Titik Lemah Jaringan Komputer

Endi Dwi Kristianto
endidwikristianto@engineer.com
http://endidwikristianto.blogspot.com

Lisensi Dokumen:
Copyright © 2012-2013 IlmuKomputer.Com
Seluruh dokumen di IlmuKomputer.Com dapat digunakan, dimodifikasi dan disebarkan secara bebas untuk tujuan bukan komersial (nonprofit), dengan syarat tidak menghapus atau merubah atribut penulis dan pernyataan copyright yang disertakan dalam setiap dokumen. Tidak diperbolehkan melakukan penulisan ulang, kecuali mendapatkan ijin terlebih dahulu dari IlmuKomputer.Com.

Pemahaman dasar pada keamanan jaringan computer sangat perlu untuk merawat jaringan komputer tanpa harus terjadi insiden keamanan didalam jaringan itu. Artikel ini juga sebagai bahan ilustrasi beberapa masalah keamanan jaringan terjadi. Artikel ini tidak akan menjelaskan secara detil akan tetapi para pembaca setidaknya telah mendapat suatu gambaran yang bagus dan mungkin mendapat ide untuk mencari solusi dari kelemahan-kelemahan tersebut.

Masalah keamanan

Jaringan komputer moderen adalah entitas dari banyak komponen kecil. Disini akan dijelaskan beberapa titik lemah dari komponen yang berbeda.

Weak protocols (protokol yang lemah).

Komunikasi jaringan komputer menggunakan protokol antara client dan server. Kebanyakan dari protokol yang digunakan saat ini merupakan protocol yang telah digunakan beberapa dasawarsa belakangan. Protokol lama ini, seperti File Transmission Protocol (FTP), TFTP ataupun telnet, tidak didesain untuk menjadi benar-benar aman. Malahan faktanya kebanyakan dari protocol ini sudah seharusnya digantikan dengan protokol yang jauh lebih aman, dikarenakan banyak titik rawan yang dapat menyebabkan pengguna (user) yang tidak bertanggung jawab dapat melakukan

eksploitasi. Sebagai contoh, seseorang dengan mudah dapat mengawasi "traffic" dari telnet dan dapat mencari tahu nama user dan password.

Software issue (masalah perangkat lunak).

Menjadi sesuatu yang mudah untuk melakukan eksploitasi celah pada perangkat lunak. Celah ini biasanya tidak secara sengaja dibuat tapi kebanyakan semua orang mengalami kerugian dari kelemahan seperti ini. Celah ini biasanya dibakukan bahwa apapun yang dijalankan oleh "root" pasti mempunyai akses "root", yaitu kemampuan untuk melakukan segalanya didalam system tersebut. Eksploitasi yang sebenarnya mengambil keuntungan dari lemahnya penanganan data yang tidak diduga oleh pengguna, sebagai contoh, buffer overflow dari celah keamanan "format string" merupakan hal yang biasa saat ini.

Eksploitasi terhadap celah tersebut akan menuju kepada situasi dimana hak akses pengguna akan dapat dinaikkan ke tingkat akses yang lebih tinggi. Ini disebut juga dengan "rooting" sebuah "host" dikarenakan penyerang biasanya membidik untuk mendapatkan hak akses "root".

Buffer overflow.

"Buffer overflow" mempunyai arti sama dengan istilahnya. Programmer telah mengalokasikan sekian besar memory untuk beberapa variabel spesifik. Bagaimanapun juga, dengan celah keamanan ini, maka variabel ini dapat dipaksa menuliskan kedalam "stack" tanpa harus melakukan pengecekan kembali bila panjang variabel tersebut diizinkan. Jika data yang berada didalam buffer ternyata lebih panjang daripada yang diharapkan, maka kemungkinan akan melakukan penulisan kembali stack frame dari "return address" sehingga alamat dari proses eksekusi program dapat dirubah.

Penulis "malicious code" biasanya akan akan melakukan eksploitasi terhadap penulisan kembali "return address" dengan merubah "return address" kepada "shellcode" pilihan mereka sendiri untuk melakukan pembatalan akses "shell" dengan menggunakan hak akses dari "user-id" dari program yang tereksploitasi tersebut. "Shellcode" ini tidak harus disertakan dalam program yang tereksploitasi, tetapi biasanya dituliskan ke dalam bagian celah dari "buffer". Ini merupakan trik yang biasa digunakan pada variable "environment" seperti ini.

Copyright © 2012-2013 IlmuKomputer.Com

"Buffer overflow" adalah masalah fundamental berdasarkan dari arsitektur komputasi modern. Ruang untuk variabel dan kode itu sendiri tidak dapat dipisahkan kedalam blok yang berbeda didalam "memory". Sebuah perubahan didalam arsitektur dapat dengan mudah menyelesaikan masalah ini, tapi perubahan bukan sesuatu yang mudah untuk dilakukan dikarenakan arsitektur yang digunakan saat ini sudah sangat banyak digunakan.

Format string.

Metode penyerangan "format string" merupakan sebuah metode penyerangan baru, ini diumumkan kepada publik diakhir tahun 2000. Metode ini ditemukan oleh hacker 6 bulan sebelum diumumkan kepada masyarakat luas. Secara fundamental celah ini mengingatkan kita akan miripnya dengan celah "buffer overflow". Kecuali celah tersebut tercipta dikarenakan kemalasan (laziness), ketidakpedulian (ignorance), atau programmer yang mempunyai skill pas-pasan. Celah "format string" biasanya disebabkan oleh kurangnya "format string" seperti "%s" di beberapa bagian dari program yang menciptakan output, sebagai contoh fungsi printf() di C/C++. Bila input diberikan dengan melewatkan "format string" seperti "%d" dan "%s"kepada program maka dengan mudah melihat "stack dump" atau penggunaan teknik seperti pada "buffer overflow".

Celah ini berdasarkan pada "truncated format string" dari "input". Ini merujuk kepada situasi dimana secara external, data yang disuplai yang diinterpretasikan sebagai bagian dari "format string argument". Dengan secara spesial membuat suatu input dapat menyebabkan program yang bermasalah menunjukkan isi memory dan juga kontrol kepada eksekusi program dengan menuliskan apa saja kepada lokasi pilihan sama seperti pada eksploitasi "overflow".

Hardware issue (masalah perangkat keras).

Biasanya perangkat keras tidak mempunyai masalah pada penyerangan yang terjadi. Perangkat lunak yang dijalankan oleh perangkat keras dan kemungkinan kurangnya dokumentasi spesifikasi teknis merupakan suatu titik lemah. Berikut ini merupakan contoh bagaimana perangkat keras mempunyai masalah dengan keamanan.

Copyright © 2012-2013 IlmuKomputer.Com

contoh 1: Cisco

Sudah lazim router cisco dianggap mempunyai masalah sistematis didalam perangkat lunak IOS (Interwork operating system) yang digunakan oleh mereka sebagai sistem operasi pada tahun 2003. Celah dalam perangkat lunak dapat menuju kepada "denial of service" (Dos) dari semua perangkat router. Masalah keamanan ini terdapat dalam cara IOS menangani protokol 53(SWIPE), 55(IP Mobility) dan 77(Sun ND) dengan nilai TTL (Time to live) 0 atau 1.

Biasanya, Protocol Independent Multicast (PIM) dengan semua nilai untuk hidup, dapat menyebabkan router menandai input permintaan yang penuh terhadap "interface" yang dikirimkan. Sebagai permintaan bila penuh, maka router tidak akan melakukan proses "traffic" apapun terhadap "interface" yang dipertanyakan. Cisco juga mempunyai beberapa celah keamanan yang terdokumentasi dan "patch" yang diperlukan telah tersedia untuk waktu yang cukup lama.

contoh 2: Linksys

Perangkat linksys mempunyai harga yang cukup murah sehingga banyak digunakan oleh orang. Beberapa perangkat linksys mempunyai masalah dengan celah keamanan yang dapat menuju kepada serangan "denial of service" (DoS). Celah keamanan yang memprihatinkan terdapat pada penanganan parameter "URL Embedded" yang dikirimkan kepada perangkat.

Misconfiguration (konfigurasi yang salah).

Kesalahan konfigurasi pada server dan perangkat keras (hardware) sangat sering membuat para penyusup dapat masuk kedalam suatu system dengan mudah. Sebagai contoh, penggantian halaman depan suatu situs dikarenakan kesalahan konfigurasi pada perangkat lunak "www-server" atapun modulnya. Konfigurasi yang tidak hati-hati dapat menyebabkan usaha penyusupan menjadi jauh lebih mudah terlebih jika ada pilihan lain yang dapat diambil oleh para penyusup.

Sebagai contoh, sebuah server yang menjalankan beberapa layanan SSH dapat dengan mudah disusupi apabila mengijinkan penggunaan protokol versi 1 atau "remote root login" (RLOGIN) diizinkan. Kesalahan konfigurasi yang jelas ini menyebabkan terbukanya celah keamanan dengan penggunaan protokol versi 1, seperti "buffer

Copyright © 2012-2013 IlmuKomputer.Com

overflow" yang dapat menyebabkan penyusup dapat mengambil hak akses "root" ataupun juga dengan menggunakan metode "brute-force password" untuk dapat menebak password "root".

DoS, DDoS.

Serangan Denial of Service adalah serangan yang mengakibatkan setiap korbannya akan berhenti merespon atau "bertingkah" tidak lazim. Contoh serangan klasik "DoS" adalah "Ping of Death" dan "Syn Flood" yang untungnya sudah hampir tidak dapat dijumpai pada saat sekarang. Biasanya serangan DoS menyerang celah yang terdapat pada layanan system atau pada protokol jaringan kerja untuk menyebabkan layanan tidak dapat digunakan. Tehnik yang lainnya adalah menyebabkan system korban "tersedak" dikarenakan banyaknya paket yang diterima yang harus diproses melebihi kemampuan dari system itu sendiri atau menyebabkan terjadinya "bottleneck" pada bandwidth yang dipakai oleh system.

Serangan "Distributed Denial of Service" (DDoS) merupakan tipe serangan yang lebih terorganisasi. Jenis serangan ini biasanya membutuhkan persiapan dan juga taktik untuk dapat menjatuhkan korbannya dengan cepat dan sebelumnya biasanya para penyerang akan mencari system kecil yang dapat dikuasai dan setelah mendapat banyak system kecil maka penyerang akan menyerang system yang besar dengan menjalankan ribuan bahkan puluhan ribu system kecil secara bersamaan untuk menjatuhkan sebuah system yang besar.

Worm "MyDoom" yang terkenal itu dibuat untuk melancarkan serangan besar-besaran dari puluhan ribu system yang terinfeksi untuk menyerang situs www.sco.com. Serangan itu sukses besar yang menyebabkan www.sco.com harus dipindahkan dari DNS untuk dapat menjalankan kembali layanan.

Viruses (virus).

Salah satu definisi dari program virus adalah menyisipkan dirinya kepada objek lain seperti file executable dan beberapa jenis dokumen yang banyak dipakai orang. Selain kemampuan untuk mereplikasi dirinya sendiri, virus dapat menyimpan dan menjalankan sebuah tugas spesifik. Tugas tersebut bisa bersifat menghancurkan atau sekedar menampilkan sesuatu ke layar monitor korban dan bisa saja bertugas untuk mencari

Copyright © 2012-2013 IlmuKomputer.Com

suatu jenis file untuk dikirimkan secara acak ke internet bahkan dapat melakukan format pada hard disk korban.

Virus yang tersebar di internet yang belum dikenali tidak akan dapat ditangkap oleh program antivirus ataupun semacamnya yang meskipun korban telah terjangkiti tetapi tidak mengetahuinya. Perangkat lunak antivirus biasanya mengenali virus atau calon virus melalui tanda yang spesifik yang terdapat pada bagian inti virus itu sendiri. Beberapa virus menggunakan tehnik polymorphic agar luput terdeteksi oleh antivirus.

Kebiasaan virus polymorphic adalah merubah dirinya pada setiap infeksi yang terjadi yang menyebabkan pendeteksian menjadi jauh lebih sulit. Praktisnya setiap platform komputer mempunyai virus masing-masing dan ada beberapa virus yang mempunyai kemampuan menjangkiti beberapa platform yang berbeda (multi-platform). Virus multi-platform biasanya menyerang executable ataupun dokumen pada Windows dikarenakan kepopuleran oleh system operasi Microsoft Windows dan Microsoft Office sehingga banyak ditemukan virus yang bertujuan untuk menghancurkan "kerajaan" Microsoft Corp.

Worms.

Sebuah "worm" komputer merupakan program yang menyebar sendiri dengan cara mengirimkan dirinya sendiri ke system yang lainnya. Worm tidak akan menyisipkan dirinya kepada objek lain. Pada saat sekarang banyak terjadi penyebaran worm dikarenakan para pengguna komputer tidak melakukan update pada perangkat lunak yang mereka gunakan, yang dimana ini berarti, sebaga contoh, Outlook Express mempunyai fungsi yang dapat mengizinkan eksekusi pada file sisipan (attachment) e-mail tanpa campur tangan dari pengguna komputer itu sendiri.

Trojan horse.

Trojan horse adalah program yang berpura-pura tidak berbahaya tetapi sebenarnya mereka sesuatu yang lain. Salah fungsi yang biasa terdapat pada "trojan horse" adalah melakukan instalasi "backdoor" sehingga si pembuat program dapat menyusup kedalam komputer atau system korban.

junk mail (surat sampah).

Copyright © 2012-2013 IlmuKomputer.Com

"junk mail" sesungguhnya bukan suatu ancaman keamanan yang serius, tetapi dengan penyebaran virus dan worm melalui e-mail, maka jumlah junk mail juga ikut bertambah. Ancaman keamanan sesungguhnya bukan dari e-mail sampah itu sendiri melainkan file sisipannya (attachment) yang patut diwaspadai dikarenakan penyebaran virus dan worm menggunakan metode ini.

Time bomb (bom waktu).

"Time bomb" adalah program yang mempunyai tugas tetapi dengan waktu tertentu baru akan menjalankan tugasnya. Beberapa jenis virus dan worm juga mempunyai kesamaan fungsi dengan aplikasi ini. Time bomb berbeda dengan virus ataupun worm dikarenakan dia tidak melakukan replikasi terhadap dirinya tetapi melakukan instalasi sendiri kedalam system.

Biografi

Endi Dwi Kristianto. Biasa dipanggil Endi. Penulis lahir di Tegal, 28 Oktober 1991. Menyelesaikan pendidikan vokasi di SMK Telkom Sandhy Putra Purwokerto Jurusan Teknik Komputer Jaringan, dan sekarang masih terdaftar sebagai mahasiswa tingkat akhir Politeknik Negeri Semarang, Program Studi D4 Teknik Telekomunikasi. Bidang kesukaan adalah Networking, Komunikasi data, Linux, WLAN, Security Network, dan Jaringan Powerline atau PLC (lagi belajar). Kegiatan saat ini adalah melakukan penelitian tentang virtual access point dan implementasi jaringan powerline.

Copyright © 2012-2013 IlmuKomputer.Com