BAB II
TINJAUAN PUSTAKA

2.1 Tinjauan Perusahaan

Tahap tinjauan perusahaan ini merupakan peninjauan terhadap tempat penelitian studi kasus yang dilakukan di PT. Dataquest Laverage Indonesia. Tinjauan perusahaan meliputi profil perusahaan, visi dan misi perusahaan, struktur organinsasi dan deskripsi tugas yang ada di PT. Dataquest Laverage Indonesia.

2.1.1 Profil Perusahaan PT. Dataquest Leverage Indonesia

PT. Dataquest Leverage Indonesia merupakan perusahaan nasional yang bergerak dalam bidang "Human Capital & Corporate Learning" serta dibidang layanan teknologi IT dan telah berpengalaman dalam pembuatan jasa yang mereka tawarkan seperti website, Service dan mobile application (Android, Ios) kemudian PT. Dataquest Leverage Indonesia adalah suatu perusahaan yang bergerak pada bidang jasa perancangan, pengelolaan dan pengembangan teknologi IT seperti e-learning. PT. Dataquest dapat menerima berbagai macam proyek pembangunan perangkat lunak baik untuk instansi pemerintah maupun swasta. Fokus layanan Dataquest meliputi kegiatan pembelajaran, pelatihan dan konsultan IT serta bergerak dalam bidang research dan development software seperti pembangunan aplikasi Learning Management Sistem, Video Conference dan lainnya. PT. Dataquest Leverage Indonesia sendiri aktif menyelenggarakan pelatihan dan pengembangan bagi perusahaan di bidang e-learning dan Knowledge management.

Info Perusahaan:

Nama Perusahaan	:	PT. Dataquest Laverage Indonesia
Alamat	:	Jalan PHH Mustopa No 39 Surapati Core Blok K, 3, Pasirlayung, bandung, Kota

		Bandung, Jawa Barat 40132
Telepon	:	022 87241375
Email	:	sobari@dataquest
Mobile	:	087825412805 / 085220434344

2.1.2 Visi dan Misi PT. Dataquest Laverage Indonesia

Visi adalah suatu pandangan jauh tentang program perushaan di masa depan, tujuan – tujuan perusahaan dan apa yang harus dilakukan untuk mencapai tujuan pada masa yang akan datang, sedangkan misi adalah pernyataan tentang apa yang harus dikerjakan oleh perusahaan dalam usahanya mewujudkan visi tersebut, Adapun Visi dan Misi dari PT. Dataquest adalah sebagai berikut.

1. Visi

   Dataquest diakui sebagai institusi layanan TI terbaik di level asia tenggara dalam rangka mendukung perkembangan e-learning di indonesia.

2. Misi
   1. Meningkatkan kualitas sumber daya pengelola layanan E-Learning yang mencakup informasi, aplikasi, infrastruktur dan personil.
   2. Menyediakan layanan E-Learning terbaik kepada Indonesia dalam mendukung pendidikan, penelitian dan pengabdian masyarakat serta manajemen organisasi.
   3. Memberikan solusi terbaik bagi pengembangan SDM profesional dan komunitas di bidang E-Learning pada tingkat nasional dan regional.
   4. Melaksanakan program yang dapat menjamin pencapaian visi dengan meningkatkan ketahanan dan keberlanjutan organisasi serta kesejahteraan personil.

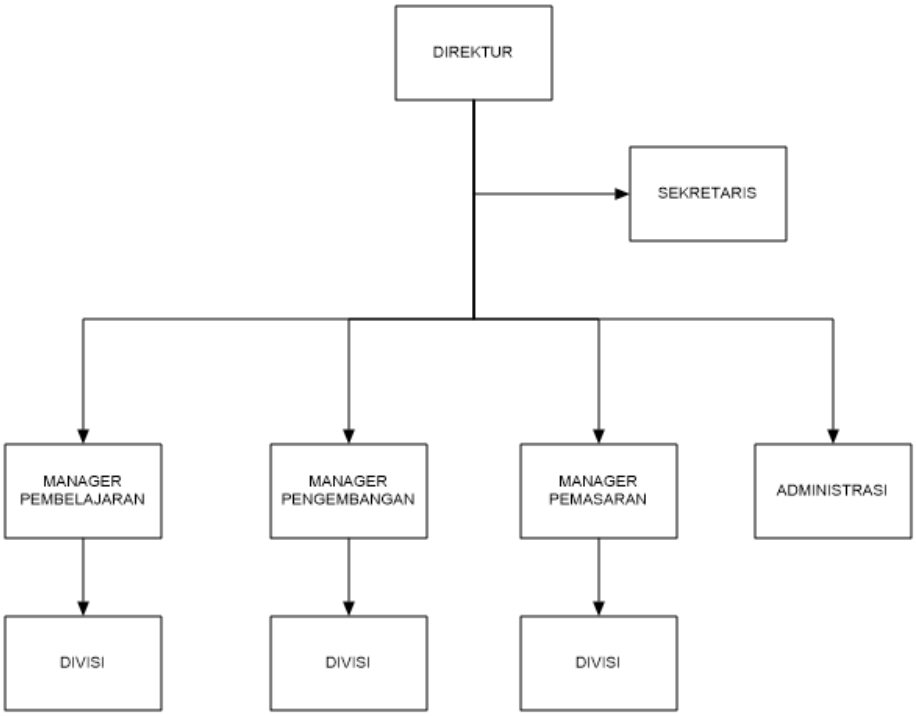
2.1.3 Logo Perusahaan

Logo Perusahaan PT. Dataquest Laverage Indonesia dapat dilihat pada gambar 2.1 berikut:

Gambar 2.1 Logo PT. Dataquest Laverage Indonesia

2.1.4 Struktur Organisasi Perusahaan

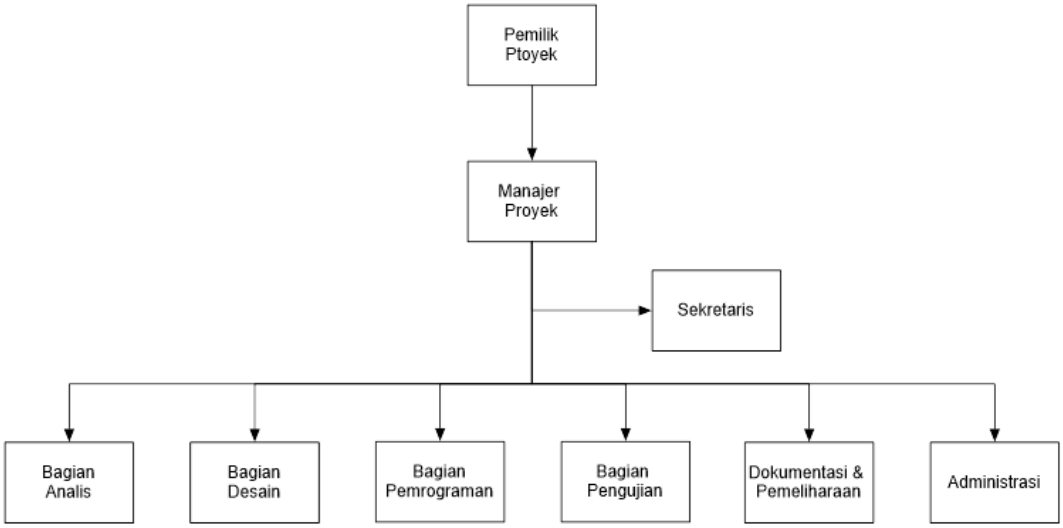
Struktur Organisasi merupakan penggambaran secara grafik seperti struktur kerja dari setiap bagian yang mempunyai wewenang dan tanggung jawab di PT. Dataquest Laverage Indonesia. Berikut Struktur Organisasi Perusahaan PT. Dataquest pada gambar 2.2 berikut:



Gambar 2.2 Organisasi perusahaan

2.1.5 Struktur Organisasi Proyek

Berikut Struktur Organisasi Proyek PT. Dataquest dapat dilihat pada gambar 2.3 berikut:



Gambar 2.3 Struktur Organisasi Proyek

2.1.6 Deskripsi Tugas dan Tanggung Jawab

Deskripsi tugas dan tanggung jawab digunakan untuk mengetahui tugas, wewenang dan tanggung jawab dari masing-masing bagian. Adapun deskripsi tugas yang ada pada PT. Dataquest Laverage Indonesia adalah sebagai berikut:

1. Direktur

   Direktur mempunyai tugas dan tanggung jawab sebagai berikut:

   1. Mempunyai wewenang tertinggi serta menentukan dan memutuskan kebijakan peraturan dan kebijakan perusahaan.
   2. Mengembangkan sumbependapatan perusahaan.
   3. Mengawasi kinerja perusahaan dari segala bagian.
   4. Fokus untuk menetapkan berbagaimacam strategi untuk mencapai tujuan visi dan misi perusahaan.

2. Manajer Proyek

   Manajer Proyek mempunyai tugas dan tanggung jawab sebagai berikut:

   1. Membuat rencana kerja proyek.
   2. Memberikan tugas dan pekerjaan ke anggota atau tim proyek.

3. Memonitor jalannya proyek dan kerja tim proyek.
4. Bertanggung jawab atas keberhasilan eksekusi proyek.
5. Memastikan proyek dapat berjalan dengan sukses sesuai dengan jadwal dan ruang lingkup yang disetujui.
6. Mengadakan meeting proyek secara berkala untuk menangani permintaan perubahan.
7. Membuat progress report.
8. Menjembatani penganalisa system dengan desainer sehingga antara hasil analisa system dan bentuk desain sesuai dengan yang diharapkan.
9. Menjebatani desainer dengan programmer sehingga desain baru yang dibuat tidak menyulitkan tim programmer dalam membuat dan mewujudkan.
10. Melaporkan setiap kemajuan projek hasil dan hasil akhir proyek kepada pemilik proyek.
11. Membuat dokumentasi manajemen proyek yang dibantu oleh administrator.

3. Sekretaris
    1. Membantu manajer proyek melakukan pencatatan proyek.
    2. Mewakili organisasi proyek untuk melakukan persetujuan dan kesepakatan dengan pihak-pihak tertentu.
    3. Mewakili organisasi untuk menghadiri acaradan agenda tertentu lainnya.
4. Bagian Analisis

    Bagian Analisis mempunyai tugas dan tanggung jawab sebagai berikut:
    1. Melakukan analisis sistem informasi perpustakaan yang akan dibangun dengan melakukan wawancara kepada pihak yang ditunjuk.
    2. Melaporkan hasil pekerjaan kepada manajer proyek.
    3. Berdiskusi dengan manajer proyek mengenai langkah-langkah yang harus ditempuh untuk menyelesaikan proyek sesuai dengan perencanaan manajemen proyek.

4. Berdiskusi dengan bagian desainr untuk menentukan desain sesuai dengan yang diinginkan.

5. Bagian Desain

   Bagian Desain mempunyai tugas dan tanggung jawab sebagai beriku:

   1. Membuat desain sistem yang akan dibangun.
   2. Berdiskusi dengan bagian analisis terkait desain yang akan dibangun.
   3. Berdiskusi dengan programmer tentang bentuk desain yang akan dibangun.
   4. Membuat dokumentasi desain yang dibantu oleh dokumentator.
   5. Menyediakan desain sistem yang akan dibangun.

6. Bagian Pemrograman

   Bagian Pemrograman mempunyai tugas dan tanggung jawab sebagai berikut:

   1. Membuat program sesuai dengan hasil Analisa dan desain yang ditentukan.
   2. Berdiskusi dengan desain dan analisis agar program atau sytem yang dibuatnya sesuai dengan yang telah ditentukan.
   3. Memberi usulan pada desainer dan penganalisa system (jika diperlukan).
   4. Mengajukan pertanyaan kepada desainer dan system analisis apabila terdapat hal yang kurang jelas.
   5. Memperbaiki program atau system berdasarkan hasil invertigasi.
   6. Membuat dokumtasi program yang dibantu oleh dikumentator.

7. Bagian Pengujian

   Bagian Pengujian mempunyai tugas dan tanggung jawab sebagai berikut:

   1. Melakukan test terhadap program atau system informasi yang telah dibuat.
   2. Membuat daftar atau list hal yang perlu diperbaiki.
   3. Memberi rokomendasi tentang solusi permasalahan yang dihadapi.
   4. Membuat dokumentasi tentang hasil testing terhadap program aplikasi.

8. Bagian Dokumentasi & Pemeliharaan

   Bagian Dokumentasi mempunyai tugas dan tanggung jawab sebagai berikut:

1. Membuat dokumentasi system, berkoordinasi dengan system analyst, desainer dan programmer.
2. Berkoordinasi dengan bagian analisis, dengan pihak yang ditunjuk untuk memberikan keterangan mengenai system yang akan dibangun.
3. Mendokumentasikan manajemen proyek yang telah dibuat oleh manajer proyek bersama bagian administrasi.
4. Bekerja sama dengan bagian administrasi untuk membuat dokumentasi adminitrasi proyek.
5. Penambahan fungsi baru dan kebutuhan baru.
6. Perbaikan kualitas perangkat lunak.

9. Bagian Administrasi

Bagian Administrasi mempunyai tugas dan tanggung jawab sebagai berikut:

1. Melaksanakan administrasi proyek dari awal hingga akhir proyek.
2. Membantu manajer proyek dalam membuat dokumen manajemen proyek.
3. Mendokumentasikan arsip yang berkaitan dengan administrasi proyek dan berkoordinasi dengan bagian dokumentasi.

2.2 Landasan Teori

Landasan teori merupakan suatu konsep berupa teori-teori yang tertata rapi dan sistematis, teori-teori yang berlaku sesuai dengan sumber-sumber yang tepat dan terpercaya. Landasan teori pada penelitian ini akan menerangkan mengenai teori-teori yang berhubungan dengan Sistem Informasi Manajemen Sumber Daya Manusia Proyek di PT. Dataquest Laverage Indonesia.

2.2.1 Keamanan Sistem Informasi

Informasi semakin mudah diperoleh dengan menggunakan teknologi yang terus berkembang pesat di zaman modern. Selain sebagai layanan yang mendukung relibilitas informasi, teknologi harus memiliki keamanan yang baik. Kemanan diperlukan guna melindungi informasi dari pihak yang tidak berwenang. Keamanan teknologi informasi memiliki tiga prinsip utama yang biasa disebut CIA Triad yaitu Kerahasiaan (Confidentiality), Integritas (Integrity), dan

Ketersediaan (Availability) (Raj et al., 2018). Tiga prinsip mempunyai hubungan yang erat antara satu dengan yang lain sehingga membentuk sebuah segitiga.

Gambar 2.4 CIA Triad

Confidentility adalah prinsip yang menjaga kerahasian informasi objek dan melakukan pencegahan dengan meminimalisir akses illegal (Chapple et al., 2018). Keamanan yang dilakukan pada aspek ini dapat berupa pengelolaan pada pembatasan hak terhadap informasi. Confidentiality mempunyai hubungan yang erat dengan Integrity, karena jika integritas data dari objek diragukan maka aspek kerahasiaan telah hilang. Contohnya adalah ketika sebuah website diharuskan memasukkan informasi pendaftar seperti nama, nomor telepon, dan alamat e-mail yang dapat dimanfaatkan hacker untuk melakukan spamming atau social enginering (Ren et al., 2018). Informasi tersebut tersimpan di dalam whois database yang dapat oleh semua pihak. Registrar mennyediakan fitur whois privacy sehingga dapat menyembunyikan informasi pribadi pendaftar.

Integrity adalah aspek yang berhubungan dengan integritas data yang dimiliki sehingga keaslian dan kemurnian dilindungi ketat dari manipulasi ilegal. Implementasi integrity yang baik menyediakan perubahan data oleh pihak yang memiliki kewenangan dan melindungi dari perubahan data yang dilakukan oleh pihak tidak berwenang dalam waktu yang sama. Kerentanan utama pada Integrity adalah ketika komunikasi data berlangsung, dimana data dapat diubah dengan melakukan serangan siber seperti Man-in-the-Middle (MITM) dan penerima tidak menyadari data telah berubah. Dalam kasus ini, menggunakan message authentication code dapat melindungi aspek Integrity (Rahardjo, 2017).

Availability menyediakan informasi terhadap akses dengan relibilitas tinggi dari tempat tertentu dengan format yang benar. Kesulitan dalam mempertahankan Availability adalah karena bila suatu informasi tersedia untuk seseorang maka hal itu berlaku untuk setiap orang tetapi penggunaan informasi tersebut dapat dimanfaatkan dengan tujuan yang berbeda-beda (Cardwell, 2016) . Jika keamanan berhasil melaksanakan availability maka setiap pihak yang memiliki izin dapat mengakses informasi dari berbagai sumber menggunakan jalur yang aman. Contohnya menggunakan HTTPS, SSL, atau TLS ketika user mengakses suatu website sehingga terhindar dari serangan seperti phishing, CSRF, XSS, SQLI.

Keamanan yang baik dinilai dari penerapan tiga prinsip tersebut digunakan untuk mencapai visi organisasi untuk mengamankan aset-aset informasi yang berharga. Oleh karena itu setiap Registrar diharapkan menerapkan manajemen keamanan informasi yang baik seperti ISO 27001.

2.2.2 Website

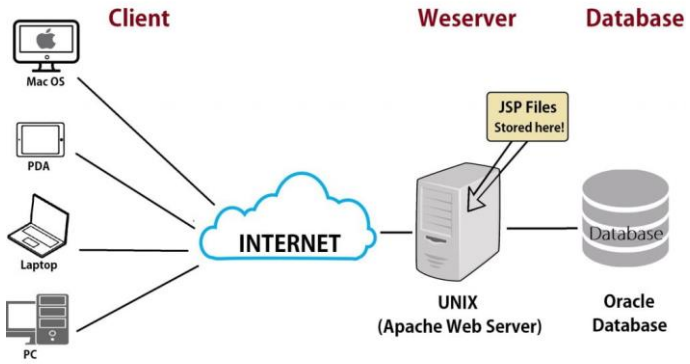
Website adalah sekumpulan halaman web yang saling berhubungan yang umumnya berada pada peladen yang sama berisikan kumpulan informasi yang disediakan secara perorangan, kelompok, atau organisasi.

Website awalnya merupakan suatu layanan sajian informasi yang menggunakan konsep hyperlink, yang memudahkan surfer atau pengguna internet melakukan penelusuran informasi di internet. Informasi yang disajikan dengan web menggunakan konsep multimedia, informasi dapat disajikan dengan menggunakan banyak media, seperti teks, gambar, animasi, suara, atau film.

2.2.3 Web Server

Web server adalah software yang memberikan layanan data yang mempunyai fungsi untuk menerima permintaan HTTP (HyperText Transfer Protocol) atau HTTPS yang dikirim oleh klien melalui web browser dan mengirimkan kembali hasilnya dalam bentuk halaman web yang umumnya.

berbentuk dokumen HTML (HyperText Markup Language). Web server berguna sebagai tempat aplikasi web dan sebagai penerima request dari client (Indra Warman & Zahni, 2013). Pada umumnya web server telah dilengkapi pula dengan mesin penerjemah bahasa skrip yang memungkinkan web server menyediakan layanan situs web dinamis dengan memanfaatkan pustaka tambahan seperti PHP (PHP: Hyper Text Preprocessor) dan ASP (Active Server Pages).



Gambar 2.5 Arsitektur Web server

Gambar 2.5 merupakan arsitektur dari web server. Client melakukan HTTP request ke web server dan web server akan mengembalikan request berupa halaman website meliputi HTML, image, CSS, dan javascript. Server juga dapat melakukan query atau request data ke database jika client ingin mengelola data. Database akan mengembalikan request dari server berupa data dan server menampilkannya berupa halaman web ke client. Dua contoh web server yang sering digunakan adalah Apache 15 dan IIS. Sedangkan database yang digunakan adalah MySQL, MySQL merupakan software sistem manajemen database (DBMS) yang sangat populer atau banyak digunakan untuk membangun aplikasi web sebagai sumber data. MySQL bersifat open source, mudah, dan cepat dalam mengeksekusi query.

2.2.4 PHP

PHP merupakan kependekan dari kata Hypertext Preprocessor. PHP adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML. Pemrograman PHP sangat cocok dikembangkan dalam lingkungan web, karena

PHP bisa dilekatkan pada script HTML atau sebaliknya. PHP dikhususkan untuk pengembangan web dinamis. Maksudnya, PHP mampu menghasilkan website yang secara terus-menerus hasilnya bisa berubah-ubah sesuai dengan pola yang diberikan. Hal tersebut bergantung pada permintaan client browser-nya (bisa menggunakan browser Opera, Internet Explorer, Mozilla, dan lain-lain).

Pada umumnya, pembuatan web dinamis berhubungan erat dengan database sebagai sumber data yang akan ditampilkan. PHP tergolong juga sebagai bahasa pemrograman berbasis server (serverside scripting). Ini berarti bahwa semua script PHP diletakkan di server dan diterjemahkan oleh web server terlebih dahulu, kemudian hasil terjemahan itu dikirim ke browser client. Secara teknologi, bahasa pemrograman PHP memiliki kesamaan antara bahasa ASP (Active Server Page), Cold Fusion, JSP (Java Server Page), ataupun Perl.

2.2.4.1 Tipe Data

PHP tidak memerlukan pendeklarasian tipe data suatu variable secara eksplisit, tetapi lebih ditentukan oleh runtime program PHP, tergantung pada konteks bagaimana variable tesebut digunakan

2.2.4.2 Jenis Tipe Data

PHP mendukung delapan jenis tipe data, antara lain:

1. Tipe scalar.

Tipe scalar tidak bisa dipecah lagi menjadi bagian yang lebih kecil, boleh dikatakan merupakan tipe dasar.

a. Boolean

   Boolean adalah jenis tipe data yang paling sederhana; banyak digunakan untuk mencari nilai kebenaran. Boolean bisa bernilai TRUE atau FALSE dan keduanya bersifat case insensitive.

b. Integer

   Integer adalah sederet angka yang dituliskan sebagai set Z={…,-2,-1,0,1,2,..}. Penulisan bilangan integer bisa dalam notasi desimal (10-based), heksadesimal (16-based), atau octal (8-based), termasuk penanda (-atau +). 50 Jika digunakan notasi octal, penulisan harus

didahului dengan angka 0 (nol) dan jika digunakan notasi heksadesimal, penulisan harus didahului dengan angka 0x;.

c. Float (floating point, ‘double’)

Jenis floating point merupakan bilangan pecahan dengan presisi tinggi. Termasuk dalam bilangan floating point, antara lain float, double, dan real. Besar ukuran tipe data float bergantung pada platform yang digunakan; secara umum adalah 1.8 x 10308 dengan tingkat presisi 14 digit desimal. Hal ini mengacu pada standar format 64 bit IEEE.

d. String

String boleh dikatakan sebagai serangkaian karakter. Besarnya karakter sama dengan byte. Ada tiga cara penulisan string yaitu:

1. Single quoted / petik tunggal

   Penulisan string dengan single quoted harus diawali dan diakhiri petik tunggal (‘…’). Cara ini sedikit membingungkan jika ada karakterkarakter khusus (escaped character) yang disertakan. Misalnya, jika ada karakter petik tunggal yang akan disisipkan, karakter tersebut harus didahului dengan backslash (\).

2. Double quoted / petik ganda

   Penulisan string dengan double quoted harus diawali dan diakhiri tanda petik ganda (“…”). Pada dasarnya, cara penulisan double quoted hampir 51 sama dengan single quoted, tetapi double quoted lebih fleksibel dan memiliki lebih banyak escaped character yang bisa disisipkan.

2. Tipe compound/Tipe campuran

a. Array

Array adalah sekumpulan data yang disimpan dalam suatu variable dengan nama yang sama. Untuk membedakan antara data satu dan data yang lain, digunakan index atau keys. Setiap data dalam array disebut element. Array dalam PHP sedikit berbeda dengan array pada bahasa pemrograman yang lain. Pada umumnya, setiap elemen array harus memiliki kesamaan tipe, tetapi hal tersebut tidak berlaku bagi PHP. Di dalam PHP, diperbolehkan adanya perbedaan jenis tipe data di setiap

elemen array, karena perlu diingat bahwa PHP tidak memerlukan pendeklarasian variabel, termasuk variabel array. Dengan kata lain, setiap elemen array bisa memiliki berbagai macam jenis tipe data yang tidak sejenis dalam satu nama variabel array. Array dapat diciptakan dengan pernyataan array() yang disertai dengan "key=>value" lebih dari satu, di setiap "key=>value" harus dipisahkan dengan tanda koma (",").

b. Object
c. Tipe special/Tipe khusus
d. Resource
e. Null

   Nilai null mewakili suatu variabel yang tidak memiliki nilai apa pun. Tipe null dikenali PHP sejak versi 4 ke atas. Beberapa kemungkinan jika variabel null terjadi:

   1. Jika variabel diberi nilai dengan konstanta NULL;
   2. Variabel belum diberi nilai atau belum di-set sama sekali;
   3. Jika perintah unset() dikenakan pada suatu variable

2.2.5 Penetration Testing

Penetration Testing adalah subclass dari etchical hacking yang terdiri dari kumpulan metode-metode dan prosedur-prosedur yang bertujuan untuk menguji atau melindungi sebuah keamanan organisasi. Menurut Baloch dalam buku Ethical Hacking and Penetration Testing Guide menyatakan bahwa Penetration Testing terbukti membantu dalam menemukan kerentanan-kerentanan di dalam sebuah organisasi dan sekaligus memeriksa apakah seorang penyerang mampu untuk menyerangnya untuk mendapatkan akses yang tidak sah terhadap suatu aset (Baloch, 2015). Pengujian dilakukan atas izin dari pemilik objek pengujian sehingga dibutuhkan persetujuan dalam menentukan batasan-batasan dalam ruang lingkup terhadap metode dan target yang akan diujikan.

Terdapat tiga jenis metode Penetration Testing yang terkenal, yaitu white-box testing, black-box testing, dan gray-box testing.

1. White Box

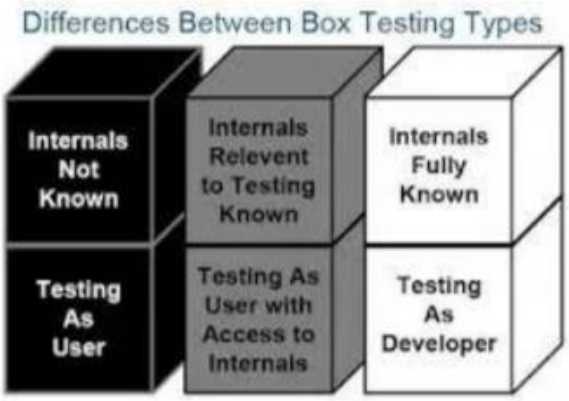
White box merupakan metode pengujian yang mendapatkan segala informasi secara penuh yang digunakan dari sistem tersebut seperti teknologi yang digunakan, source code yang ada didalamnya, dan lain sebagainya. Dapat disebut berperan sebagai developer.

2. Gray Box

   Gray box merupakan metode pengujian yang tidak secara penuh mendapatkan informasi didalamnya contohnya hanya diberi username dan password untuk login. Metode ini dapat dikatakan berperan sebagai pengguna yang ingin masuk kedalam sistem.

3. Black Box

   Black box sendiri adalah metode pengujian yang berkebalikan dari white box. Jika white box mendapatkan secara penuh informasi yang ada pada sistem, maka berbeda dengan black box yang sama sekali tidak mendapatkan informasi yang ada dalam sistem tersebut atau bisa disebut sebagai pengguna.

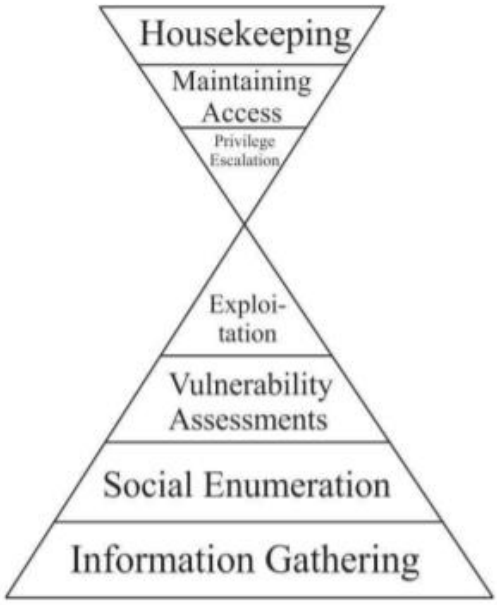


Gambar 2.6 Perbedaan Metode Penetration Testing

Berikut ini beberapa fase yang biasanya digunakan dalam penetration testing :

1. Information Gathering merupakan fase yang berguna untuk mendapatkan informasi dari target baik perseorangan maupun perusahaan,
2. Service Enumeration merupakan fase pengumpulan informasi yang dilakukan secara aktif bersinggungan dengan target,

3. Vulnerability Assessments merupakan fase yang dilakukan untuk mendeteksi, mengidentifikasi, dan mempelajari kelemahan yang terdapat pada suatu target,
4. Exploitation merupakan fase yang berguna untuk menyerang suatu target,
5. Privilege Escalation merupakan fase untuk meningkatkan hak istimewa untuk mengaksesnya agar pengguna dengan hak akses rendah tidak dapat masuk,
6. Maintaining Access merupakan fase untuk mempertahankan akses yang disusupi seperti mengambil sesi yang sudah ada sebelumnya dari ekspolitasi sistem dan layanan web untuk memfasilitasi akses berulang dan eksploitasi lebih lanjut dari sistem komputer dan infrastruktur jaringan yang terpasang.
7. Housekeeping merupakan fase yang berguna untuk memperbaiki celah pada sistem yang sudah di eksplotasi.



Gambar 2.7 Fase Penetration Testing

2.2.6 Metode ISSAF

ISSAF (The Information System Security Assessment Framework) adalah kerangka pengujian penetrasi yang memiliki beberapa keunggulan kontrol

keamanan, memiliki struktur intuitif yang dapat memberikan arahan kepada penguji sistem melalui langkah-langkah yang kompleks.

Framework ISSAF dikembangkan oleh OISSG (Open Information System Security Group). Metodologi uji penetrasi melalui Framework ISSAF dibuat untuk mengevaluasi jaringan, sistem dan kontrol aplikas. Framework ISSAF memberikan tahapan proses pengujian penetrasi secara optimal yang bertujuan memberikan arahan kepada auditor melakukan pengujian secara lengkap dan benar, serta menghindari kesalahan dalam melakukan pengujian serangan yang bersifat acak. Ada tiga langkah dalam kerangka kerja ISSAF yang meliputi persiapan dan perancangan, pengujian, serta pelaporan dan pembersihan jejak serangan.

ISSAF pada pedomannya menjelaskan proses uji penetrasi dilakukan untuk memberikan arahan pengujian secara benar dan lengkap, serta menghindari adanya kesalahan umum yang terkait dengan metode serangan yang dilakukan secara acak .

Berikut tahapan metode ISSAF :

1. Information Gathering

Tahap information gathering merupakan tahapan pengumpulan informasi secara umum yang dilakukan pada target. Informasi yang dikumpulkan meliputi informasi mengenai IP target, informasi mengenai registrant dan admin, informasi mengenai reverse DNS dan IP lookup, dan informasi umum lainnya.

2. Network Mapping

Tahap network mapping merupakan tahapan pengumpulan informasi secara spesifik mengenai jaringan pada target. Salah satu informasi yang dikumpulkan pada tahap ini meliputi informasi mengenai port TCP dan UDP pada sistem target.

3. Vulnerability Identification

Tahap vulnerability identification merupakan tahapan pemindaian website target untuk mengetahui kerentanan keamanan didalamnya. Pengujian pada penelitian ini menggunakan Vega Vulnerability Tools sebagai proses scanning untuk mengetahui kerentanan keamanan pada website.

4. Penetration

Tahap penetration merupakan tahapan simulasi serangan yang dilakukan pada website target yang bertujuan untuk memperoleh celah pada keamanan

sistem. Jenis serangan yang dilakukan pada tahap ini yaitu serangan Cross-Site Scripting (XSS) dan serangan SQL Injection yang dilakukan pada website target.

5. Gaining Access and Privilege Escalation

Tahap gaining access and privilege escalation merupakan tahapan pengujian dengan mencoba akses ke dalam sistem target. Jenis akses yang dilakukan pada penelitian ini adalah akses ke dalam sistem user admin dan akses ke dalam sistem Cpanel.

6. Enumerating Futher

Tahap enumerating further merupakan tahapan pengujian dengan melakukan pengambilan dan pemecahan seluruh informasi mengenai password yang diperoleh dari website target.

7. Compromise Remote User/Sites

Tahap compromise remote user/sites merupakan tahapan pengujian dengan melakukan eksploitasi akses ke dalam user root melalui hubungan jarak jauh/ remote pada website.

8. Maintaining Access

Tahap maintaining access merupakan tahapan pengujian dengan melakukan penanaman backdoor ke dalam sistem website target. Penanaman backdoor dapat dilakukan dengan memanfaatkan fitur file upload yang tersedia pada website target.

9. Covering Tracks

Tahap covering tracks merupakan tahapan terakhir dari pengujian penetration testing. Pengujian tahap ini yaitu dengan melakukan penghapusan log serangan yang telah dilakukan pada tahapan-tahapan sebelumnya.

2.2.7 Terminologi – Terminologi Dasar Dalam Keamanan Sistem

Berikut terminology dasar dalam keamanan sitem diantaranya:

2.2.7.1 Vulnearlbility

Vulnerability adalah Kelemahan dari sebuah aset atau sekumpulan aset yang dapat dimanfaatkan oleh satu atau lebih ancaman (ISO 27005). Sedangkan menurut definisi dariIETF (Internet Engineering Task Force) melalui RFC 2828

vulnerability adalah sebuah celah atau kelemahan dalam sebuah system, baik dalam desain, implementasi, atau operasional dan manajemen yang dapat dimanfaatkan untuk menyerang sebuah system informasi.

2.2.7.2 Threat

Dalam definisi yang diungkapkan oleh Id-SIRTII/CC (2016) threat atau ancaman adalah segala sesuatu yang memiliki potensi untuk mengganggu jalannya operasi, fungsi, integritas atau ketersediaan sistem informasi.

2.2.8 Serangan Siber

Serangan siber atau yang biasa disebut cyber crime merupakan kejahatan yang dilakukan oleh seorang atau pun kelompok yang mampu menggunakan teknologi informasi yang terkoneksi dengan internet sebagai alat kejahatan.

Menurut Murti (2005) cyber crime adalah sebuah istilah yang digunakan secara luas untuk menggambarkan tindakan kejahatan dengan menggunakan media komputer ataupun internet. Gregory (2015) menggemukan cyber crime adalah bentuk kejahatan virtual dengan memanfaatkan media komputer yang terhubung melalui internet, dan dapat mengekspolitasi komputer lain yang terhubung dengan internet. Keamanan sistem yang memiliki banyak celah dapat menyebabkan seorang hacker memanfaatkan celah keamanan untuk masuk ke dalam sistem, merusak serta mengambil data-data yang tidak seharusnya diketahui olah pihak luar.

Hacker merupakan istilah yang digunakan untuk menggambarkan seorang yang mempelajari, memodifikasi, menerobos masuk ke dalam komputer baik untuk kepentingan sendiri maupun kelompok. Berdasarkan beberapa pengertian tentang cyber crime diatas, dapat disimpulkan bahwa cyber crime adalah perbuatan melawan hukum yang dilakukan dengan menggunakan internet. Berdasarkan tindakan dan motif yang dilakukan oleh seorang yang melakukan cyber crime, menurut Hius, et al. (2014) permasalahan terbagi menjadi lima bagian yaitu:

1. Cybercrime sebagai tindakan kejahatan murni

   Tindakan kejahatan yang dilakukan secara disengaja, dimana orang tersebut secara sengaja dan terencana untuk melakukan pengrusakkan, pencurian, tindakan anarkis, terhadap suatu sistem informasi atau sistem komputer.

2. Cybercrime sebagai tindakan kejahatan abu-abu

   Tindakan kejahatan ini tidak jelas antara kejahatan kriminal atau bukan karena dia melakukan pembobolan tetapi tidak merusak, mencuri atau18 melakukan perbuatan anarkis terhadap sistem informasi atau sistem komputer tersebut.

3. Cybercrime yang menyerang individu

   Kejahatan yang dilakukan terhadap orang lain dengan motif dendam atau iseng yang bertujuan untuk merusak nama baik, mencoba ataupun mempermainkan seseorang untuk mendapatkan kepuasan pribadi. Contoh dari tindakan tersebut adalah: Pornografi, cyberstalking, dan lain-lain.

4. Cybercrime yang menyerang hak cipta (hak milik)

   Kejahatan yang dilakukan terhadap hasil karya seseorang dengan motif menggandakan, memasarkan, mengubah yang bertujuan untuk kepentingan pribadi atau umum ataupun demi materi atau non materi.

5. Cybercrime yang menyerang pemerintah

   Kejahatan yang dilakukan terhadap pemerintah sebagai objek dengan motif melakukan teror, membajak ataupun merusak keamanan suatu pemerintahan yang bertujuan untuk mengacaukan sistem pemerintahan, atau menghancurkan suatu Negara.

2.2.8.1 Shell Backdoor

Backdoor adalah sebuah program ataupun hasil pengkodean yang memungkinkan seseorang dapat mengakses secara remote komputer korban (tempat backdoor ditanam). Bisa disebut juga sebagai ’jalan belakang’ untuk masuk ke database komputer/website korban tanpa harus melalui form login.

2.2.8.2 Web Deface

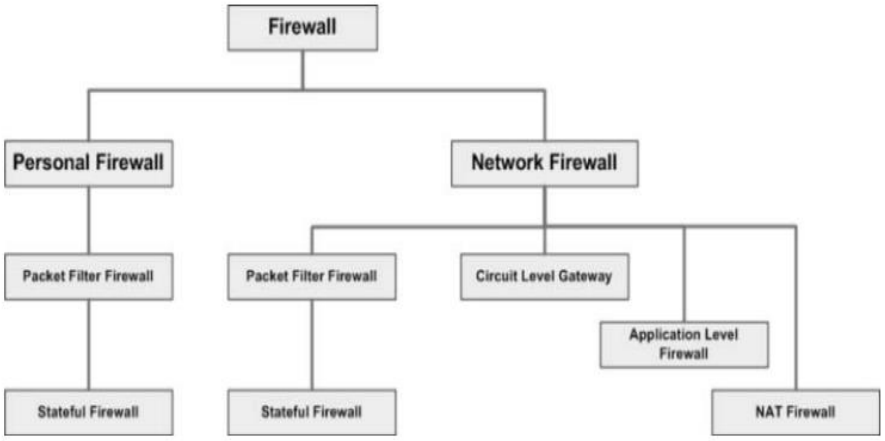
Web Deface merupakan jenis teknik serangan yang dilakukan oleh seorang hacker dengan mengubah halaman web tanpa diketahui oleh pemilik sah dari web tersebut. Perubahan tampilan web dapat berupa berubahnya gambar atau teks maupun link terhadap halaman web lain. Menurut CSIRT (2014), situs web yang dirusak umumnya memanfaatkan kerentanan yang terdapat pada web server untuk

mendapatkan shell root, kemudian menyuntikkan kode berbahaya ke halaman web target yang berada pada server.

Serangan seperti Sql Injection, Ddos, dan Web deface merupakan serangan siber yang bersifat teknis. Selain itu juga terdapat serangan yang bersifat non teknis seperti tsunami, letusan gunung berapi, kebakaran dan gempa bumi. Fenomena alam digolongkan sebagai serangan non teknis karena manusia dan sistem tidak bisa mengantisipasi kapan adanya bencana alam yang dapat merusak sistem.

2.2.9 Firewall

Firewall merupakan salah satu cara yang efektif unutk melindungi system dari ancaman terhadap keamanan jaringan komputer. Firewall perlu diterapkan karena dapat meningkatkan host security dari serangan para cracker bahkan hacker melalui celah-celah yang terbuka, seperti protocol UDP/TCP (panduan lengkap jaringan komputer, Lukmana, Lukas., 2004). Umumnya, sebuah firewall diimplementasikan dalam sebuah mesin terdedikasi, yang berjalan pada pintu gerbang (gateway) antara jaringan lokal dan jaringan lainnya. Firewall umumnya juga digunakan untuk mengontrol akses terhadap siapa saja yang memiliki akses terhadap jaringan pribadi dari pihak luar. Saat ini, istilah firewall menjadi istilah generik yang merujuk pada sistem yang mengatur komunikasi antar dua jaringan yang berbeda. Mengingat saat ini banyak perusahaan yang memiliki akses ke internet dan juga tentu saja jaringan korporat di dalamnya, maka perlindungan terhadap aset digital perusahaan tersebut dari serangan para hacker, pelaku spionase, ataupun pencuri data lainnya, menjadi esensial.



Gambar 2.8 Taksonomi Firewall

2.2.9.1 Jenis – Jenis Firewall

Firewall terbagi menjadi dua jenis, yakni sebagai berikut :

1. Personal Firewall

   Personal firewall didesain untuk melindungi sebuah komputer yang terhubung ke jaringan dari akses yang tidak dikehendaki. Firewall jenis ini akhir-akhir ini berevolusi menjadi sebuah kumpulan program yang bertujuan untuk mengamankan komputer secara total, dengan ditamb ahkannya beberapa fitur pengaman tamb ahan semacam perangkat proteksi terhadap virus, anti-spyware, anti-spam, dan lainnya. Bahkan beberapa produk firewall lainnya dilengkapi dengan fungsi pendeteksi gangguan keaman an jaringan (Intrusion Detection System). Contoh dari firewall jenis ini adalah Microsoft Windows Firewall (yang telah terintegrasi dalam sistem operasi Windows XP Service Pack 2, Windows Vista dan Windows Server 2003 Service Pack 1), Symantec Norton Personal Firewall, Kerio Personal Firewall, dan lain-lain. Personal firewall secara umum hanya memiliki dua fitur utama, yakni Packet Filter Firewall dan Stateful Firewall.

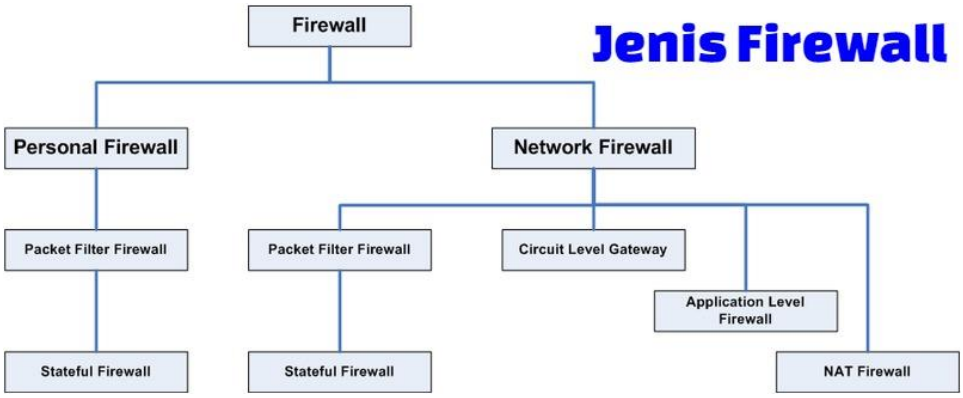
2. Network Firewall

   Network firewall didesain untuk melindungi jaringan secara keseluruhan dari berbagai serangan. Umumnya dijump ai dalam dua bentuk, yakni sebuah perangkat terdedikasi atau sebagai sebuah perangkat lunak yang diinstalasikan dalam sebuah server. Contoh dari firewall ini adalah

Microsoft Internet Security and Acceleration Server (ISA S erver), Cisco PIX, Cisco ASA, IPTables dalam sistem operasi GNU/Linux, pf dalam keluarga sistem operasi Unix BSD, serta SunScreen dari Sun Microsystems, Inc. yang dibundel dalam sistem operasi Solaris. Network Firewall secara umum memiliki beberapa fitur utama, yakni apa yang dimiliki oleh personal firewall (packet filter firewall dan stateful firewall), Circuit Level Gateway, Applica tion Level Gateway, dan juga NAT Firewall. Network firewall umumnya bersifat transparan dari pengguna dan menggunakan teknologi routing untuk menentukan paket mana yang diizinkan, dan mana paket yang akan ditolak.

Secara fundamental, firewall dapat melakukan hal-hal berikut:

1. Mengatur dan mengontrol lalu lintas data yang terjadi di dalam jaringan
2. Melakukan autentikasi terhadap akses
3. Melindungi sumber daya dalam jaringan privat
4. Mencatat semua kejadian danmelaporkan kepada administrator



Gambar 2.9 Jenis – Jenis Firewall

Pada firewall terjadi beberapa proses yang memungkinkan firewall dapat melindungi jaringan. Proses yang terjadi pada firewall ada tiga macam, yaitu:

1. Modifikasi header paket

   Digunakan untuk memodifikasi kualitas layanan bit paket TCP sebelum terjadi routing.

2. Translasi alamat jaringan

   Translasi alamat jaringan yang terjadi antara jaringan private dan jaringan public dapat berupa translasi satu ke satu (one to one) yang mana satu alamat IP private dipetakan ke satu alamat IP public, serta translasi banyak ke satu (many to one) yang mana beberapa alamat IP private dipetakan ke satu alamat IP public

3. Packet Filtering

   Berbagai kebijakan dapat diterapkan dalam melakukan operasi packet-filtering. Pada intinya, berupa mekanisme pengontrolan data yang diperbolehkan mengalir dari dan / atau ke jaringan internal, dengan menggunakan beberapa parameter yang tercantum dalam header paket data: arah (inbound atau outbound), address asal dan tujuan, port asal dan tujuan, serta jenis protokol transport. Router akan mengevaluasi informasi ini dalam setiap paket data yang mengalir melaluinya, kemudian menetapkan aksi yang harus dilakukan terhadap paket tersebut, berdasarkan set aturan / program dalam packet-filtering. Sehingga keputusan routing dasar router tersebut, kemudian dilengkapi dengan bagian dari kebijakan sekuriti jaringan.

2.2.9.2 Mengatur Dan Mengontrol Lalu Lintas Jaringan

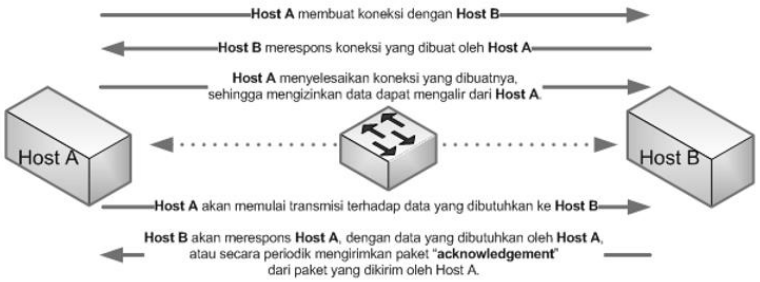
Fungsi pertama yang dapat dilakukan oleh firewall adalah firewall harus dapat mengatur dan mengontrol lalu lintas jaringan yang diizinkan untuk mengakses jaringan privat atau komputer yang dilindungi oleh firewall. Firewall melakukan hal yang demikian, dengan melakukan inspeksi terhadap paket-paket dan memantau koneksi yang sedang dibuat, lalu melakukan filtering terhadap koneksi berdasarkan hasil inspeksi paket dan koneksi tersebut. (Kaufman, 2002. p.13)

1. Proses inspeksi Paket

   Inspeksi paket (packet inspection) merupakan proses yang dilakukan oleh firewall untuk 'menghadang' dan memproses data dalam sebuah paket untuk menentukan bahwa paket tersebut diizinkan atau ditolak, berdasarkan

kebijakan akses (access policy) yang diterapkan oleh seorang administrator. Firewall, sebelum menentukan keputusan apakah hendak menolak atau menerima komunikasi dari luar, ia harus melakukan inspeksi terhadap setiap paket (baik yang masuk ataupun yang keluar) di setiap antarmuka dan membandingkannya dengan daftar kebijakan akses. Inspeksi paket dapat dilakukan dengan melihat elemen-elemen berikut, ketika menentukan apakah hendak menolak atau menerima komunikasi:

1. Alamat IP dari komputer sumber
2. Port sumber pada komputer sumber
3. Alamat IP dari komputer tujuan
4. Port tujuan data pada komputer tujuan
5. Protokol IP
6. Informasi head er-head er yang disimp an dalam paket



Gambar 2.10 Ilustrasi Firewall

2. Koneksi dan Keadaan Koneksi

   Agar dua host TCP/IP dapat saling berkomunikasi, mereka harus saling membuat koneksi antara satu dengan lainnya. Koneksi ini memiliki dua tujuan:

   1. Komputer dapat menggunakan koneksi tersebut untuk mengidentifikasikan dirinya kepada komputer lain, yang meyakinkan bahwa sistem lain yang tidak dapat mengirimkan data ke komputer tersebut. Firewall juga dapat menggunakan informasi koneksi untuk menentukan koneksi apa yang diizinkan oleh kebijakan akses dan menggunakannya untuk menentukan apakah paket data tersebut akan diterima atau ditolak.

2. Koneksi digunakan untuk menentukan bagaimana cara dua host tersebut akan berkomunikasi antara satu dengan yang lainnya (apakah dengan menggunakan koneksi connection-oriented atau connectionless).

Kedua tujuan tersebut dapat digunakan untuk menentukan keadaan koneksi antara dua host tersebut, seperti halnya cara manusia bercak ap-cakap. Jika Amir bertanya kepada Aminah mengen ai sesuatu, maka Aminah akan meresponnya dengan jawaban yang sesuai dengan pertanyaan yang diajukan oleh Amir. Pada saat Amir melontarkan pertanyaannya kepada Aminah, keadaan percakap an tersebut adalah Amir menunggu respon dari Aminah. Komunikasi di jaringan juga mengikuti cara yang sama untuk memantau keadaan percakapan komunikasi yang terjadi.

Firewall dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah firewall: state table) yang memantau keadaan semua komunikasi yang melewati firewall.