BAB II

LANDASAN TEORI

2.1 Network Protocol Analyzer

*Network Protocol Analyzer*adalah sebuah tool yang ditujukan untuk menganalisa paket data jaringan dalam hal ini tool yang digunakan adalah wireshark. Wireshark mmelakukan pengawasan paket secara nyata (*real time*) dan kemudian menangkap data dan menampilkannyaselengkap mungkin. Wireshark bisa digunakan secara gratis karena aplikasi ini berbasis *open sources.* Aplikasi wireshark dapat berjalan di banyak *platform*, seperti linux, windows dan Mac.

Ada banyak ha yang dapat dilakukan dengan wireshark. Berikut adalah contoh skenario yang mungkin menggambarkan kapan menggunakan wireshark.

1. Melakukan *troubleshoot* permasalahan jaringan.
2. Melakukan pengujian masalah keamanan.
3. Malakukan *debugging* implementasi protokol.
4. Belajar protokol jaringan.

Wireshark diibaratkan sebagai media tool sehingga pemakaiannya diserahkan kepada penggunanya, apakah untuk kebaikan atau kejahatan. Hal ini karena wireshark dapat digunakan untuk mencuri informasi sensitif yang berkeliaran pada jaringan seperti kata sandi, *cookie* dan sebagainya.

2.1.1 Fitur Wireshark

Wireshark dapat dikatakan sebagai tool analisis paket data jaringan yang paling sering digunakan. Berikut adalah sebgaian fitur pada wireshark.

1. Tersedia untuk *platform* UNIX, Linux, Windows dan Mac**.**
2. Dapat melakukan *capture* paket data jaringan secara real time.
3. Dapat menampilkan informasi protokol secara lengkap.
4. Paket data dapat disimpan menjadi file dan nantinya dapat dibuka kembali.
5. Pemfilteran paket data jaringan.
6. Pencarian paket data dengan kriteria spesifik.
7. Pewarnaan penampilan paket data sehingga mempermudah penganalisisan paket data
8. Menampilkan data statistik.

Wireshark memerlukan antarmuka fisik untuk menangkap paket data yang keluar-masuk antar muka. *Wireshark* mendukung antar muka jaringan sebagai berikut.

1. ATMoth.
2. Bluetooth.
3. Tautan (*link*) CiscoHDLC.
4. DOCSIS.
5. Ethernet.
6. FrameRelay.
7. IRDA.
8. Tautan PPP.
9. SS7.
10. TokenRing.
11. USB.
12. LAN.

Selain antar muka fisik, wireshark juga mendukung antarmuka virtual, seperti Loopback, Pipes, VLAN danWinCapRemote.

2.2 *Network Attack*

Network attacks dapat dikategorikan menurut letak dapat dibagi menjadi dua yaitu network attacks yang berasal dari dalam network itu sendiri dan network attacks yang berasal dari luar network. Bentuk network attacks dapat berasal dari sebuah host dan dapat juga berupa sebuah device/perangkat keras yang berhubungan dengan target, sebagai contoh kasus wiretapping. Yang menjadi sasaran atau target dari sebuah attacks dapat berupa host maupun network itu sendiri.

Jika diasumsikan bahwa pengamanan terhadap infrastruktur dari sebuah network telah dilakukan, maka yang perlu diwaspadai adalah serangan dari luar network, dimana hanya proteksi saja yang dapat diandalkan untuk menghindari bahaya dari network attacks yang berasal dari luar.

Untuk mengetahui bagaimana cara untuk memproteksi sebuah network dari attacks yang berasal dari luar network maka ada baiknya mengetahui apa yang menjadi motifasi adanya sebuah attacks (Bayu Krisna, 2003).

Berdasarkan tujuannya maka network attacks dapatdibedakan menjadi beberapa kategori yaitu:

1. Berbahaya

Attack terjadi karena seseorang atau sekelompok orang bermaksud untuk melumpuhkan sistem, mencuri atau memodifikasi data dari sebuah network atau memanfaatkan *resource* yang dimiliki oleh *network sistem* yang diserang.

2. Tidak berbahaya

Attack yang terjadi akibat kelalaian atau ketidak sengajaan seseorang dan tidak sama sekali tidak pernah berniat untuk melakukannya.

Jika dilihat dari tujuan seseorang dalam melakukan *attack* maka dapat dibedakan menjadi:

a. Kontrol Akses

Attacker ingin menguasai secara penuh akses pada sebuah target.*Attacker* dapat melakukan apa saja setelah mendapatkan akses penuh pada sebuah target termasuk didalamnya melangsungkan *attack* berseri ke target lain.

b. Pemanfaatan *Resources*

Attacker ingin memanfaatkan *resource* yang tersedia pada sistem atau network seperti CPU dan koneksi internet.

c. Pencurian dan Manipulasi Data

Sistem atau network memiliki data yang diinginkan oleh *attacker*, data tersebut dapat berupa informasi penting seperti: profil kesehatan seseorang, laporan keuangan, atau rencana kerja sebuah perusahaan.

d. Merusak dan Menghancurkan

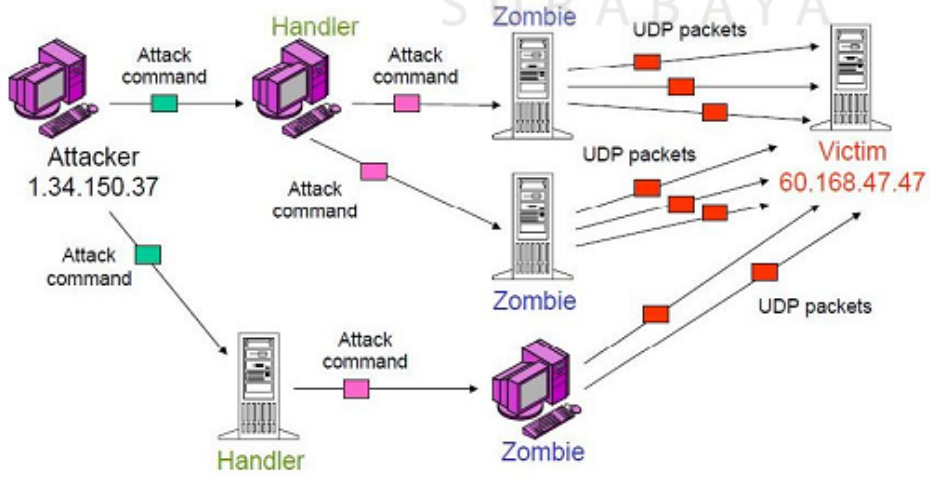
Attacker bermaksud merusak atau menghancurkan sebuah sistem atau network. Biasanya *attack* yang seperti ini didasarkan oleh alasan personal atau permintaan orang lain.

e. Just for Fun

Dalam beberapa kasus, seringkali ditemukan attacker hanya bermaksud untuk pamer dikomunitasnya dengan melakukan *attack* pada sistem atau network yang terkenal.

2.2.1 Proses Serangan dalam Jaringan

Serangan atau *attacks* pada sebuah network biasanya mempunyai proses atau tahap atau fase yang harus dilalui. Disini kami memberikan tiga buah fase yang dilalui oleh *attackers.*Fase pertama adalah fase persiapan. Dalam fase persiapan, attacker akan mengumpulkan informasi sebanyak mungkin mengenai target yang menjadi sasaran mereka. Fase kedua adalah fase eksekusi, fase ini merupakan attack yang sebenarnya dimana attacker melangsungkan attack pada sebuah sistem.Antara fase pertama dan fase kedua terkadang ditemui kasus dimana saat fase pertama berlangsung, berlangsung juga fase kedua. Contoh *scanning* untuk mendapatkan informasi pada sebuah host sama dengan attack pada network yang melingkupinya. Fase ketiga adalah fase akhir yang kami sebut dengan fase *post-attack*.Fase ketiga merupakan fase akibat dari fase pertama dan fase kedua.Bisa jadi terjadinya kerusakan pada sebuah network, atau dikuasainya sebuah sistem network yang kemudian digunakan kembali oleh *attacker* untukmelakukan serangan pada sistem network lainnya (Bayu Krisna, 2003).



Gambar 2.1.*Attack* dalam topologi jaringan (Zenhadi, 2011)

2.2.2 Beberapa Jenis Serangan Secara Umum

Adapun beberapa jenis *network attack* secara umum yang dapat mengancam sebuah sistem keamanan jaringan, bebrapa di antaranya adalah (http://technet.microsoft.com/en-us/library) :

1. *Eavesdropping*

Eavesdropping adalah penyadapan informasi di jalur transmisi privat.Misalnya adalah yang dilakukan oleh Mark Koenig sebagai konsultan dari GTE.Dia menyadap informasi penting lewat telpon dari nsabah-nasabah Bank of America dan menggunakan informasi tersebut untuk membuat sebanyak 5500 kartu ATM palsu.

2. Modifikasi Data

Setelah attacker berhasil menyadap dan membaca data, langkah yang paling mungkin dilakukan attacker adalah merubah atau memodifikasi data dalam *packet*tanpa sepengetahuan pengirim dan penerima.

3. Identity Spoofing (IP Address Spoofing)

IP Spoofing merupakan salah satu teknnik untuk menyusup ke dalam suatu sistem komputer.Teknik yang digunakan adalah degan melakukan pemalsuan IP penyerang (*attacker*). Suatu contoh dari *IP Spoofing* adalah sebagai berikut:

a. *IP Address* komputer sumber yang digunakan untu mengirim data adalah 203.45.98.1
b. *IP Address* komputer yang akan dijadikan sebagai target adalah 202.14.12.1
c. *IP Address* sistem yang akan digunakan untuk mengiri data adalah 173.23.45.89

Secara normal komputer target akanmengidentifikasi *IP Address* dari komputer yang mengirimkan data adalah 202.45.98.1, namun dalam trik *IP Spoofing*komputer target akan mengira bahwa data yang dikirim adalah dari komputer dengan *IP Address* 173.23.45.89.

Ada beberapa cara untuk mencegah serangan IP Spoofing ini, salah satunya adalah dengan menggunakan autentikasi berdasarkan pada *key exchange* pada komputer di dalam jaringan. Sebagai contoh Ipsec akan secara signifikan mengurangi resiko dari *spoofing.*

d. Password-Based Attacks

Sebuahserangan di manaupaya dilakukan secaraberulang-ulangyang bertujuanuntuk dapat mendapatkan dan menduplikasilogon atauusername dan password yang valid (Glosasary). Setelah penyerang (*attacker*) berhasil mendapatkan akses ke dalam sebuah jaringan dengan menggunakan *account* yang valid, *attacker* dapat melakukan hal-hal berikut :

a. Mendapatkandaftarpenggunayang valid dannamakomputer sertajaringan informasi.

b. Memodifikasi konfigurasi server dan jaringan, yang termasuk kontrol akses dan table routing.

c. Memodifikasi, merouting ulang atau menghapus routing tabel

e. Man-ing-the-Middle Attack (MITM)

*Man-in-The-Middle*Merupakan jenis serangan yang sangat berbahaya dan bisa terjadi di mana saja, baik di website, telepon seluler, maupun di peralatan komunikasi tradisional seperti surat menyurat. Dalam serangan *Man-in-The-*

Middle(MITM), seorang attacker akan berada di tengah-tengah komunikasi antara dua pihak. Seluruh pembicaraan yang terjadi di antara mereka terlebih dahulu melalui *attacker* dahulu di tengah.*Attacker* dengan leluasa melakukan penyadapan, pencegatan, pengubahan bahkan memalsukan komunikasi (Wicaksono, 2009).

f. Sniffer Attack

Sniffer adalah sebuah aplikasi atau *device*yang dapat membaca, memonitor dan menangkap paket data dalam jaringan.Jika sebuah paket tidak di enkripsi, sebuah *sniffer* dapat menampilkan seluruh informasi data yang ada di dalam sebuah paket. Bahkan enkapsulasi data pun belum sepenuhnya aman dari ancaman *tools* sejenis *sniffer*.

Dengan menggunakan sniffer, seorang attacker dapat melakukan hal-hal seperti menganalisa atau melakukan penetrasi ke dalam sebuah jaringan guna mendapatkan informasi dan membaca komunikasi dalam jaringan.

g. Application-Layer Attack

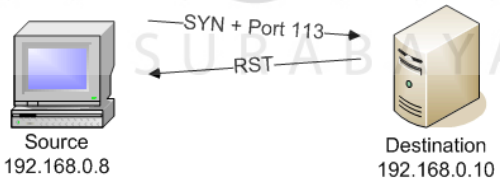
Application-Layer Attack adalah pada umumnya mejadikan layer aplikasi layer server sebagai target dan dapat mnyebabkan kegagalan dalam sistem operasi server dan aplikasi server. Dengan begitu *attacker*mendapatkan keuntungan untuk dapat mengontrol aplikasi, sistem atau jaringan dan dapat melakukan beberapa hal di antaranya :

a. Membaca, menambahkan atau memodifikasi data atau systemoperasi.
b. Memasukkan program virus dan aplikasi software untuk menduplikasi virus ke seluruh jaringan.

c. Memasukkan sebuah program sniffer untuk menganalisa jaringan dan mendapatkan informasi yang dapat di menyebabkan terjadinya *crash* dan mengakibatkan sebuah sistem dan jaringan menjadi *corrupt* dan menonaktifkan sistem keamanan yang ada.

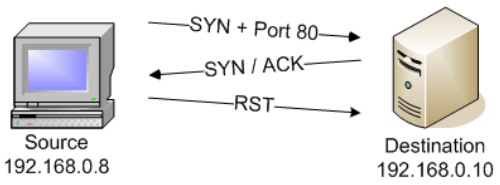
h. TCP Syn Scan

TCP SYN scan digunakan untuk mendeteksi port apa saja yang terbuka. Teknik ini sering disebut *Half Open Scan* karena dalam melakukan evaluasi terhadap port tidak membuka hubungan komunikasi TCP/IP secara penuh. Artinya secara teknis komputer yang digunakan untuk mendeteksi port tersebut akan mengirimkan paket SYN ke host target.Apabila host yang di-scan memberikan respon dengan mengirim balik paket SYN dan ACK, maka dipastikan bahwa port tersebut aktif/Open. Sebaliknya apabila dari server target mengirimkan respon dengan RST, maka dipastikan bahwa port tersebut adalah Closed. TCP SYN scan hanya memberikan informasi mengenai status sebuah port, *open, closed*atau *filtered port*.



Gambar 2.2.Sumber, NETWORK

UPTIME:(http://www.networkuptime.com/nmap/page3-2.shtml, 2013)



Gambar 2.3. Sumber, NETWORK

UPTIME:(http://www.networkuptime.com/nmap/page3-2.shtml, 21013)

i. Port Scan

Port bisa diibaratkan sebagai suatu pintu, lebih tepatnya disebut pintu virtual, yang terdapat pada komputer agar suatu komputer dapat terhubung dengan dunia luar. Port yang tersedia dalam komputer secara keseluruhan ada 65536.Suatu organisasi yang terletak di Amerika, IANA, bertanggung jawab untuk mengatur pendaftaran nomor-nomor port. Umumnya unruk mencari suatu pintu (port) yang terbuka digunakan tools yang disebut dengan Port Scanner. Dengan port scanner, kita bisa memanfaatkan suatu komputer yang kebetulan portnya terbuka untuk dieksploitasi lebih lanjut.

Ada beberapa teknik port *scanning* yang umum digunakanan di dalam nmap, seperti *open scanning, half-open scanning*(TCP SYN) dan *stealth scanning*(TCP FIN). Selain Nmap masih banyak tool yang mendukung untuk port scan yang lebih mudah dalam penggunaannya seperti *ScanPort, Super Scan, trojan port scanner* dan sebagainya.

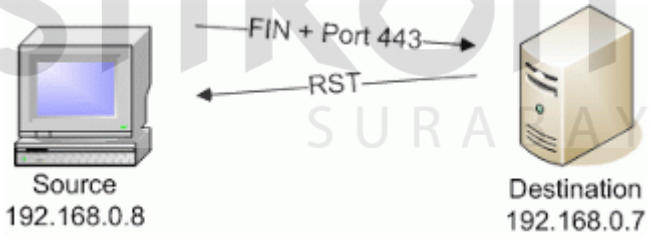
j. ACK Scan

Scan tipe ini agak sedikit berbeda karena tidak digunakan untuk menentukan apakah PORT tersebut terbuka tau tertutup. Scan ini hanya menunjukkan apakah state korban terfiltered atau unfiltered. Jika terfiltered, maka PORT mana yang terfiltered.Dengan kata lain, TCP ACK scan dipergunakan untuk memetakan set aturan firewall. Tehnik ini akan membantu menentukan apakah *firewall* itu merupakan suatu simple packet filter yang membolehkan hanya koneksi-koneksi tertentu (koneksi dengan bit set ACK) atau suatu *firewall* yang menjalankan *advance packet filtering*.

Jenis *scanning* ini mengirimkan paket dengan ACK flag. Jika paket yang dikembalikan ternyata TTL (Time To Live) lebih kecil dibandingkan dengan paket dengan RST bit yang diterima, atau ukuran *window*nya lebih besar dari pada 0, maka bisa dipastikan port tersebut sedang dalam kondisi *Listening* atau *Open*. ACK *Scanning* model ini juga termasuk kategori stealth scan dan sering digunakan untuk mem-*bypass firewall* sehingga *scanning* bisa menjangkau sampai ke host di jaringan internal sesudah *firewall.*

k. FIN Scan

Cara kerja dari FIN Scan adalah mengirimkan paket denga FIN bitke port target. Apabila port tersebur ternyata tidak aktif atau *Closed Port*, maka target sistem akan membalas dengan mengirimkan pesan RST yang memberitahukan bahwa port tersebut berstatus *Closed.* Dan apabila dikirimkan ke port yang *open*, maka tidak ada respon, port tersebut akan mengabaikan paket dengan FIN bit tersebut atau dengan kata lain di *drop*.



Gambar 2.4.Sumber, NETWORK UPTIME:

(http://www.networkuptime.com/nmap/page3-4.shtml, 2013)

2.3 Statistik dan Probabilitas

Statistika adalah ilmu yang mempelajari bagaimana merencanakan, mengumpulkan, menganalisis, menginterpretasi, dan mempresentasikan data (Gunawan, 2012).

Penggunaan metode statistik bayak digunakan di dalam pembuatan, pengembangan produk makanan. Perangkat lunak komputer, farmasi dan berbagai bidang lain melibatkan pengumpulan informasi atau data ilmiah. Tentu saja pengumpulan data tersebut bukanlah hal yang baru, hal ini telah dikerjakan dengan selama lebih dari seribu tahun. Data dikumpulkan, dirangkum, dilaporkan dan disimpan untuk diteliti (Ronald E. Walpoe, 2000)

2.3.1 Distribusi Frekuensi

Untuk data yang banyak sekali jumlahnya, akan lebih baik bila data diorganisasikan ke dalam bentuk yang lebih ringkas, kompak dan tanpa menghilangkan fakta pentingnya. Hal ini akan tercapai dengan mengelompokkan data ke dalam sejumlah kelas kemudian menentukan banyaknya data yang termasuk dalam masing-masing kelas atau frekuensi kelas. Susunan data yang terbentuk di sebut distribusi frekuensi.

Adapun tahap-tahap menyusun distribusi frekuensi adalah sebagai berikut:

a. Menentukan interval kelas

Untuk menentukan banyaknya kelas dapat digunakan “Kriterium Sturges”

$$k = 1 + 3{,}322 \log n$$

dimana :

k : Jumlah kelas

n : Banyaknya nilai observasi(data)

b. Menentukan batas kelas bawah

Menentukan batas bawah dari tiap-tiap kelas berdasarkan table distribusi frekuensi dari sampel.

c. Menentukan batas kelas atas

Menentukan batas atas dari tiap-tiap kelas berdasarkan table distribusifrekuensi dari sampel.

d. Menentukan batas nyata kelas

e. Menentukan panjang kelas untuk menentukan pajang kelas dapat digunakan rumus:

Panjang kelas (c) = Tepi Atas – Tepi Bawah

f. Menetukan nilai tengah, nilai tengah kelas diperoleh dengan membagi-dua jumlah dari batas kelas bawah dan batas kelas atas suatu interval kelas. Untuk mencari nilai tengah dapat menggunakan rumus:

Nilai tengah (Xi) = (Batas kelas bawah – Batas kelas atas) / 2

2.3.2 Distribusi Probabilitas

Kunci aplikasi probabilitas dalam statistik adalah memperkirakan terjadinya peluang/probabilitas yang dihubungkan dengan terjadinya peristiwa tersebut dalam beberapa keadaan.Jika kita mengetahui keseluruhan probabilitas dari kemungkinan outcome yang terjadi, seluruh probabilitas kejadian tersebut akan membentuk suatu distribusi probabilitas. Adapun macam distribusi probabilitas diantaranya adalah :

1. Distribusi Normal (Gaussian)

Distribusi Normal (Gaussian) merupakan distribusi probabilitas yang paling penting baik dalam teori maupun aplikasi statistk. Terminologi “normal” itu sendiri bukan tidak pada tempatnya, karena memang distribusi ini adalah yang paling banyak digunakan sebagai model bagi data riil diberbagai bidang. Bahkan

meskipun variabel yang ditangani dalam distribusi adalah variabel diskrit, kurva distribusi normal sering juga digunakan sebagai pendekatan.

Sekurang-kurangnya terdapat empat alasan mengapa distribusi normal menjadi distribusi yang paling penting.

a. Distribusi normal terjadi secara alamiah. Seperti diuraikan sebelumnya banyak peristiwa di dunia nyata yang terdistribusi secara normal
b. Beberapa variabel acak yang tidak terdistribusi normal dapat dengan mudah ditransformasi menjadi suatu suatu distribusi variabel acak yang normal.
c. Banyak hasil dan teknik analisis yang berguna dalamm pekerjaan statistik hanya bisa berfungsi dengan benar jika model distribusinya merupakan distribusi normal.
d. Ada beberapa variabel acak yang tidak menunjukkan distribusi normal pada populasinya, namun terdistribusi dari rata-rata sampel yang diambil secara random dari populasi tersebut ternyata menunjukkan distribusi normal.

Sebuah variabel acak kontinu X dikatakan memiliki distribusi normal dengan parameter $\mu_x$dan $\sigma_x$dimana $-\infty < \mu_x < -\infty$ dan $\sigma_x > 0$ jika fungsi kepadatan probabilitas *(pdf)* dari X adalah

$$= \frac{1}{\sigma x\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

Dimana μ_x adalah mean dan σ_x adalah deviasi standar. Untuk setiap nilai μ dan σ , kurva fungsi akan simetris terhadap μ dan memiliki total luas dibawah kurva tepat 1. Nilai dari σ menetukan bentangan dari kurva sedangkan μ

menetukan pusat simetrisnya. Karena kurva distribusi normal menyerupai lonceng maka kurva distribusi normal sering juga disebut sebagai distribusi bentuk lonceng *(bell shaped distribution)*.

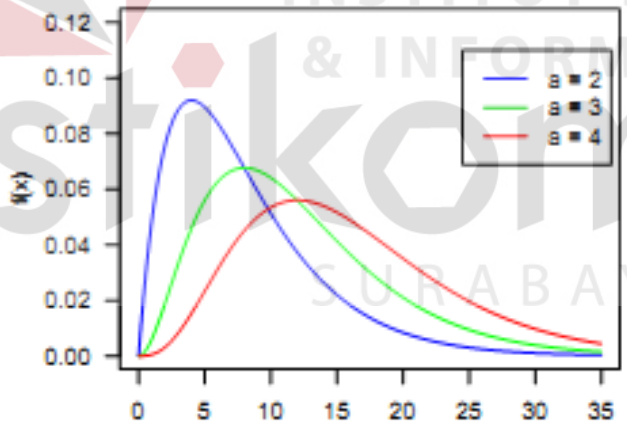
2. Distribusi Gamma

Distribusi Gamma adalah distribusi fungsi padat yang terkenal luas dalam bidang matematika, dengan fungsi probabilitas:

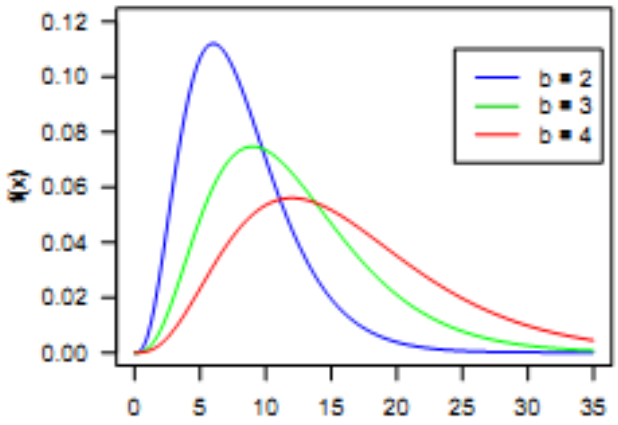
$$f(x) = \begin{cases} \frac{1}{\beta^{\alpha}\Gamma(\alpha)} x^{\alpha-1} e^{-\frac{x}{\beta}} & ; \quad x > 0 \\ 0 & ; x \text{ yanglain} \end{cases}$$

Untuk : $\alpha > 0, \beta > 0$

Dibawah ini adalah contoh beberapa kurva dari distribusi gamma dengan parameter α dan β :



Gambar2.5. Bentuk kurva distribusi gamma (Nunung, 2012)



Gambar2.6. Bentuk kurva distribusi gamma(Nunung, 2012)

3. Distribusi Log Normal

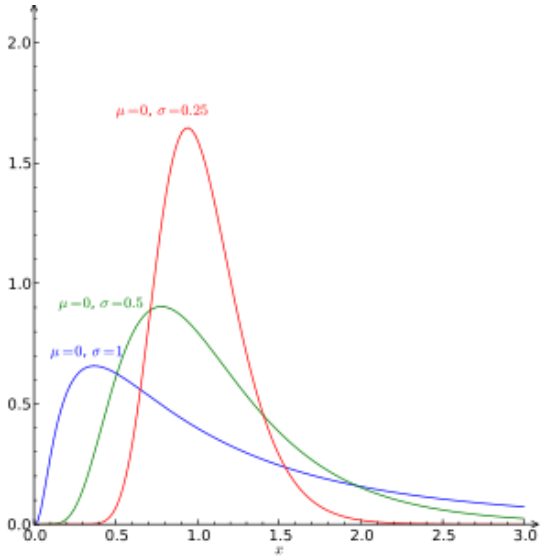
Distribusi log normal merupakan distribusi teoritis yang banyak digunakan digunakan di bidang teknik, khususnya sebaga model untuk berbegai jenis sifat material.

Sebuah variabel acak kontinu non-negatif X dikatakan memiliki distribusi log-normal jika ln(x) memiliki sebuah distribusi normal. Fungsi kepadatan probabilitas dari sebuah variabel acak yang memenuhi distribusi lognormal jika ln(x) terdistribusi normal dengan parameter μ dan σ.

$$= \frac{1}{2\sigma\sqrt{2\pi}} e^{-(\ln(x)-\mu)^2}$$

Sedangkan fungsi distribusi kumulatif lognormalnya adalah

$$P(X \leq x) = \int_0^x \frac{1}{\sqrt{2\pi}\sigma t} e^{-(\ln(t)-\mu)\ /(2\sigma^2)} dt$$



Gamabar 2.7. Grafik Distribusi *lognormal*, (Nunung, 2012)

Perlu diingat bahwa μ dan σ adalah mean dan deviasi standar dari ln(x) dan bukan dari X, karena ln(x) mempunyai sebuah distribusi normal maka fungsi distribusi kumulatif X dapat dinyatakan dengan menggunakan fungsi distribusi kumulatif normal standar F(□).

4. Distribusi Weibull

Penggunaann distribusi weibull pada tugas akhir ini didasarkan pada pola kurva yang memiliki kemiripan dengan distribusi gamma dan log normal serta histogram data. Hal ini menjadi acuan penulis untuk menggunakan distribusi weibull dalam proses fitting distribusi untuk mengetahui tingkat kemiripan suatu distribusi terhadapa histogram data sampel yang du uji.

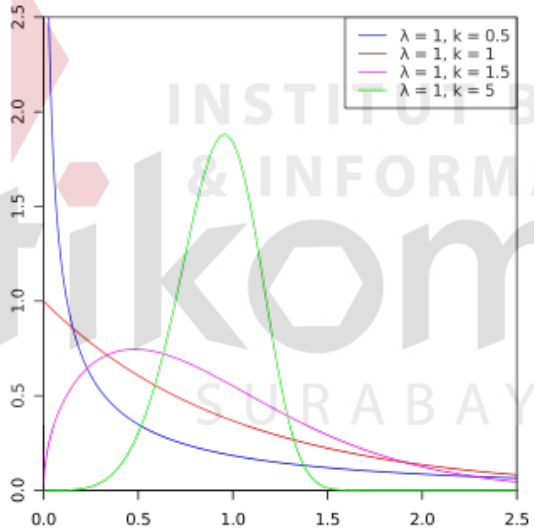
Fungsi kepadatan probabilitas dan fungsi distribusi kumulatif dari weibull dirumuskan, jika sebuah variabel acak kontinu X memiliki distribusi weibull dengan parameter bentuk α dan faktor skala β, di mana α> 0 dan β> 0, maka fungsi kepadatan probabilitas dari X adalah.

$$f_w(x;\alpha;\beta) = \frac{\alpha}{\beta} x^{\alpha-1} e^{-(x/\beta)^2} \qquad x \geq 0$$

Fungsi di atas mudah untuk diintegralkan, sehingga diperoleh fungsi distribusi kumulatif weibull berikut

$$F_w(x;\alpha;\beta) = P(X \leq x) = \int_0^x \frac{\alpha}{\beta^\alpha} t^{\alpha-1} e^{-(t/\beta)^2} dt = 1 - e^{-(x/\beta)\alpha}$$

Berikut contoh grafik distribusi weibull dengan beberapa parameter yang berbeda.



Gambar 2.8. Grafik Distribusi weibull, (Nunung, 2012)

2.4 Metode Anderson Darling

Metode Anderson Darling digunakan untuk menguji apakah sampel data berasal dari populasi dengan distribusi tertentu.Anderson Darling merupakan modifikasi dari uji Kolmogorov-Smirnov (KS). Nilai-nilai kritis dalam uji

KStidak tergantung pada distribusi tertentu yang sedang diuji, sedangkan uji Anderson Darling memanfaatkan distribusi tertentu dalam menghitung nilai kritis yang memiliki keuntungan yang menungkinkan tes yang lebih sensitif. Misalkan X1, X2, X3.....Xn adalah data yang akan diuji distribusi normalnya dengan tingkat signifikan α maka uji Anderson Darling dapat diperoleh dengan menggunakan rumus sebagai berikut

$$A = -n - s \tag{1}$$

Dengan

$$s = \frac{1}{n}\sum_{i=1}^{n}[2\mathrm{i} - 1][\ln(\mathrm{F(Zi)}) + \ln(1 - \mathrm{F(Zn + 1 - i)})] \tag{2}$$

$$Z = \frac{x_{i-\bar{X}}}{s} \tag{3}$$

Akibatnya persamaan (1) menjadi

$$A = -n - \frac{1}{n}\sum_{i=1}^{n}[2\mathrm{i} - 1][\ln(\mathrm{F(Zi)}) + \ln(1 - \mathrm{F(Zn + 1 - i)})] \tag{4}$$

Dengan

A = Statistik uji untuk metode Anderson Darling

n = Ukuran sampel

Xi = Data ke-i yang telah diurutkan

Zi = Data Xi yang distandarisasi

$\bar{X}$ = Rata-rata data

S = Standar deviasi data

F(Zi) = Nilai fungsi distribusi kumulatif normal baku di Zi