BAB II
LANDASAN TEORI

2.1 Cloud Computing

Cloud computing, merupakan suatu paradigma atau tren baru yang dimana suatu informasi secara permanen tersimpan di server (internet) yang disediakan oleh pihak ketiga dan tersimpan secara sementara di komputer pengguna (client) termasuk didalamnya adalah desktop, tablet komputer, laptop, dan lain-lain [1]. Dengan adanya cloud computing, muncullah tren baru di bidang komputasi terdistribusi dimana berbagai pihak (pengguna personal maupun perusahaan) dapat mengembangkan aplikasi dan layanan berbasis SOA (Service Oriented Architecture) di jaringan internet terlebih dengan cloud computing pengguna baik personal maupun perusahaan dapat menghemat biaya dalam mengembangkan aplikasi serta layanannya karena pengguna tidak perlu mengeluarkan cost berlebih dalam pengadaan hardware maupun software yang dimana merupakan syarat dalam menjalankan aplikasi dan layanannya, dan user hanya perlu menyediakan koneksi internet saja. Semua pengadaan hardware maupun software diserahkan kepada pihak ketiga dalam hal ini penyedia layanan cloud (Cloud Service Providers/CSP) dan pengguna hanya perlu menyewa dan membayar sesuai layanan yang disewanya.

Untuk mengetahui lebih jelas bagaimana implementasi cloud computing dapat digambarkan pada gambar 2.1.



Gambar 2.1 Implementasi Cloud Computing [7]

2.1.1 Jenis Cloud Computing

Dalam perkembangannya sampai saat ini, menurut Ono W. Purbo Cloud Computing terbagi menjadi dua jenis, yaitu: [2]

1. Private Cloud

   Merupakan layanan yang berada pada jaringan LAN (bisa berupa suatu perusahaan, instansi, sekolah yang berada pada area yang sama), dan biasanya untuk private cloud bersifat terbatas, atau artinya hanya orang tertentu yang bisa mengaksesnya. Contoh private cloud adalah Perwalian Online Unikom.

2. Public Cloud

   Sedangkan public cloud merupakan layanan cloud (untuk jenis layanannya dijelaskan di bagian selanjutnya) yang dijual oleh perusahaan menggunakan internet dan hampir semua orang yang terhubung bisa mengaksesnya, dengan kata lain untuk public cloud bersifat umum. Contoh public cloud adalah Facebook, Twitter, Amazon EC2 dan lain-lain. [2]

2.1.2 Jenis Layanan Cloud Computing

Ada berbagai macam layanan yang ditawarkan dalam cloud computing. Tetapi ada tiga jenis utama layanan dari cloud computing:

1. Infrastructure-as-a-Service (IaaS)

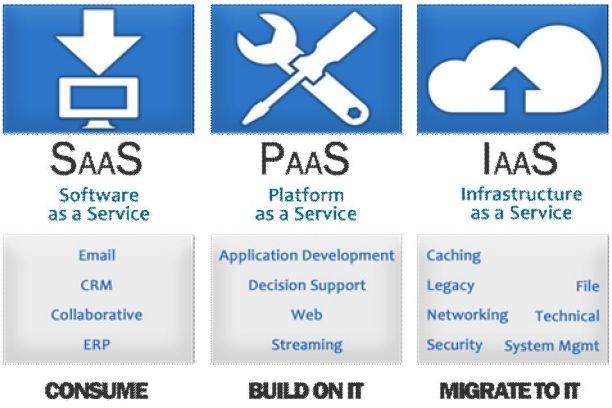
   IaaS merupakan suatu layanan yang disediakan oleh CSP yang dimana layanan yang ditawarkan adalah hardware computer (servers, networking technology, storage, dan data center space), selain layanan berbentuk perangkat keras, sistem operasi dan teknologi virtualisasi untuk mengelola sumberdayanya. Dengan kata lain pelanggan IaaS menyewa sumberdaya komputasi dibandingkan membeli dan memasangnya pada data center yang dimiliki pengguna. Contoh IaaS adalah Amazon EC2.

2. Platform-as-a-Service (PaaS)

   PaaS merupakan suatu layanan dimana yang disediakan pada layanan cloud adalah computing platform yang didalamnya termasuk kumpulan set-set pengembangan, middleware, dan kemampuan untuk menjalankannya secara langsung. Contoh PaaS adalah Windows Azure.

3. Software-as-a-Service (SaaS)

SaaS merupakan layanan cloud yang menawarkan layanan aplikasi sebagai layanan utamanya. Maksud dan contoh dari layanan aplikasi ini adalah yang salah satunya bisa menunjang produktivitas seperti aplikasi akunting, pengolah kata dan lain-lain. Contoh dari SaaS adalah Google Docs. Untuk lebih lengkapnya mengenai apa saja jenis layanan cloud computing, digambarkan pada gambar berikut. [8]



Gambar 2.2 Layanan Utama Cloud Computing [10]

2.2 Network Security

Network security atau keamanan jaringan merupakan suatu bidang yang terdiri dari ketentuan-ketentuan serta kebijakan-kebijakan yang diterapkan seorang administrator jarigan (Network Adminsistrator) untuk mencegah serta memantau/monitor akses yang tidak berhak (Unathorized Access), penyalahgunaan, modifikasi , atau penolakan dari sebuah jaringan computer dan sumber daya yang dapat diakses jaringan. Dengan kata lain, Network security memiliki tujuan yang paling utama yaitu, mengamankan jaringan. Karena, sifat internet yang bersifat terbuka yang artinya semua orang dapat terkoneksi pada internet. Dari semua orang yang terkoneksi ke internet tidak semuanya memiliki maksud baik, terkadang ada saja orang yang "menyalahgunakan" internet demi kepentingan pribadinya. Misalnya mencuri password dan username untuk mendapatkan suatu akses ke suatu sumber daya (web, file, rekening bank, dan lain-lain), menyalahgunakan akses yang dimiliki, melakukan penipuan, menyerang/melumpuhkan suatu situs/jaringan demi mendapatkan hak admin dari

situs/jaringan tersebut, dan ancaman serta serangan lainnya. Sehingga dari berbagai macam hal tersebut, Network Security menjadi perhatian lebih bagi para administrator jaringan dalam mengamankan jaringan. Berikut merupakan serangan ataupun ancaman yang ada di internet secara umum dan pada cloud computing secara khusus.

2.2.1 Jenis Serangan atau Ancaman Keamanan di Internet

Berikut merupakan contoh-contoh jenis serangan atau ancaman keamanan yang sering terjadi di internet.

2.2.1.1 Denial Of Service (DOS)

Serangan DOS atau DOS Attack merupakan suatu serangan yang dimana bertujuan untuk mendapatkan hak akses penuh pada server misalnya penyerang ingin mendapatkan suatu data di database server, menginstall program jahat (malware), dan lain-lain yang pada intinya melumpuhkan komputer target. DOS dilakukan dengan cara membanjiri server target dengan pesan-pesan ataupun permintaan secara terus-menerus dalam satu waktu, sehingga mengakibatkan server menjadi overload karena sumber daya (memory, CPU usage, bandwidth) yang dimiliki server tersebut habis terpakai melayani pesan dan permintaan datang.[7]

2.2.1.2 Spoofing (IP Spoofing)

Spoofing atau lebih sering dikenal dengan IP Spoofing merupakan suatu teknik atau cara yang digunakan untuk mendapatkan akses yang tidak berhak kepada komputer korban, dengan cara penyerang/penyusup mengirim pesan ke sebuah komputer dengan sebuah alamat IP yang menandakan pesan tersebut berasal dari host yang terpercaya. Dengan kata lain IP Spoofing adalah merubah/memodifikasi alamat sumber IP penyerang/penyusup pada IP Headers menjadi sebuah alamat IP baru yang terpercaya.

2.2.1.3 Sniffing (Packet Sniffing)

Packet Sniffing merupakan pencegatan data paket-paket yang mengalir pada jaringan. Dengan sebuah program Sniffer yang bekerja pada layer 2 serta kombinasi dari NIC yang berada pada mode promiscuous (mode mendengar)

untuk men-capture semua traffic yang mengalir dari dan ke internet pada suatu jaringan. Dengan demikian, semua aktivitas yang dilakukan oleh komputer yang berada pada jaringan tersebut dapat diketahui. Sniffing merupakan ancaman keamanan yang bersifat pasif karena tidak melibatkan penyerangan secara langsung, hanya mendengarkan traffic yang ada di jaringan.

2.2.1.4 Port Scanning

Port Scanning merupakan suatu usaha mengumpulkan informasi/reconnaissance terhadap suatu komputer target (biasanya server), yang dimana informasi yang dicari berupa layanan-layanan apa saja yang disediakan, sistem operasi komputer target dan lain-lain. Sehingga dari informasi yang didapatkan, dapat menentukan langkah selanjutnya dalam melakukan penyerangan.

2.2.1.5 Hijacking (Man-in-the-middle-attack/MITM)

MITM merupakan sebuah teknik yang mengambil keuntungan dari kelemahan protocol stack TCP/IP, dan bagaimana cara header-header dibangun. MITM terjadi ketika ada seseorang diantara 2 titik yang dimana kedua titik itu saling berkomunikasi, tetapi seseorang tersebut secara aktif memonitor, men-capture, dan mengontrol komunikasi 2 titik tersebut secara transparan. Dan pada akhirnya kedua titik tersebut tidak sadar bahwa mereka tidak berkomunikasi satu sama lain, tetapi padahal berkomunikasi dengan seseorang tersebut.

2.2.1.6 Trojans (Malicious Software/Malware)

Trojan merupakan sebuah program berbahaya yang pada penampilannya hanya berupa sebuah software/paket biasa yang dimana software/paket tersebut berisi kode-kode berbahaya begitu diluncurkan dan masuk ke komputer korban. Kebanyakan program remote control spyware merupakan jenis ini.

2.2.2 Jenis Serangan atau Ancaman Keamanan di Cloud Computing

Berikut merupakan jenis-jenis serangan/ancaman keamanan yang dapat terjadi pada Cloud Computing:

2.2.2.1 Data Stealing

Salah satu cara tradisional dan pendekatan paling umum dalam melakukan serangan terhadap suatu jaringan adalah menembus sebuah user account. User account dan password-nya dicuri dengan segala cara. Sebagai hasilnya dengan dicurinya data rahasia atau bahkan menghancurkan datanya, dapat merusak integritas storage dan keamanan cloud.

2.2.2.2 Flooding Attacks

Flooding attacks merupakan suatu bentuk serangan dari DOS yang dimana penyerang menyerang sistem cloud secara terbuka. Cara kerja flooding attacks ini adalah memanfaatkan sifat sistem cloud yang dimana secara berulang meningkat ukurannya ketika ada request lebih lanjut dari client, sistem cloud akan meninisialisasi permintaan layanan baru untuk memenuhi kebutuhan client. Sehingga secara dasar, Flooding attack ini yaitu mendistribusikan sejumlah besar permintaan non-sense untuk suatu layanan. Begitu penyerang melemparkan sejumlah besar permintaan, dengan menyediakan sumber daya lebih sistem cloud akan mencoba untuk bekerja melayani permintaannya, dan pada akhirnya sistem akan menghabiskan sumber daya dan tidak dapat menyediakan layanan terhadap permintaan normal dari user normal.

2.2.2.3 Malware Injection Attack

Merupakan suatu serangan yang dimana penyerang berusaha untuk menyuntikkan (inject) layanan atau kode jahat yang dimana terlihat seperti layanan yang valid yang berjalan di cloud. Jike penyerang berhasil, maka layanan cloud akan menderita dari eavesdropping (menguping). Ketika ada user cloud resmi yang ingin meminta layanan cloud maka user tersebut akan terkena virus/malware/spyware dari program jahat yang berhasil ditanam oleh penyerang sebelumnya di sistem cloud lewat internet.

2.2.2.4 Man-in-the-middle Attack (MITM)

Serangan yang dilakukan dengan cara menempatkan penyerang ditengah/diantara dua titik komputer yang sedang berkomunikasi (dalam hal ini pengguna cloud, dan cloud itu sendiri). Kapanpun penyerang dapat menempatkan dirinya sendiri di jalur komunikasi dua pengguna, sehingga terjadi kemungkinan

penyerang dapat menghadang ataupun memanipulasi komunikasi kedua titik tersebut.

2.3 Router

Router adalah peralatan jaringan yang dapat menghubungkan satu jaringan dengan jaringan yang lain. Fungsi dari Router adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya, melalui sebuah proses yang dikenal sebagai routing. Routing sendiri merupakan proses pemindahan data dari satu network ke network yang lain dengan cara meneruskan paket data melalui gateway. [4]

Router bekerja menggunakan routing table yang disimpan di memorinya untuk membuat keputusan tentang ke mana dan bagaimana paket dikirimkan. Router dapat memutuskan rute terbaik yang akan ditempuh oleh paket data. Perbedaan router dengan wireless router yaitu hanya media penghantarnya. apabila wireless router menghubungkan jaringan yang berbeda yang menggunakan gelombang mikro, sedangkan router menghubungkan jaringan yang berbeda yang menggunakan kabel. Peran router sangat penting dan krusial dalam jaringan sebab dengan adanya router suatu paket dapat disampaikan kepada jaringan yang berbeda. Berikut merupakan contoh Router yaitu Cisco Router 2600:



Gambar 2.3 Router Cisco 2600 [11]

2.4 PC Router

PC Router mempunyai pengertian secara umum yaitu sebuah komputer yang difungsikan sebagai router. Dengan kata lain PC Router merupakan sebuah komputer yang dimodifikasi sedemikian rupa hingga menjadi memiliki fungsi

sebuah router, yaitu memfasilitasi transmisi paket data yang ada di jaringan komputer. Sedangkan Linux Box merupakan suatu PC yang difungsikan sebagai Router dengan menggunakan Linux sebagai sistem operasinya. Router sangat banyak digunakan dalam jaringan berbasis teknologi protokol TCP/IP, dan router jenis itu disebut juga dengan IP Router. Selain IP Router, ada lagi AppleTalk Router, dan masih ada beberapa jenis router lainnya. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak router IP. PC Router memiliki beberapa kelebihan dibandingkan dengan Router stand-alone itu sendiri yaitu, karena Router yang digunakan dalam bentuk PC maka admin dapat menambahkan beberapa fitur pada PC Router-nya seperti bandwidth management, Proxy, Fitur keamanan seperti Firewall, Intrusion Detection System (IDS), serta fitur-fitur lainnya. Sehinggan PC Router memiliki fleksibilitas serta skalabilitas yang tinggi.

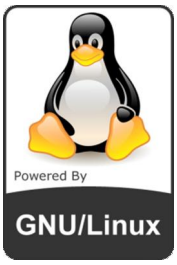
2.5 Sistem Operasi

Secara garis besar, sistem operasi merupakan perangkat lunak pada lapisan pertama yang ditempatkan pada memori komputer pada saat komputer pertama kali dinyalakan. Sedangkan perangkat lunak lainnya dijalankan setelah sistem operasi berjalan, dan sistem operasi akan melakukan layanan inti umum untuk perangkat lunak tersebut. Yang dimaksud dengan layanan inti umum adalah seperti akses ke disk, manajemen memori, scheduling task, dan user interface. Sehingga dengan demikian masing-masing perangkat lunak tidak perlu lagi melakukan tugas-tugas inti umum tersebut, karena dapat dilayani dan dilakukan oleh sistem operasi. Bagian kode yang melakukan tugas-tugas inti umum tersebut dinamakan dengan kernel.

2.5.1 Linux

Linux adalah sistem operasi yang bersifat open source dan bebas dibawah lisensi GNU (GNU is not unix), GPL (General Public License). Arti kata open source adalah pada linux kode sumber penyusun sistem operasi tersebut dapat dilihat oleh siapa saja tanpa harus menandatangani suatu perjanjian khusus. Arti kata bebas atau free bukan berarti bebas biaya tetapi mengacu pada kebebasan. Kebebasan disni adalah bebas untuk diduplikasikan, dimodifikasi, dan disebarluaskan baik untuk tujuan non-komersial maupun komersial.

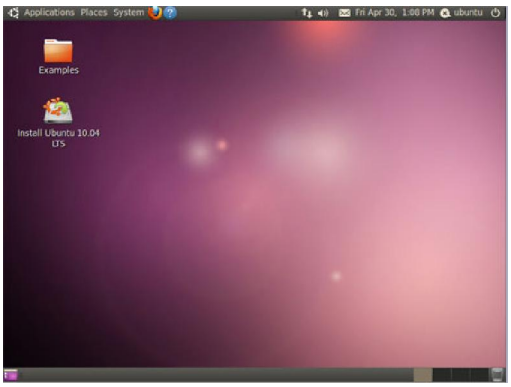
Linux lahir pada tahun 1991. Pada saat itu, Linus Torvald, seorang mahasiswa dari Suoen Tasavalta, Republik Finlandia memulai sebuah proyek pembuatan sistem operasi yan stabil dan bisa dijalankan pada mesin Intel x86. Pada awalnya, Linus Torvald menggunakan salah satu sistem operasi berbasis Unix yaitu Minix. Namun akhirnya Torvald merasa bahwa sistem ini memiliki banyak kekurangan, sehingga Torvald merasa dapat membuat sistem operasi yang lebih baik dari Minix. Pada bulan Oktober 1991, Linus Torvald mempublikasikan sistem operasi yang diberi nama Linux (Linus Unix). Torvald mengajak pengembang perangkat lunak di seluruh dunia untuk bersama-sama mengembangkan sistem operasi Linux. Dimulailah kemudian era open source.



Gambar 2.4 Logo Linux, Tux

Salah satu distro Linux yang terkenal dan paling banyak digunakan adalah Linux Ubuntu yang dimana merupakan turunan dari Debian. Ubuntu berasal dari bahasa kuno Afrika, yang berarti rasa perikemanusiaan terhadap sesama manusia. Tujuan dari Distribusi Linux Ubuntu adalah membawa semangat yang terkandung di dalam Ubuntu ke dunia perangkat lunak. Ubuntu tersedia secara bebas dan mempunyai dukungan baik yang berasal dari komunitas maupun tenaga ahli professional.

Ubuntu 10.04 LTS (Long Term Support) merupakan Distro Ubuntu yang dirilis pada bulan April tahun 2010 dan memiliki codename Lucid Lynx. Versi 10.04 LTS ini merupakan versi pembaruan dari Ubuntu 9.10 yang memiliki codename Karmic Koala. Salah satu pembaruannya adalah versi kernel yang pada ubuntu 9.10 memiliki versi 2.6.31 tetapi pada Ubuntu 10.04 memiliki versi kernel 2.6.32 yang dimana pada bulan Maret 2012 telah keluar versi kernel 2.6.39 untuk Ubuntu 10.04 LTS. Berikut contoh gambar dari Desktop Ubuntu 10.04 LTS:



Gambar 2.5 Desktop Linux Ubuntu 10.04 LTS

Ubuntu cocok digunakan baik untuk desktop maupun server. Ubuntu saat ini mendukung berbagai arsitektur computer seperti PC Intel x86, PC 64-bit, AMD64, PowerPC, dan lain-lain. Ubuntu menyertakan lebih dari 16.000 buah perangkat lunak, dan untuk instalasi desktop dapat dilakukan dengan menggunakan satu buah CD saja.

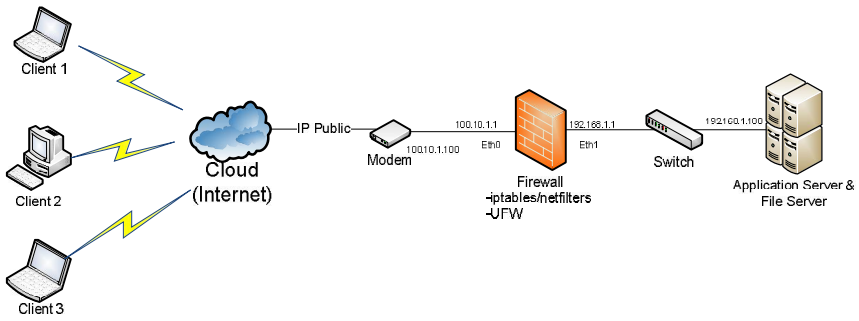
2.5.2 Windows

Microsoft Windows atau lebih dikenal dengan sebutan Windows adalah sistem operasi computer pribadi yang dikembangkan oleh Microsoft yangmenggunakan antarmuka berbasis grafik GUI (Grapichal User Interface). Sistem operasi Windows telah berevolusi dari MS-DOS, sebuah sistem operasi yang berbasis modul teks dan command-line. Sistem operasi Windows adalah sistem operasi yang paling banyak digunakan oleh masyarakat global.

Salah satu contoh sistem operasi buatan Microsoft yang terkenal dan popular adalah Windows XP. Windows XP merupakan sebuah sistem operasi yang dibuat dan dikembangkan oleh Microsoft untuk keperluan komputer personal, termasuk yaitu untuk desktop rumah, perkantoran, laptop dan media centers. Diluncurkan pertama kali pada 24 Agustus Tahun 2001, dan sampai tahun 2004 telah terjual 400 juta kopi di seluruh dunia. Windows XP merupakan sistem operasi penerus dari Windows 2000 dan Windows ME dan juga merupakan sistem operasi Windows kedua yang paling popular sampai tahun 2011 (yang pertama adalah Windows 7).

2.6 Firewall

Firewall merupakan suatu perangkat atau kumpulan dari software-software yang didesain untuk mengizinkan ataupun menolak transmisi jaringan yang didasarkan pada kumpulan peraturan-peraturan (rules) dan sering digunakan untuk melindungi suatu jaringan dari akses yang tidak diizinkan atau unauthorized access sementara mengizinkan komunikasi yang cocok untuk melewati firewall itu sendiri. Sehingga dalam perancangan firewall sangat bergantung kepada rules yang diterapkan pada firewall itu sendiri. Sekarang banyak sistem operasi dari PC menyertakan firewall yang berbasis Software untuk melindungi PC tersebut dari serangan maupun ancaman dari luar khususnya Internet. Selain berbasis software pada PC, banyak Router yang dapat mengizinkan data melewati jaringan yang dilindungi firewall, dan sebaliknya banyak firewall juga yang memiliki fungsi dasar routing.



Gambar 2.6 Contoh Firewall

Dalam perancangan sistem keamanan firewall itu sendiri terdapat dua pendekatan:

1. Negative List
2. Positive List

Berikut merupakan penjelasan lebih lengkap dari metode pendekatan pembangunan Firewall:

1. Negative List

   Negative List merupakan pembangunan sistem keamanan firewall dengan yang dilakukan pertama kali adalah membuka semua port dan memiliki Policy menerima semua paket yang masuk (Accept), lalu kemudian berpikir port apa

saja yang harus ditutup. Pendekatan ini dalam pembangunan firewall mudah dilakukan tetapi cenderung beresiko sistem keamanan yang nanti akan diterapkan tembus karena lupa menutup port. Sehingga pendekatan ini kurang aman bila dibandingkan menggunakan metode postitive list.

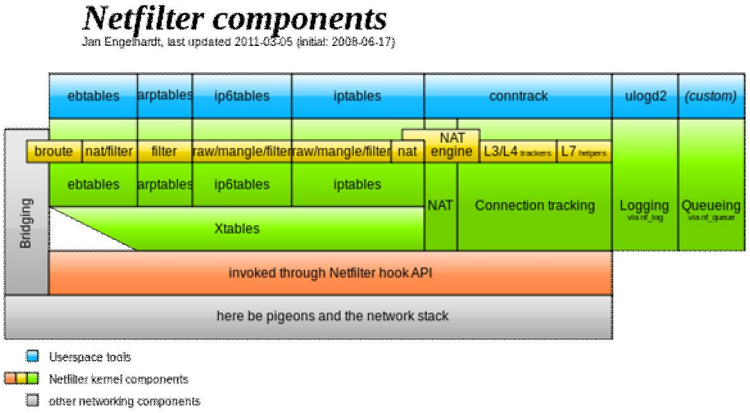
2. Positive List

   Positive List merupakan pembangunan sistem firewall yang dimana hal yang dilakukan pertama kali adalah menutup semua port yang ada dan menerapkan Policy Drop semua paket yang masuk. Pembangunan Firewall dengan melakukan pendekatan ini sangat rumit dan sulit tetapi sangat secure, karena semua port akan ditutup kecuali port yang digunakan dalam layanan cloud. [6]

2.6.1 Iptables/netfilters

Netfilter merupakan suatu framework atau lingkungan kerja yang menyediakan “hook handling” atau pengaturan langsung didalam Linux Kernel yang bertujuan untuk mencegah dan manipulasi dari paket-paket jaringan. Untuk lebih jelasnya, Netfilter bekerja dengan dipicu contohnya oleh packet reception dan routine-routine yang dikirim dari atau ke network interfaces (NIC). Dengan kata lain netfilters merupakan tools firewall yang sudah ada pada linux kernel.

Project Netfilters dimulai pada tahun 1998 oleh Rusty Russel yang dimana merupakan pemimpin project sebelumnya yaitu ipchains. Pada tahun 2000 netfilter dihasilkan dan dilisensi dibawah GNU General Public License (GPL) dan di bulan Maret tahun yang sama Netfilter dimasukkan kepada kernel linux versi 2.3. Berikut merupakan gambar komponen-komponen pada netfilters. [6]



Gambar 2.7 Komponen-komponen pada netfilter [6]

Sedangkan iptables merupakan sebuah program aplikasi untuk user yang dimana mengizinkan seorang admin sistem untuk mengkonfigurasi tabel-tabel firewall yang telah disediakan pada Linux Kernel (dalam hal ini netfilters) dan rantai-rantai atau biasa disebut dengan chains dan peraturan-peraturan atau rules yang disimpannya. Modul kernel dan program yang berbeda juga digunakan untuk protokol yang berbeda pula, contoh iptables untuk IPv4, ip6tables untuk IPv6, arptables untuk ARP, dan ebtables untuk frame Ethernet.

Sebelum adanya iptables, paket-paket software yang lebih banyak digunakan untuk pembuatan firewall linux adalah ipchains pada kernel 2.2 dan ipfwadm pada kernel 2.0, yang dimana ipfwadm didasarkan pada firewall BSD, yaitu ipfw. Keduanya, ipchains dan ipfwadm merubah kode-kode jaringan sehingga dapat memanipulasi paket-paket, tetapi tidak ada framework untuk general-packet control sampai adanya netfilter.

2.6.1.1 Tabel-tabel Iptables

Semua paket yang diperiksa oleh iptables, melewati beberapa tahap antrian dari tabel yang ada didalam iptables untuk diproses paket tersebut. Setiap dari antrian tersebut ditujukan untuk menangani paket secara khusus berdasarkan perilakunya dan antrian tersebut dikendalikan oleh rantai (chain) transformation/filtering packet yang berhubungan

Pada iptables secara default terdapat 3 tabel (table) secara keseluruhan yaitu tabel filter, nat dan mangle. Berikut merupakan penjelasan lebih lengkapnya. Berikut merupakan tabel-tabel pada iptables secara keseluruhan:

1. Tabel Filter

   Tabel Filter merupakan tabel default dari iptables, Jadi ketika admin tidak mendefinisikan tabelnya maka secara otomatis dianggap menggunakan tabel filter. Tabel Filter bertanggung jawab untuk melakukan antrian filter untuk packet yang datang atau dengan kata lain melakukan packet filtering.
2. Tabel NAT

   Tabel NAT merupakan tabel atau antrian yang dimana bertanggung jawab untuk melakukan Network Address Translation (NAT), atau dengan kata lain bertanggung jawab untuk melakukan “penerjemahan alamat jaringan”.

3. Tabel Mangle

   Tabel Mangle (Penghalusan) merupakan tabel yang dikhususkan untuk menangani packet alteration (pengubahan paket). Pengubahan ini salah satunya merubah bit-bit pada QOS (Quality of Service) di TCP Header. Tabel ini sangat jarang digunakan untuk lingkungan SOHO (Small Office Home Office).

2.6.1.2 Chains

Chains (rantai) merupakan suatu kumpulan dari rules (peraturan-peraturan) yang dimana digunakan untuk menentukan apa yang harus diperlakukan terhadap suatu packet. Dengan kata lain, Chains merupakan suatu wadah/tempat untuk menyimpan rules yang akan kita buat pada firewall. Chains terletak/dikelompokkan di dalam tabel. Berikut merupakan penjelasan lebih detilnya:

1. Tabel Filter

   Pada Tabel Filter memiliki Chains sebagaimana berikut:

   a. INPUT chain

      Ditujukan untuk paket yang datang (masuk) ke firewall. Paket yang diperuntukkan untuk server/PC Router.

   b. OUTPUT chain

      Ditujukan Paket yang keluar dari firewall. Dengan kata lain paket yang dihasilkan secara lokal dan pergi keluar dari server lokal/PC Router.

   c. FORWARD chain

      Ditujukan Packet yang diperuntukkan untuk NIC (Network Interface Card) lain pada server lokal/PC Router. Dengan kata lain untuk packet yang di-route melewati lokal server.

2. Tabel NAT

   Pada tabel NAT memiliki Chains sebagaimana berikut:

   a. PREROUTING chain

      Mengubah packest sebelum proses Routing. Artiya Packet Translation (penerjemahan paket) terjadi secepatnya begitu paket datang ke sistem (dan sebelum proses routing). Ini membantu untuk menterjemahkan tujuan

alamat IP paket yang sebagaimana cocok untuk di-routing pada lokal server. Chain ini digunakan untuk proses DNAT (Destination NAT).

b. POSTROUTING chain

Mengubah packets sesudah proses Routing. Artinya Packet Translation (penerjemahan paket) terjadi ketika packet meninggalkan sistem. Ini membantu untuk menerjemahkan alamat IP sumber dari paket yang sebagaimana cocok untuk proses routing pada server tujuan. Chain ini digunakan untuk proses SNAT (Source Address).

c. OUTPUT chain

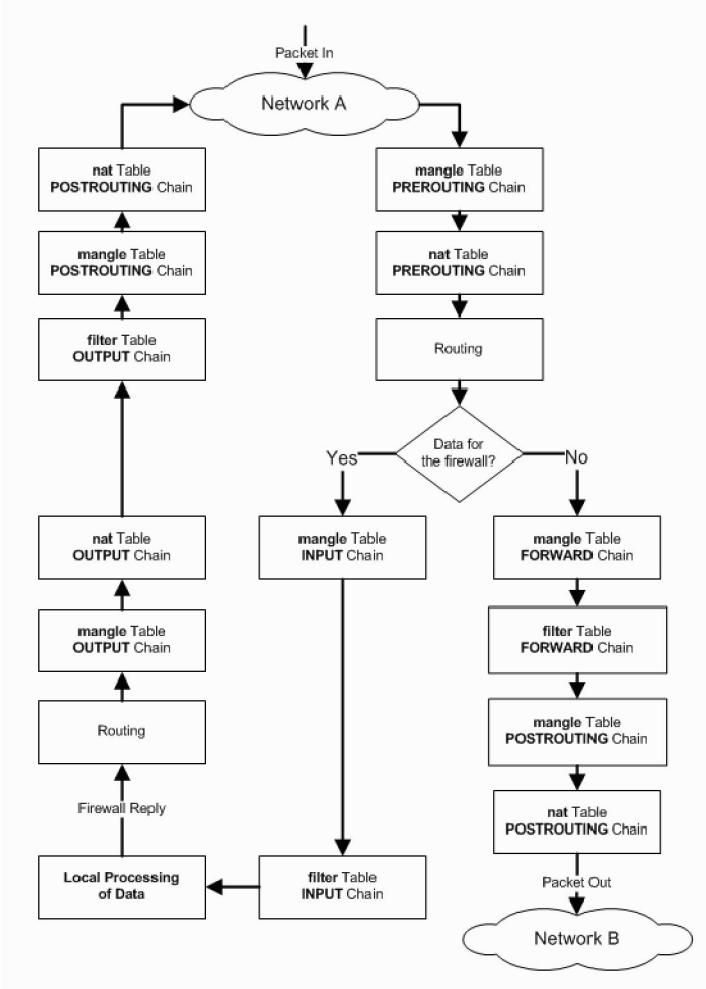
Proses NAT yang dimana paket dihasilkan secara lokal pada firewall.

3. Tabel Mangle

Pada tabel Mangle memiliki Chains berikut:

a. INPUT chain
b. FORWARD chain
c. OUTPUT chain
d. PREROUTING chain
e. POSTROUTING chain
f. FORWARD chain

Agar lebih jelas, berikut merupakan gambar bagaimana paket mengalir melewati tabel dan chains pada iptables:



Gambar 2.8 Diagram Alir Packet Flow [5]

2.6.1.3 Rules Iptables

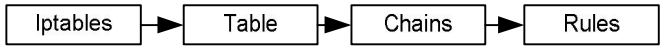
Rules merupakan suatu aturan-aturan yang dimana dibuat oleh admin untuk menentukan bagaimana seharusnya suatu packet diperlakukan. Rules disimpan pada chains dari suatu tabel di iptables [5].

Misalkan apabila PC Router ingin menolak/Drop semua packet icmp yang masuk dari jaringan luar (internet) lewat NIC eth0 tanpa memberikan balasan kepada yang mengirimnya, yaitu:

```
Iptables –A INPUT –i eth0 –p tcp icmp --icmp-type echo-request –j DROP
```

Maksud dari syntax diatas adalah memasukkan sebuah rule pada chain INPUT di tabel Filter (karena tidak didefinisikan maka otomatis rule tersebut ditujukan untuk tabel Filter) yang dimana mendefinisikan bahwa permintan paket TCP ICMP yang masuk dari eth0 untuk PC Router, agar ditolak permintaannya tanpa memberikan balasan.

Sehingga dengan kata lain, berikut merupakan diagram blok bagaimana struktur packet di iptables diperlakukan:



Gambar 2.9 Struktur Diagram Blok Iptables

2.7 Psad (Port Scanner Attack Detector)

Psad merupakan suatu software yang pada dasarnya merupaka suatu tools untuk melakukan log analysis dengan menggunakan pesan-pesan log iptables untuk mendeteksi, memberikan alert kepada admin dan (secara opsional) dapat mem-blok suatu port scans dan traffic mencurigakan lainnya (IDS/Intrusion Detection System) . Untuk TCP Scans, psad menganalisis TCP Flags untuk menentukan tipe scan (syn, fin, xmas, dan lain-lain) dan opsi command line yang bersangkutan agar nmap melakukan scan tersebut. Psad memasukkan banyak signature dari Snort IDS untuk mendeteksi probes dari berbagai macam backdoor programs (contoh EvilFTP, SubSeven), DDoS tools (mstream, shaft) dan advanced port scans (FIN, NULL, XMAS) yang dimana mudah dilakukan terhadap sistem dengan menggunakan nmap. [3]

Cara kerja psad secara umum adalah psad membaca semua iptables log data secara default yang disimpan pada file /var/log/messages. Dengan men-parsing (menerjemahkan) firewall log messages, psad menyediakan dengan data yang merepresentasikan paket-paket yang telah di-log (dan mungkin di drop) oleh policy dan rules iptables yang berjalan. Dengan kata lain, psad diberi masukan dengan sebuah data stream murni yang secara eksklusif mengandung paket-paket yang oleh firewall ditentukan tidak cocok untuk masuk ke dalam jaringan. Psad terdiri dari tiga daemons (modul/program yang berjalan di system), yaitu psad,kmsgsd, dan psadwatchd. Berikut merupakan penjelasan lebih detilnya:

1. Psad

   Psad bertanggung jawab untuk memproses semua paket yang telah di-log oleh firewall dan mengaplikasikan signature logic dengan tujuan agar dapat menentukan tipe scan/serangan apa yang digunakan kepada sistem atau jaringan.

2. Kmsgsd

   Kmsgsd bertanggung jawab untuk membaca semua pesan yang telah ditulis pada /var/lib/psad/psadfifo yang bernama pipe dan menulis pesan apapun yang cocok terhadap suatu regular expression (atau string) ke /var/log/psad/fwdata. Kmsgsd hanya digunakan jika variabel ENABLE_SYSLOG_FILE disabled pada psad.conf .

3. Psadwatchd

   Psadwatchd merupakan sebuah software watchdog (pengawas) yang akan men-restart kedua daemon yang lain ketika daemon tersebut mengalami kegagalan/mati karena suatu alasan.

Psad pertama kali dikembangkan pada akhir tahun 1999 yang dimana pada saat itu masih bagian dari software project Bastille Linux, yang dimana dimulai ketika tim pengembangan memutuskan bahwa Bastille seharusnya menawarkan sebuah komponen NIDS yang ringan. Pada waktu yang sama, Peter Watkins juga sedangkan mengembangkan script firewall yang bagus yang masih dibundel dengan Bastille sampai sekarang, sehingga merupakan hal yang alami untuk melakukan langkah selanjutnya untuk mngembangkan sebuah tools IDS berdasarkan informasi yang disediakan dalam log iptables. Pada tahun 2001, Michael Rash memisahkan proyek Bastille-NIDS menjadi proyeknya sendiri yang dimana dapat berjalan dengan sendirinya tanpa dibutuhkan Bastille harus diinstal pada sistem, dan proyek tersebut bernama Port Attack Scanner Detector (Psad).[3]

2.7.1 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) merupakan suatu sistem keamanan yang bekerja dengan cara melakukan pengawasan terhadap paket yang ada pada jaringan serta pengawasan kegiatan-kegiatan paket yang mencurigakan dalam jaringan. Jika ditemukan paket atau kegiatan yang mencurigakan dalam jaringan,

IDS secara umum akan memberikan peringatan kepada sistem atau administrator jaringan. Tetapi secara khusus selain memberi peringatan kepada sistem atau admin jaringan, secara native IDS dapat juga reaktif terhadap paket atau kegiatan mencurigakan tersebut. Salah satu caranya dengan melakukan pemblokiran user atau alamat IP sumber dari paket mencurigakan tersebut. IDS sendiri terbagi menjadi beberapa macam, yaitu:

1. Active and Passive IDS

   Active IDS (atau lebih dikenal dengan Intrusion Prevention System/IPS), merupakan sebuah sistem yang dikonfigurasi/diatur untuk memblok suatu serangan yang sedang berlangsung tanpa "ikut campur" pengguna/user. Dengan kata lain, IPS secara otomatis memblok serangan tersebut tanpa perlu admin turun tangan.

   Sedangkan, Passive IDS merupakan sebuah sistem yang dikonfigurasi hanya untuk memonitor/memantau dan menganalisa aktivitas trafik jaringan dan meng-alert operator ketika ada celah potensial dan serangan. Passive IDS tidak dapat secara otomatis melindungi jaringan dengan sendirinya.

2. Network-based and Host-based IDS

   Network-based IDS terdiri dari sebuah peralatan jaringan (atau sensor) dengan NIC-nya yang beroperasi dalam mode promiscuous (mode mendengar) dan sebuah management interface yang terpisah.

   Host-based IDS membutuhkan program-program kecil (atau biasa disebut agents) untuk diinstal pada sistem individu untuk dimonitor. Agents tersebut memonitor sistem operasi dan menulis data untuk mencatat (log) file dan/atau men-trigger alarms.

3. Knowledged-based and Behavior-based

   Knowledge-based (atau sering disebut Signature-based) merupakan sebuah IDS yang memiliki basis data yang berisi profil-profil serangan sebelmnya dan celah sistem yang diketahui untuk mengidentifikasi usaha penyusupan. Knowledge-based merupakan IDS yang lebih umum digunakan dibandingkan Behavior-based.

   Behavior-based (atau sering disebut Anomaly-based) merupakan IDS yang dimana mendeteksi suatu penyusupan/serangan dengan cara membandingkan

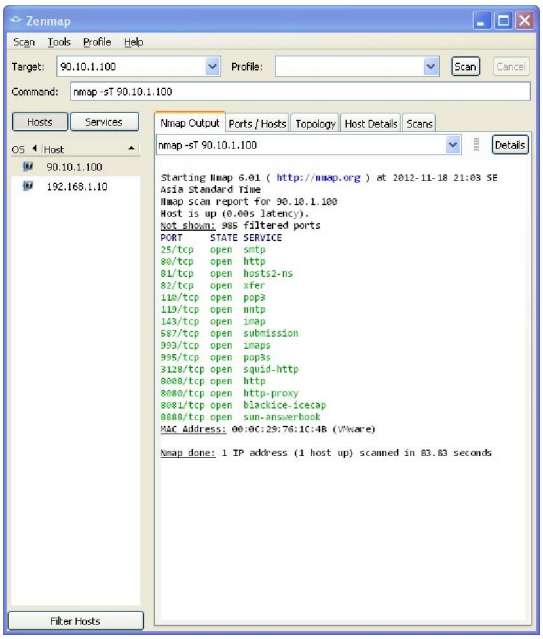
trafik yang sedang discan dengan trafik dalam keadaan normal. Penyimpangan dari keadaan trafik normal ini yang dianggap sebagai sebuah serangan.

2.8 Nmap (network mapper)

Nmap (Network Mapper) merupakan sebuah tools open source yang paling terkenal dan telah menjadi standar de facto bagi para security analyst serta hackers untuk melakukan eksplorasi dan audit keamanan jaringan. Nmap dirancang untuk memeriksa jaringan besar secara cepat, meskipun dapat pula memeriksa jaringan dengan skala yang lebih kecil Nmap menggunakan paket IP raw dengan cara yang kompleks untuk menentukan host mana saja yang tersedia pada jaringan, layanan yang tersedia, system operasi (serta versinya) apa yang digunakan, apa jenis firewall/packet filtering yang digunakan, dan sejumlah karakterisktik lainnya terhadap suatu komputer/jaringan. [14]

Output nmap adalah sebuah daftar target yang diperiksa, dengan informasi tambahannya tergantung pada opsi yang digunakan. Output nmap biasanya berbentuk tabel yang dimana tabel tersebut berisi daftar angka port dan protocol, nama layanan, dan status. Statusnya adalah `open`, `filtered`, `closed`, atau `unfiltered`. `open` berarti aplikasi pada komputer target sedang mendengarkan (listening) untuk koneksi/paket pada port tersebut. `filtered` berarti sebuah firewall, packet filtering, atau penghalang jaringan lainnya memblokir port sehingga nmap tidak dapat mengetahui apakah itu `open` atau `close`. `close` berarti port tidak memiliki aplikasi yang sedang mendengarkan port tersbut, meskipn port tersebut dapat terbuka kapanpun. Port digolongkan `Unfiltered` ketika port menanggapi probe dari nmap, namun nmap tidak dapat menentukan apakah port tersebut terbuka atau tertutup.

Nmap biasanya digunakan dengan menggunakan mode CLI (Command Line Interface), tetapi sekarang telah ada nmap dengan mode GUI (Graphical User Interface) yaitu bernama Zenmap.



Gambar 2.10 Zenmap dan contoh Output.

2.9 Hping3

Hping3 merupakan suatu tools packet generator (penghasil paket) yang didistribusikan oleh Salvatore Sanfilipo (atau lebih dikenal dengan nama antirez). Sama dengan Nmap, Hping3 merupakan tools de facto bagi para security analyst, hackers dan network administrator untuk melakukan audit keamanan jaringan dan ujicoba firewall dan teknik idle scan dari Hping3 diimplementasikan juga kepada Nmap. Hping3 menggunakan bahasa TCL (Tool Command Language) dan mengimplementasikan sebuah engine berbasis string yang dimana yang dapat dibaca oleh manusia dari deskripsi paket TCP/IP sehingga programmer dapat menulis suatu script yang berkaitan dengan manipulasi paket TCP/IP di pada tingkatan Low Level dengan waktu yang singkat.