatu kelemahan (vulnerabilitas) dalam sebuah sistem jaringan komputer seringkali dikesampingkan, hingga apabila terjadi suatu ancaman /serangan *logic* maupun *physic* yang merusak pada sistem tersebut, dampaknya akan menjadi lebih buruk dan sangat merugikan, biaya pemulihan (*recovery*) justru akan menjadi membengkak diluar perkiraan sebelumnya. Pertimbangan akan bahaya dan kerugian penyalahgunaan servis-servis jaringan lokal dan semua aplikasi berbasis internet saat ini, maka sudah seharusnya para pelaku bisnis dan organisasi menerapkan suatu strategi langkah awal untuk menanggulanginya. Salah satu bentuk yang ditempuh diantaranya adalah melakukan sebuah analisis secara periodik, baik itu *logic* dan *physic*, sehingga nantinya diharapkan dari analisis tersebut menghasilkan suatu laporan audit yang berisi deteksi dari berbagai macam vulnerabilitas yang ada, untuk kemudian diambil langkah-langkah proteksi yang tepat, yang diperlukan sebagai jaminan keamanan untuk keberlangsungan sistem tersebut.

LANDASAN TEORI

Pengertian Analisis

Analisis adalah “suatu cara membagi-bagi, melepaskan, atau menguraikan suatu subjek ke dalam komponen-komponen” (Kusmayadi, 2008:35).

Pengertian Jaringan Komputer

Jaringan komputer adalah sekumpulan komputer beserta mekanisme dan prosedurnya yang saling terhubung dan berkomunikasi. Komunikasi yang dilakukan oleh komputer tersebut dapat berupa *transfer* berbagai data, instruksi, dan informasi dari satu komputer ke computer lainnya (Ramadhan, 2006 :2).

Konsep Keamanan Komputer

Sebuah sistem yang aman (*secure system*) diasumsikan sebagai sebuah sistem dimana seorang *intruder* harus mengorbankan banyak waktu, tenaga, dan biaya besar yang tak dikehendakinya dalam rangka penyerangan tersebut, atau resiko yang harus dikeluarkan sangat tidak sebanding dengan keuntungan yang akan diperoleh (Rafiudin, 2002:2).

Kebutuhan keamanan untuk sebuah system komputer berbeda-beda bergantung pada aplikasi-aplikasi yang dikandungnya, sistem transfer keuangan elektronik, akan berbeda kebutuhannya dengan sistem reservasi atau sistem-sistem kontrol lainnya. Begitupun juga ketersediaan dana si pemilik sistem turut melahirkan variasi-variasi tingkat keamanan. Kesimpulannya, tidak ada jaminan apakah suatu sistem dapat dikatakan *secure* atau *reliable*. Namun, keamanan dapat ditingkatkan dalam skala berkelanjutan dari 0 hingga 1, atau dari kondisi tidak *secure* menjadi relatif *secure*.

Kebijakan Keamanan Komputer (*Security Policy*)

Kebijakan keamanan (*security policy*) adalah suatu set aturan yang menetapkan hal-hal apa saja yang diperbolehkan dan apa saja yang dilarang terhadap penggunaan atau pemanfaatan akses pada sebuah system selama operasi normal. Penetapan kebijakan keamanan (*security policy*) ini hendaknya ditulis secara *detail* dan jelas. Tugas dan penetapan *security policy* biasanya merupakan keputusan politis dari manajemen perusahaan.(Rafiudin, 2002:2).

Analisa ancaman adalah sebuah proses *audit* di mana semua kemungkinan penyerangan terhadap system diidentifikasi secara cermat. Sebuah catatan yang memuat semua daftar kemungkinan penyalahgunaan dan gangguan terhadap sistem hendaknya dibuat sebagai basis peringatan.



Gambar 1. Rule Security Policy

Penerapan kebijakan aturan-aturan *security policy* *hendaknya* dilakukan secara sistematis dengan terlebih dahulu melakukan sebuah analisis awal, baik itu analisis terhadap instalasi fisik maupun *logic*, meliputi: audit dan penyeimbangan antara ongkos proteksi *system* dengan resiko-resiko yang ditimbulkan, barulah kemudian dilakukan implementasi mekanisme-mekanisme *security* yang telah dirancang tersebut, sebagai contoh mekanisme *access control* yang menerangkan objek-objek mana saja yang diizinkan untuk diakses publik dan mana yang tidak.

Sekilas Tentang *Tool Nessus*

Nessus adalah termasuk kelompok *scanner* gratis baru. Ditulis oleh Renaud Deraison saat berusia 18 tahun dan ia berasal dari Paris. Renaud sudah familiar dengan sistem operasi linux sejak usia 16 tahun, dan ia sangat tertarik dengan bidang isu-isu *security* komputer. *Nessus* didistribusikan di bawah *GNU Public License* dari *Free Software Foundation*. Renaud memulai untuk mengkonsep *linux* pada permulaan tahun 1998, adapun karakter daripada aplikasi *Nessus* adalah :

Scanner Type : TCP Port Scanner

Author : Renaud Deraison

Language : C

Build Platform : Linux

Target Platform : UNIX, Multiple

Requirements : Linux, UNIX, C

Nessus bekerja dengan memeriksa target yang anda telah anda tentukan, seperti sekumpulan *host* atau bisa juga *host* dalam fokus tersendiri. Begitu aktivitas *scan* selesai, anda dapat melihat informasi hasilnya baik dalam bentuk grafikal atau baris, *Interface* (tampilan) grafikal *Nessus* dibangun dengan menggunakan *Gimp Toolkit* (gtk). *Gtk* adalah sebuah *library* gratis yang banyak digunakan untuk membangun *interface* grafikal dibawah X. Alasan kenapa kebanyakan *Administrator Security Computer* memilih *Nessus* adalah karena distribusi aplikasi ini selalu *up to date* (selalu diperbarui), berbasis *web interface*, mudah dioperasikan dan gratis (Rafiudin, 2002:350).

Tenable Network Security, Inc. adalah sekelompok organisasi yang berwenang menulis dan membangun aplikasi *Nessus Security Scanner*. Dan secara konsisten organisasi ini pun terus mengembangkan aplikasi ini. *Tenable* dalam hal ini menulis hampir semua fasilitas *Plugin* yang tersedia saat ini, seperti khususnya untuk membantu aktifitas *Scanner* sesuai dengan kebutuhan dan kebijakan audit yang semakin luas.

Suatu kebijakan atau *Policy* yang ditentukan pada aplikasi *Nessus* mendukung beberapa teknik pilihan konfigurasi, pilihan-pilihan ini meliputi:

1. Adanya parameter yang mengontrol aspek-aspek teknik pemindaian, seperti efisiensi penggunaan waktu (*timeouts*), jumlah banyaknya *host*, tipe pemindaian *port* dan lain-lain.
2. Keamanan untuk pemindaian jaringan lokal, seperti protocol IMAP atau Autentikasi berbasis aplikasi *Kerberos*.
3. Pemeriksaan kebijakan dalam penggunaan *database*, seperti deteksi pemindaian pada servis, dan lain-lain.

Ada empat bagian konfigurasi pada menu *Policies*, diantaranya adalah: **General, Credentials, Plugins dan Preferences**. Adapun penjelasan terhadap bagian-bagian konfigurasi di atas adalah :

a. General

Bagian *General* berfungsi untuk memberikan penamaan suatu kebijakan (*policy*) dan memberikan beberapa teknik konfigurasi terhadap pemindaian yang sedang berlangsung.

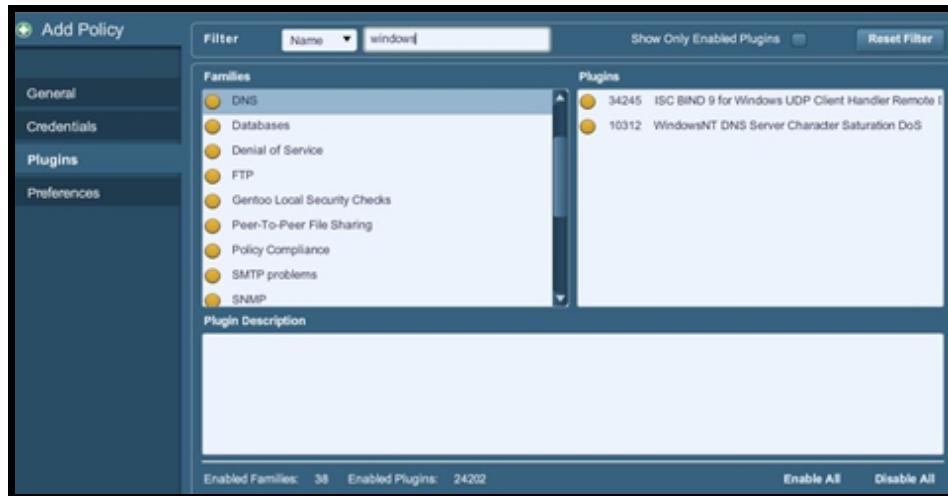
b. Credentials

Pada bagian *tab Credentials* kita dapat menambah konfigurasi keamanan seperti autentikasi kata kunci atau *password* pada protocol SMB (*service messages block*), *domain name*, kata kunci protokol *SSH* di sepanjang proses pemindaian, dengan memberikan

konfigurasi pada tab *Credentials*, kita akan mendapatkan hasil pemindaian dan pemeriksaan yang semakin akurat dan beragam.

c. Plugins

Pada pilihan *tab plugin* pengguna dapat memilih secara spesifik jenis-jenis *plugin* yang dibutuhkan, pilihan menu *plugin* ini akan membantu anda di dalam mengkategorikan jenis-jenis serangan, maupun vulnerabilitas yang sering terjadi saat ini, baik itu terhadap servis yang sedang dijalankan, *port-port* yang sebaiknya tidak terbuka, kerentanan suatu sistem operasi, *bug* atau celah keamanan pada *platform* perangkat-perangkat tertentu dan jenis-jenis varian virus terbaru saat ini.

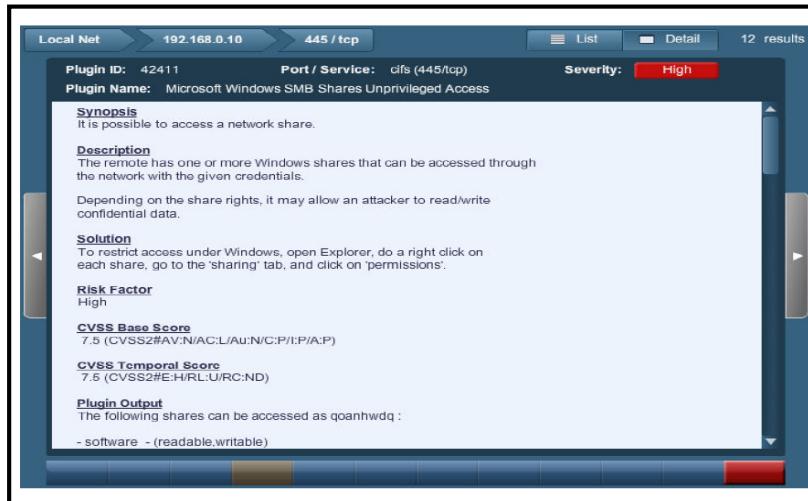


Gambar 2. Plugins dan PreferencesNessus

Di bawah ini beberapa jenis laporan yang akan terlihat, apabila target *host* yang telah anda *scan* terdapat suatu vulnerabilitas di dalamnya, apakah itu mengenai servis yang mencurigakan, terbukanya port yang dapat mengakibatkan penyusup untuk dapat melakukan eksplorasi, dan lain-lain akan dijelaskan pada gambar berikut :

LAN Scan		192.168.0.10	445 / tcp	List	Detail	13 results
Plugin ID	Name		Port	Severity		
10396	Microsoft Windows SMB Shares Access		cifs (445/tcp)	High		
26919	SMB guest account for all users		cifs (445/tcp)	Medium		
10397	SMB LanMan Pipe Server browse listing		cifs (445/tcp)	Low		
10859	SMB get host SID		cifs (445/tcp)	Low		
10860	SMB use host SID to enumerate local users		cifs (445/tcp)	Low		
10395	SMB shares enumeration		cifs (445/tcp)	Low		
11011	SMB Detection		cifs (445/tcp)	Low		
10394	SMB log in		cifs (445/tcp)	Low		
10785	SMB NativeLanMan		cifs (445/tcp)	Low		
23974	SMB Share Hosting Office Files		cifs (445/tcp)	Low		
10400	SMB accessible registry		cifs (445/tcp)	Low		
10428	SMB fully accessible registry		cifs (445/tcp)	Low		
26920	SMB NULL session		cifs (445/tcp)	Low		

Gambar 3. Tampilan pada menu Reports

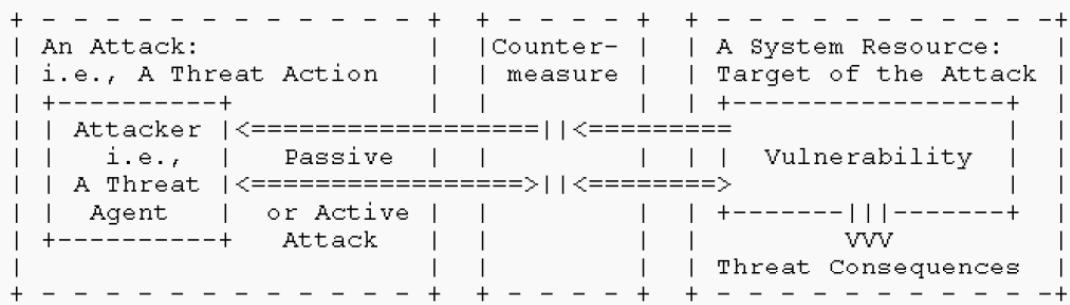


Gambar 4. Tampilan Pada Menu Reports Detail

Pengertian Dasar Vulnerabilitas

Sebuah vulnerabilitas adalah suatu poin kelemahan dimana suatu sistem rentan terhadap serangan. Sebuah ancaman (*threats*) adalah suatu hal yang berbahaya bagi keberlangsungan system (Lehtinen, Russel & Gangemi Sr, 2006:12).

Ada tiga kata kunci yang timbul dan saling berkaitan apabila kita mendiskusikan mengenai isu-isu daripada kemanan komputer, yaitu: vulnerabilitas, ancaman (*threats*), dan tindakan pencegahan (*countermeasures*). Bahaya tersebut dapat berupa manusia (*a system cracker or a spy*), suatu peralatan yang rusak, atau sebuah kejadian seperti kebakaran dan banjir, yang mungkin dapat mengeksploitasi kerentanan suatu sistem. Semakin banyak vulnerabilitas dan ancaman yang dapat terjadi di dalam suatu sistem, sudah seharusnya semakin tinggi pula kesadaran kita untuk dapat memproteksi sistem dan informasi yang berada di dalamnya. Sebuah teknik untuk melindungi suatu sistem dinamakan dengan tindakan pencegahan (*countermeasures*) (Lehtinen, Russel & Gangemi Sr, 2006:12).



Gambar 5. Diagram Vulnerabilitas

1. Vulnerabilitas yang berkaitan dengan alam (*Natural Vulnerabilities*)

Pada jaringan komputer *server* dan *workstation* di PT.Sumeks Tivi Palembang Penulis menemukan adanya vunerabilitas yang berkaitan dengan penempatan posisi perangkat terhadap ketika terjadinya bencana alam seperti gempa bumi atau getaran keras yang dapat mengakibatkan benturan dan jatuhnya perangkat keras tersebut lalu menimbulkan suatu arus pendek listrik yang pada akhirnya memicu bahaya kebakaran seperti di bawah ini:



Gambar 6. Natural Vunerabilities

2. Vulnerabilitas Emanasi (*Emanation Vulnerabilities*)

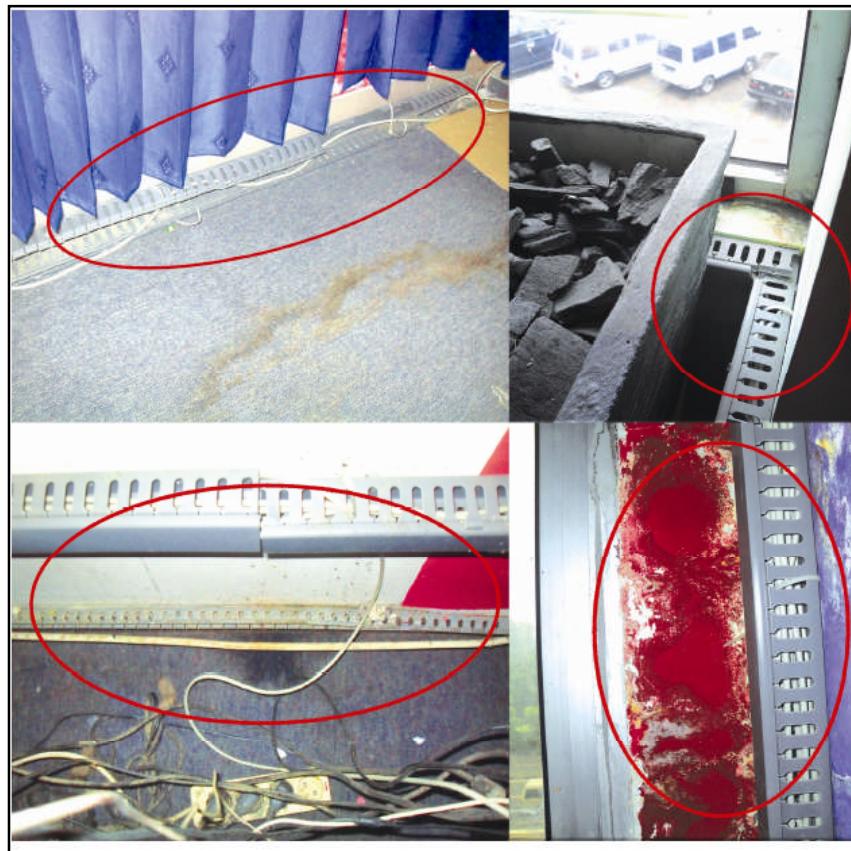
Sesuai dengan fungsinya yaitu untuk membawa aliran bit data dari satu komputer ke komputer yang lain, maka dalam pengiriman data sangatlah memerlukan media transmisi (kabel UTP) yang *reliable* atau terpercaya. Adanya *Electrical Noise* seperti sinyal elektromagnetik yang ditimbulkan oleh aliran listrik yang tidak stabil dapat menimbulkan *throughput* yang tidak maksimal terhadap proses lalu lintas pertukaran data tersebut. Interferensi dari sinyal yang berkompetisi dalam band frekuensi yang saling tumpang tindih dapat mengubah / menghapus sinyal. Interferensi dapat disebabkan karena emanasi yang keluar dari kabel yang berdekatan.



Gambar 7. Emanation Vulnerabilities

3. Vulnerabilitas Media (*Media Vulnerabilities*)

Kabel UTP merupakan suatu penghantar data dan informasi yang umumnya sering dipakai dalam penerapan jaringan komputer, penempatan instalasi kabel UTP yang baik harus memperhatikan beberapa faktor kerentanan dan kemanan, agar struktur bahan kabel tidak mudah rusak dan pada akhirnya mengganggu lalu lintas pertukaran data, kerentanan tersebut diantaranya adalah, pergantian suhu yang terlalu ekstrim disekitar kabel, gangguan binatang pengerat dan pemasangan kabel yang tidak rapih sehingga mampu menimbulkan kesan estetika yang tidak baik pada suatu ruangan atau bangunan. Di bawah ini memperlihatkan beberapa kerentanan kerusakan yang akan terjadi di PT. Sumeks Tivi Palembang apabila tidak ada tindak lanjut seperti perawatan terhadap ase-taset jaringan komputer yang ada.



Gambar 8. Media Vulnerabilities

Instalasi *plugin* dan *copy file nessus-fetch.rc* dan *all-2.0.tar.gz* dengan konfigurasi seperti berikut ini:

```
# cp nessus-fetch.rc /usr/local/nessus/etc/nessuss  
# cp all-2.0.tar.gz /usr/local/nessus/sbin  
# /usr/local/nessus/sbin/nessus-update-plugins all-  
2.0.tar.gz
```

```
imulya# cp nessus-fetch.rc /usr/local/nessus/etc/nessus/
imulya# cp all-2.0.tar.gz /usr/local/nessus/sbin/
imulya# /usr/local/nessus/sbin/nessus-update-plugins all-2.0.tar.gz
Expanding all-2.0.tar.gz...
Done. The Nessus server will restart when its scans are finished
imulya#
```

Gambar 9. Instalasi *plugin* dan file konfigurasi *Nessus*

Setelah instalasi selesai (memerlukan waktu beberapa menit) kemudian dilakukan percobaan untuk menjalankan aplikasi *Nessus* dengan menjalankan perintah sebagai berikut;

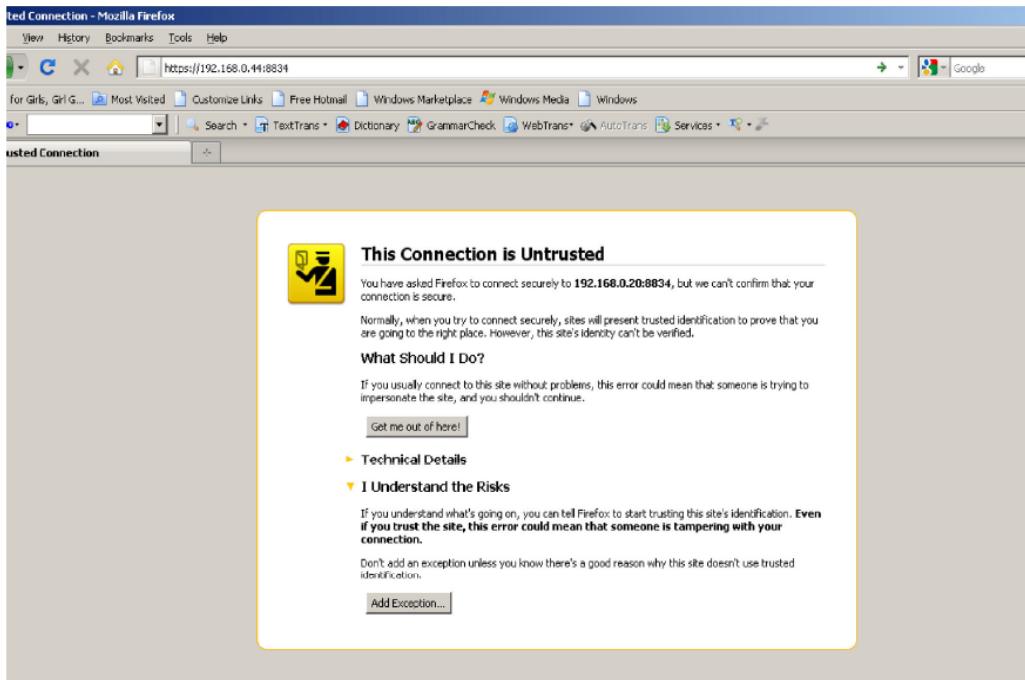
```
# /usr/local/etc/rc.d/nessusd.sh start Nessus  
(Mengaktifkan servis Nessus)
```

```
# /usr/local/etc/rc.d/nessusd.sh stop Nessus  
(Mematikan servis Nessus)
```

```
# top  
(Melihat apakah servis Nessus telah berjalan)
```

```
last pid: 1209; load averages: 0.11, 0.09, 0.06 up 0+03:37:45 23:08:03
21 processes: 1 running, 20 sleeping
CPU: 29.7% user, 8.0% nice, 6.0% system, 1.1% interrupt, 63.2% idle
Mem: 35M Active, 147M Inact, 46M Wired, 7272K Cache, 34M Buf, 3668K Free
Swap: 1144M Total, 1144M Free
■
  PID USERNAME THR PRI NICE  SIZE   RES STATE      TIME  WCPU COMMAND
1208 root      3 -8    0 33156K 30632K biord  0:04 24.71% nessusd
1209 root      1 44    0 3504K 1324K RUN   0:00  0.10% top
607 root      1 44    0 5864K 2224K select  0:00  0.00% sendmail
668 root      1 20    0 3488K 1904K pause  0:00  0.00% csh
617 root      1 8     0 3200K 1008K nanslp 0:00  0.00% cron
478 root      1 44    0 3172K 980K select  0:00  0.00% syslogd
660 root      1 8     0 3612K 1256K wait   0:00  0.00% login
611 smmsp     1 20    0 5864K 2216K pause  0:00  0.00% sendmail
432 root      1 44    0 1888K 416K select  0:00  0.00% devd
667 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
663 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
666 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
665 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
1207 root     1 8     0 3200K 736K wait   0:00  0.00% nessus-service
639 root      1 96    0 3228K 908K select  0:00  0.00% inetd
661 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
662 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
664 root      1 5     0 3172K 856K ttyn   0:00  0.00% getty
```

Gambar 10. Output servis Nessus Daemon telah berjalan



Gambar 11. Servis Nessus yang telah aktif

Setelah Penulis memberikan satu *sample* (contoh) di atas mengenai bagaimana keadaan salah satu *host* yang telah dilakukan *scanning*, maka di bawah ini secara keseluruhan saya uraikan keterangan beberapa *reports* tersebut dalam bentuk gambar dari beberapa *sample host* yang telah selesai dilakukan proses *Scanning (completed)*:

Name	Status	Last Updated
AUDIT HOST REDAKSI PALTV	Completed	Jan 13, 2011 17:44
AUDIT HOST AIRBOX PALTV	Completed	Jan 13, 2011 17:27
AUDIT HOST HRD PALTV	Completed	Jan 13, 2011 17:09
AUDIT HOST STUDIO PALTV	Completed	Jan 13, 2011 16:45
AUDIT SERVER PALTV	Completed	Jan 13, 2011 16:28

Gambar 12. Tampilan Log Reports (*Completed*)

Adapun beberapa keterangan *reports* beberapa *sample host* tersebut adalah sebagai berikut :

1. Host server.paltv.tv

a. Keterangan status High pada host server.paltv.tv :

Uraian dan Solusi :

Pada *host server.paltv.tv* yang juga bertindak sebagai *web server*, versi PHP yang digunakan terpengaruhi oleh beberapa kelemahan, yaitu menurut informasi dari *banner*

(identitas keterangan antarmuka aplikasi), versi PHP yang terinstall pada *host* tersebut adalah dibawah versi 5.2.14, dimana versi ini meliputi beberapa isu-isu kerentanan sebagai berikut :

1. Adanya *bug* (celah) kesalahan yang dapat mengakibatkan permintaan pada sesi XML-RPC (*Remote Procedure Call*) tidak akan mengarah kemana pun (*Null*), apabila ini terjadi maka apabila ada permintaan dari *client* (khususnya mengenai pemetaan/list alamat link) pada protocol HTTP akan terganggu/tidak berjalan.
2. Adanya fungsi dari perintah '*fnmatch*' yang dapat menyebabkan kerusakan ketika adanya perintah *recursive* yang berulang-ulang, contohnya pada penerapan variabel string yang panjang (*long string*).
3. Sebuah kesalahan penggunaan kapasitas memori yang berlebihan terjadi pada fungsi daripada perintah '*substr_replace*'. Adapun solusi terbaik untuk vulnerabilitas ini adalah melakukan *upgrade* (pembaruan) terhadap versi PHP yang dipakai menjadi versi 5.2.14 atau yang paling terbaru saat ini.

Port	Protocol	SVC Name	Total	High	Medium	Low	Open Port
0	tcp	general	8	0	0	8	0
0	udp	general	1	0	0	1	0
53	udp	dns	2	0	0	2	0
57	udp	booops?	1	0	0	1	0
135	tcp	epmap	1	0	0	1	0
137	udp	netbios-ns	2	0	0	2	0
139	tcp	mbn	1	0	0	1	0
443	tcp	www	10	0	0	10	0
445	tcp	cifs	6	0	0	6	0
3128	tcp	www	3	0	0	3	0
3389	tcp	ms-wbt-server?	3	0	0	3	0
4080	tcp	www	4	0	0	4	0
4081	tcp	www	10	0	0	10	0
44333	tcp	winrouteadmin?	4	0	0	4	0
49152	tcp	dce-rpc	1	0	0	1	0
49153	tcp	dce-rpc	1	0	0	1	0
49154	tcp	dce-rpc	1	0	0	1	0
49155	tcp	dce-rpc	1	0	0	1	0
49156	tcp	dce-rpc	1	0	0	1	0
49157	tcp	dce-rpc	1	0	0	1	0

Gambar 13. Reports Low pada host server.paltv.tv

PENUTUP

Dengan adanya analisis dan audit beberapa *sample host* dalam jaringan LAN di PT. Sumeks Tivi Palembang, akhirnya dapat diketahui beberapa kelemahan (vulnerabilitas) yang ada, yaitu diantaranya adalah: penempatan secara tidak ergonomis mengenai perangkat-perangkat keras seperti (*switch*, PC, *harddisk*, *Air Conditioner* (AC) dan lain-lain) yang rentan akan gangguan timbulnya bencana alam, perubahan suhu, dan serangan hewan-hewan pengerat yang dapat menimbulkan kerusakan dan kerugian seperti merusak kabel-kabel instalasi, instalasi media seperti (*docking cable*, kabel listrik) yang dapat memicu terjadinya arus pendek (*korsleting*), emanasi gangguan sinyal pada kabel UTP, penggunaan *operating system* yang *illegal* yang dapat memungkinkan sistem operasi menjadi *crash* (rusak) sehingga

diperlukan *update patch* secara berkala, tidak adanya pembatasan hak akses pada *resource sharing* (data-data tertentu), antivirus yang tidak berfungsi secara maksimal (tidak terbaharui / *non update*), dan penggunaan servis-servis jaringan seperti *DNS* (*Domain Name System*), *CIFS*, serta *port-port* yang masih banyak terdapat *bug* (celah) yang memungkinkan seorang penyusup untuk memasukkan kode-kode tertentu dan akhirnya merusak, bahkan mencuri informasi yang jelas sangat merugikan.

DAFTAR PUSTAKA

- Anonim. 2010. *Sistem Jaringan Komputer untuk Pemula*. Yogyakarta : Andi, Madcoms.
- Brenton, Hunt. 2005. *Network Security*. Jakarta : PT Elex Media Komputindo.
- Kusmayadi, Ismail. 2008. *Think Smart Bahasa Indonesia*. Bandung : Grafindo Media Pratama.
- Lammle, Todd. 2007. *CCNA Cisco Certified Network Associate Study Guide*. Inc : Indianapolis, Indiana : Wiley Publishing.
- Lehtinen, Russell, Gangemi. 2006. *Computer Security Basics*. Inc : United Stated of America : O'Reilly Media.
- Masidjo. 1995. *Penilaian Pencapaian Hasil Belajar Siswa di Sekolah*. Yogyakarta : Kanisius.
- Ramadhan, Arief. 2006. *Student Guides Series Pengenalan Jaringan Komputer*. Jakarta : PT Elex Media Komputindo.
- Rafiudin, Rahmat. 2003. *Panduan Membangun Jaringan Komputer untuk Pemula*. Jakarta : PT Elex Media Komputindo.
- Syafrizal, Melwin. 2005. *Pengantar Jaringan Komputer*. Yogyakarta : Andi.
- Utdirartatmo, Firrar. 2004. *Analisa Keamanan dan Vulnerabilitas Jaringan Komputer*. Yogyakarta : Gava Media.
- Widjono. 2007. *Bahasa Indonesia Mata Kuliah Pengembangan Kepribadian di Perguruan Tinggi*. Jakarta : PT Grasindo.
- Wahana, Komputer. 2006. *Menginstalasi Perangkat Jaringan Komputer*. Jakarta : PT Elex Media Komputindo.
- Yani, Ahmad. 2008. *Panduan Membangun Jaringan Komputer*. Jakarta : PT. Kawan Pustaka.