BAB II

APLIKASI PENDUKUNG

Pada bab kedua ini mengemukakan aplikasi-aplikasi pendukung PANS yaitu Nessus, PHP, MySQL, dan Apache.

2.1 Nessus (http://www.nessus.org)

Nessus adalah sebuah *security scanner tool* (aplikasi untuk melakukan pemeriksaan keamanan) di bawah lisensi GPL (GNU *General Public License*) yang membuat aplikasi ini bebas untuk disebarluaskan (baik gratis atau dipungut biaya), bebas untuk dimodifikasi, dan bebas untuk dikembangkan lebih lanjut ke dalam bentuk aplikasi turunan yang berlisensi GPL juga[1].

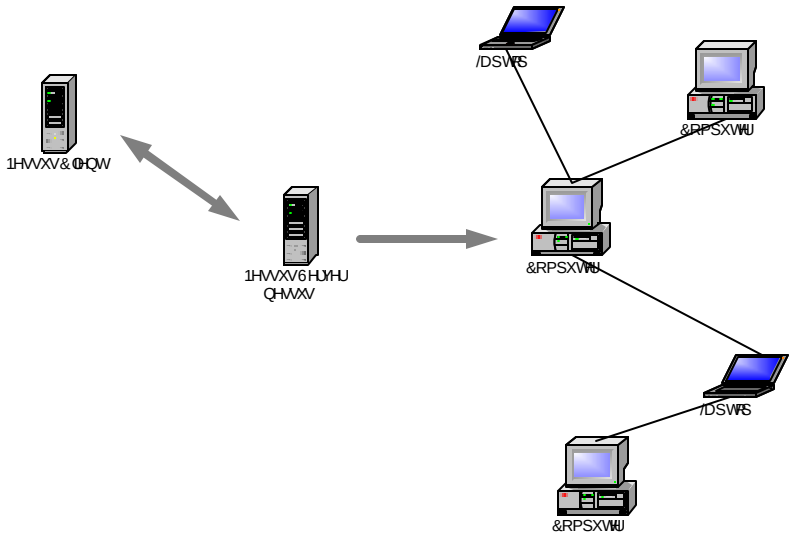
Sampai dengan tulisan ini dibuat, versi terakhir dari Nessus adalah versi 1.2.5. Nessus bisa diinstall pada berbagai sistem operasi yang varian dari UNIX, diantaranya adalah Linux, *BSD, Solaris, dll. Sedangkan sistem operasi yang digunakan disini adalah FreeBSD 4.6-STABLE. Nessus ini dibuat sejak April 1998 oleh Renaud Deraison (deraison@cvs.nessus.org)

Nessus memiliki *user interface* (diinstall pada client Nessus) yang bisa berjalan pada sistem operasi *varian* UNIX dan Windows. Pada OS Unix dibutuhkan GTK (*The Gimp Toolkit* dan X11) supaya *user interface* Nessus dapat terinstall. *User interface* ini berfungsi untuk mengoperasikan Nessus, mengatur konfigurasi *scan* dan mengeksekusi *scan*. Sedangkan yang dirancang kali ini adalah sebuah *user interface* dalam bentuk *web application* yang akan menambah fungsi dari *user interface* bawaan Nessus.

[1] http://www.opensource.org/licenses/gpl-license.php

Nessus dibuat dalam arsitektur *client-server* yang masing-masing mempunyai tugas masing-masing. *Server* Nessus ini menjalankan sebuah *daemon* yang bernama 'nessusd' yang bertugas untuk melakukan serangan/*scan* terhadap komputer/*network* tujuan. Sedangkan *client* Nessus adalah *front-end* yang mengkonfigurasi *server* dan tempat dimana semua data hasil *scan* diletakkan, disinilah *user interface* Nessus biasa dipasang. Aplikasi yang akan dibuat juga akan diletakkan pada *client* ini.

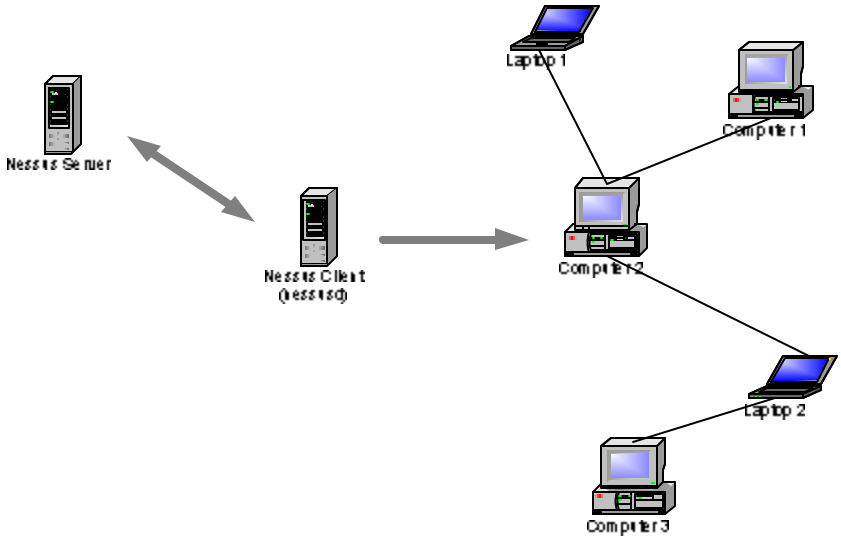
Sebutan *client-server* pada Nessus berlawanan dengan pengertian *client-server* umumnya, disini *client* bisa memiliki dan mengendalikan banyak *server*. Secara detail bisa dilihat pada gambar berikut :



Gambar 2.1. Arsitektur *client-server* pada Nessus (sebenarnya)

Komunikasi antara *client* dengan *server* berupa data terenkripsi menggunakan SSL dan sebelum terjadi komunikasi dibutuhkan autentifikasi *user* terlebih dahulu. Nessus bisa memiliki banyak *user* dan masing-masing *user* mempunyai ACL (*Access Control List*) tersendiri. Untuk memudahkan pemahaman maka dalam tulisan ini pengertian *server* dan *client* dikembalikan seperti pengertian *server* dan *client* pada umumnya, jadi *client* bertugas untuk melakukan serangan dan *server* yang berfungsi

untuk menyimpan semua data hasil pengolahan sekaligus menjadi antarmuka bagi pemakai, dapat digambarkan menjadi seperti berikut :



Gambar 2.2. Arsitektur *client-server* pada Nessus yang digunakan PANS

Salah satu kelebihan Nessus yang menonjol adalah *plugin-based*, artinya Nessus memiliki *plugin* (modul) yang digunakan untuk proses *scan* dan *plugin-plugin* ini dapat dibuat sendiri bagi yang ingin dengan menggunakan bahasa pemrograman C atau dengan NASL (*Nessus Scripting Language*). Selain dengan jalan membuat sendiri, Nessus juga menyediakan *plugin online* yang secara rutin di*update* dan bisa didownload dengan aplikasi 'nessus-update-plugins' yang menyatu dengan *source* program Nessus.

Masing-masing *plugins* pada Nessus mempunyai kemampuan untuk saling membagi pengetahuan. Sebagai ilustrasi :

- *Plugin* pertama melihat bahwa pada komputer sasaran port 137 UDP dan 139 TCP terbuka.
- *Plugin* kedua memanggil nama Netbios komputer sasaran.
- *Plugin* ketiga mencoba untuk masuk menggunakan session NULL.
- *Plugin* keempat memanggil SID komputer sasaran.

- *Plugin* kelima menggunakan SID tersebut untuk memperoleh daftar *user* dalam komputer sasaran.

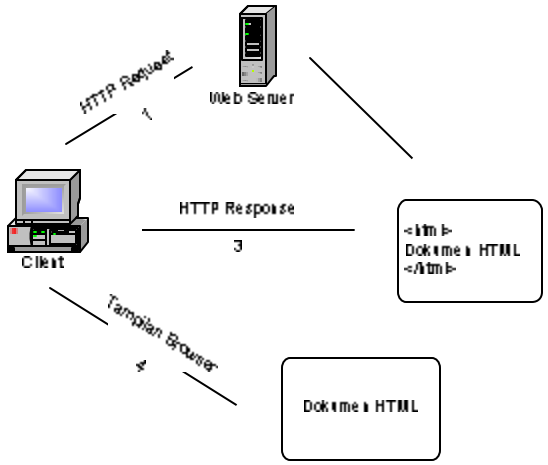
Jadi hasil dari sebuah *plugin* digunakan sebagai masukan dari *plugin* berikutnya, hal ini yang memungkinkan Nessus melakukan audit lebih *powerfull* dan lebih *comprehensive.*

Hasil *scan* Nessus bisa dikonversikan ke beberapa bentuk format data, yaitu : *.nsr (*Nessus Scan Result* – default), LaTeX, HTML, XML, dan teks.

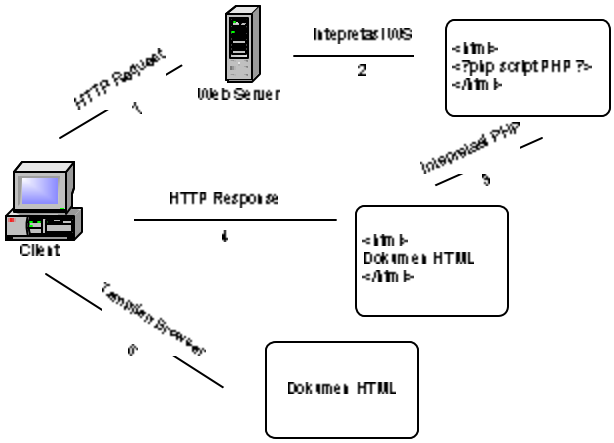
2.2 PHP (http://www.php.net)

PHP (*Hypertext PreProcessor*) merupakan *script* yang membuat sebuah halaman web menjadi dinamis, yang berarti halaman web menjadi lebih interaktif dan halaman yang akan ditampilkan dibuat saat *client* melakukan *request* halaman tersebut. Sehingga informasi yang diterima oleh *client* adalah selalu informasi yang terbaru. *Script* PHP dieksekusi pada *server* dimana *script* tersebut dijalankan (*server-side*), jadi semua informasi yang ingin ditampilkan di halaman *web* bisa dilihat dengan baik oleh semua jenis *browser client*. PHP termasuk dalam HTML-*embedded*, oleh karena itu *script* PHP bisa disisipkan pada sebuah halaman HTML.

Perbedaan utama antara *script* PHP dengan HTML adalah, HTML murni sebuah dokumen teks sedangkan *script* PHP di dalamnya terdapat program yang akan diproses oleh *web server* dan hasil pemrosesannya adalah sebuah dokumen teks. Lebih lanjut bisa dilihat pada gambar 2.3 dan 2.4 :



Gambar 2.3. Proses pada *request* HTML murni



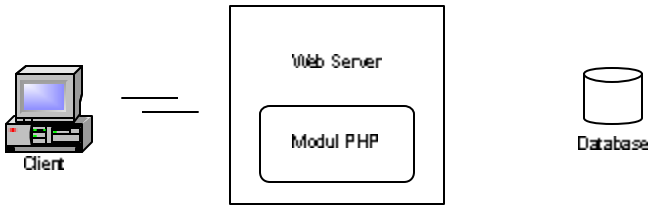
Gambar 2.4. Proses pada *request* PHP

Dari kedua gambar di atas terlihat bahwa perbedaan dari keduanya adalah adanya *script* PHP yang akan diproses/diinterpretasikan terlebih dahulu oleh PHP *intepreter* dalam *web server* sebelum dikirimkan ke *browser* pada *client*. Proses inilah yang menyebabkan PHP mampu membuat sebuah halaman *web* menjadi dinamis.

Pada awalnya PHP adalah sebuah proyek pribadi dari Rasmus Lerdorf yang membuat PHP versi pertama untuk *homepage* pribadinya, versi ini masih berupa kumpulan *script* Perl. Kemudian Rasmus membuat versi kedua dari PHP dengan cara

menulis ulang *script-script* Perl menggunakan bahasa C. Pada versi kedua ini ditambahkan dua fasilitas yang penting yaitu *Form* HTML dan koneksi dengan *database* MySQL. PHP versi ketiga dikembangkan oleh Rasmus dan suatu kelompok *open source*, dimana pada versi ini PHP mulai menampakkan keunggulannya sebagai sebuah bahasa *server scripting* yang handal. Melalui perkembangan yang pesat ini banyak fasilitas yang ditambahkan dan oleh kelompok ini PHP disebut sebagai "PHP: *Hypertext Preprocessor*". Sintak yang digunakan berasal dari bahasa C , Java, dan Perl. Sampai dengan tulisan ini dibuat, versi terakhir dari PHP adalah 4.2.3. PHP juga mendukung beberapa servis-servis yang menggunakan protokol seperti IMAP, SNMP, NNTP, POP3, HTTP, dan protokol-protokol lainnya. Beberapa *database* yang didukung oleh PHP diantaranya adalah Adabas D, Ingres, Oracle, dBase, InterBase, PostgreSQL, mSQL, MS-SQL, Sybase, IBM DB2, MySQL, Informix, ODBC.

Mekanisme kerja sebuah *web server* yang memanfaatkan PHP dan *database* dapat digambarkan seperti ini :



2.3 MySQL (http://www.mysql.com)

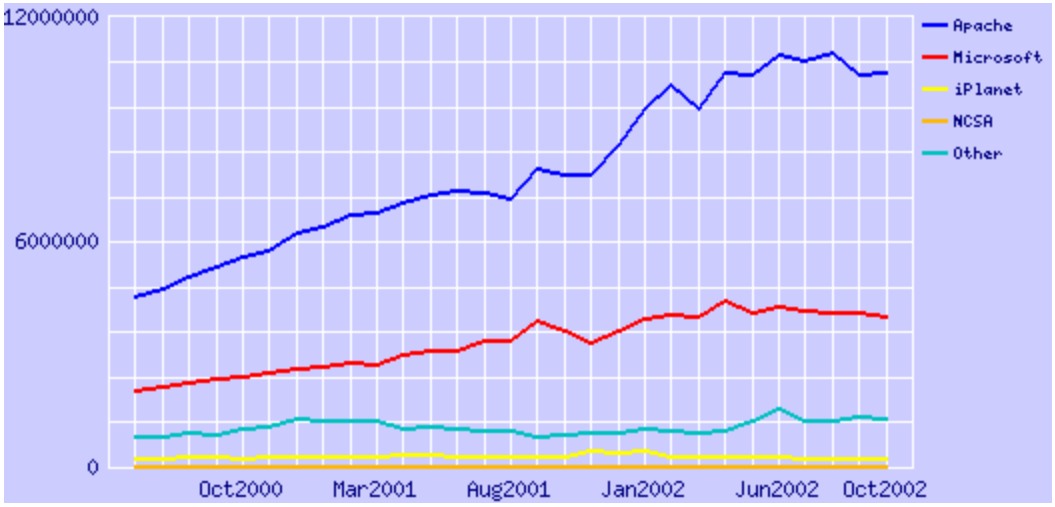
MySQL adalah sebuah sistem manajemen *database open source* yang populer dan gratis untuk *platform* Unix. Sistem manajemen *database* MySQL menggunakan kumpulan perintah sederhana untuk memasukkan, memanggil, menghapus, dan memperbarui data, dengan ini kita dapat mengembangkan *database* yang kompleks. Beberapa kemampuan MySQL adalah sebagai berikut :

- MySQL bisa diakses dan dimanipulasi dari sejumlah bahasa pemrograman terkenal, diantaranya adalah C, C++, Java, Perl, Phyton, dan PHP.
- MySQL ditulis dalam C/C++ dan dioptimasi untuk *platform* Unix dan Win32.
- MySQL mendukung tipe data yang umum digunakan, termasuk FLOAT, DOUBLE, CHAR, VARCHAR, TEXT, BLOB, DATE, SET, dan ENUM.
- MySQL mendukung subset fungsi *query* dan pengelompokan lanjut, termasuk diantaranya GROUP BY dan ORDER BY.
- MySQL memungkinkan alokasi *password* tiap *server*. *Password* yang melalui MySQL untuk melakukan autentifikasi terenkripsi.
- MySQL mendukung berbagai macam metode koneksi, seperti TCP/IP, soket Unix, dan koneksi untuk Windows NT/2000.
- MySQL bisa diperoleh secara gratis termasuk aplikasi-aplikasi lain yang diperlukan dalam memakai MySQL.

MySQL juga merupakan salah satu sistem manajemen *database* yang stabil di pasaran. Ketika MySQL diluncurkan pertama kali pada pertengahan 1996, beberapa *bug* dengan cepat dapat diketahui dan diperbaiki. Sekarang MySQL sudah menjadi sangat stabil dan banyak dipercaya oleh korporasi-korporasi di dunia untuk menyimpan data-data bisnis penting. Data-data ini biasanya membutuhkan media penyimpan yang besar dan hal ini bukan menjadi masalah bagi MySQL, karena tabel MySQL sanggup menampung data lebih dari 4 Gigabytes. MySQL 3.23 berisi jenis tabel baru yaitu MyISAM yang sanggup menampung 8 juta Terabytes.

2.4 Apache (http://httpd.apache.org)

Apache merupakan *web server* yang paling banyak dipergunakan di *Internet*. Berikut survei dari Netcraft[1] tentang perbandingan pemakaian Apache dengan *web server* yang lain :



Gambar 2.6. Data statistik penggunaan web server Apache

Program ini pertama kali didesain untuk sistem operasi lingkungan UNIX. Namun demikian, pada beberapa versi berikutnya Apache mengeluarkan programnya yang dapat dijalankan di Windows. Berdasarkan sejarahnya, Apache dimulai oleh veteran *developer* NCSA httpd (*National Center for Supercomputing Application*). Saat itu pengembangan NCSA httpd sebagai *web server* mengalami stagnasi. Rob Mc Cool meninggalkan NCSA dan memulai sebuah proyek baru bersama para *webmaster* lainnya, menambal *bug*, dan menambahkan fitur pada NCSA httpd. Mereka mengembangkan program ini lewat mailing list. Dengan berpijak pada NCSA httpd versi 1.3, Team Apache mengeluarkan rilis pertama kali secara resmi Apache versi 0.6.2. Nama Apache diambil dari kata "A Patchy Server", *server* perbaikan yang

[1] http://www.netcraft.com/survey/, tgl 24 oktober 2002

penuh dengan tambalan (*patch*). Tambalan yang dimaksud adalah penambahan fitur dan penambalan *bug* dari NCSA httpd Versi 1.3.

Saat ini Apache dipergunakan secara luas, hal ini disebabkan karena programnya yang gratis dengan kinerja relatif stabil. Dalam pengembangannya pun mempergunakan sistem terbuka, yakni tiap orang dibuka kesempatan seluas-luasnya untuk dapat memberikan kontribusi dalam mengembangkan program. Kontribusi dikomunikasikan lewat *mailing list*.

Apache mempunyai program pendukung yang cukup banyak. Hal ini memberikan layanan yang cukup lengkap bagi penggunanya. Beberapa dukungan Apache :

1. Kontrol Akses
   Kontrol ini dapat dijalankan berdasarkan nama *host* atau nomor IP.
2. CGI (*Common Gateway Interface*), yang paling terkenal untuk digunakan adalah perl (*Practical Extraction and Report Language*), didukung oleh Apache dengan menempatkannya sebagai modul (mod_perl)
3. PHP (*PHP Hypertext Processor*), program dengan metode semacam CGI, yang memproses teks dan bekerja di *server*. Apache mendukung PHP dengan menempatkannya sebagai salah satu modulnya (mod_php). Hal ini membuat kinerja PHP menjadi lebih baik.

Platform yang didukung oleh Apache saat ini antara lain Linux, SunOS, UnixWare, FreeBSD, Solaris, AIX, OpenBSD, IRIX, SCO, NetBSD, HPUX, BSDI, Digital Unix.