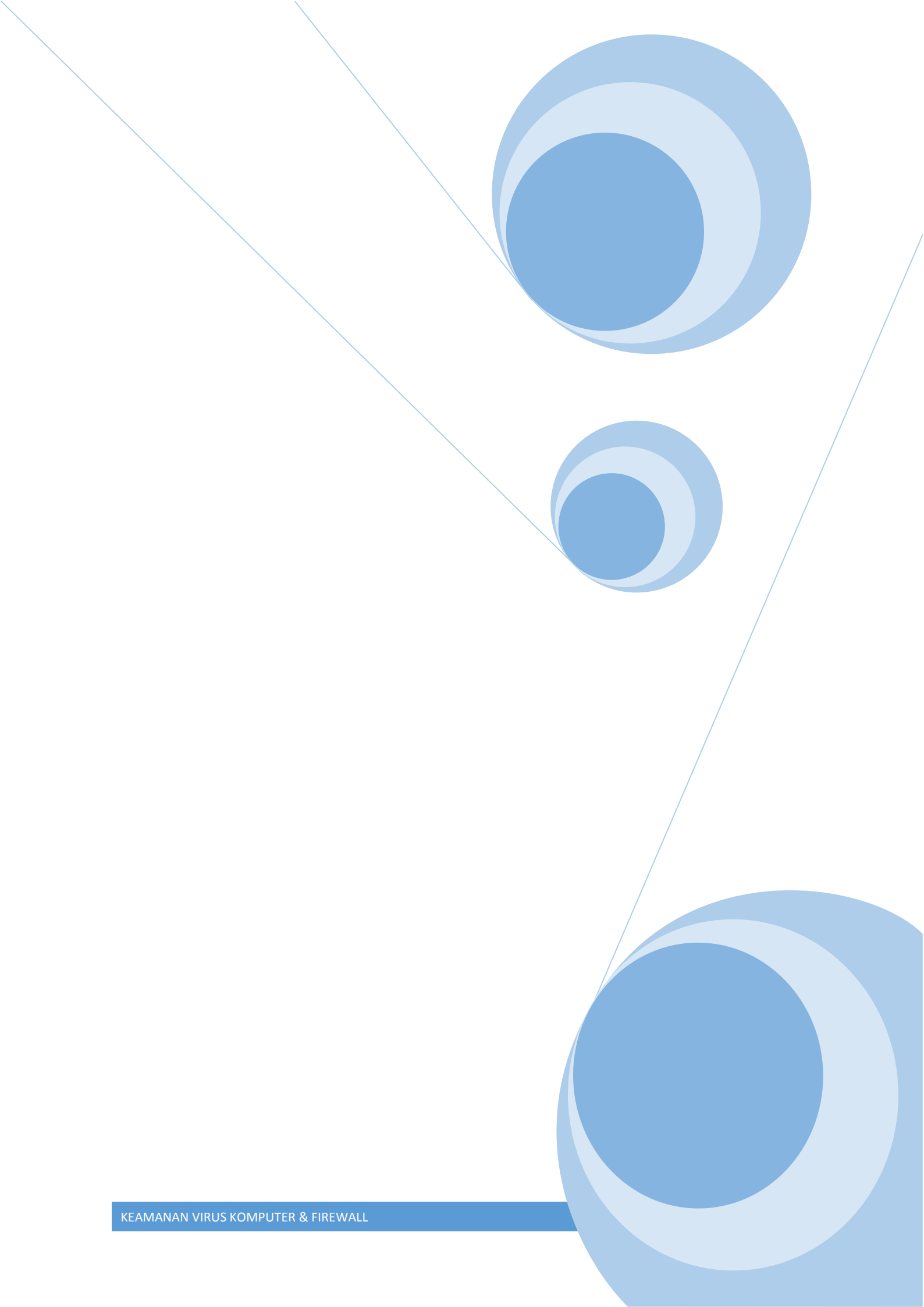

Keamanan Virus Komputer & Firewall

Target pembelajaran:

- Defenisi Virus dan Firewall
- Siklus hidup Virus
- Cara Kerja Virus dan penanggulanganya
- Arsitektur & Firewall

ASAL MUASAL VIRUS

1949, John Von Neuman, menggungkapkan " teori self altering automata " yang merupakan hasil riset dari para ahli matematika.

1960, lab BELL (AT&T), para ahli di lab BELL (AT&T) mencoba-coba teori yang diungkapkan oleh john v neuman, mereka bermain-main dengan teori tersebut untuk suatu jenis permainan/game. Para ahli tersebut membuat program yang dapat memperbanyak dirinya dan dapat menghancurkan program buatan lawan.Program yang mampu bertahan dan menghancurkan semua program lain, maka akan dianggap sebagai pemenangnya. Permainan ini akhirnya menjadi permainan favorit ditiap-tiap lab komputer.semakin lama mereka pun sadar dan mulai mewaspadai permainan ini dikarenakan program yang diciptakan makin lama makin berbahaya, sehingga mereka melakukan pengawasan dan pengamanan yang ketat.

1980, program tersebut yang akhirnya dikenal dengan nama "virus" ini berhasil menyebar diluar lingkungan laboratorium, dan mulai beredar di

dunia cyber.

1980, mulailah dikenal virus-virus yang menyebar di dunia cyber.

Virus Komputer adalah program / aplikasi yang dapat menggandakan dirinya sendiri dan menyebar dengan cara menyisipkan dirinya pada program dan data lainnya . biasanya user tidak mengetahui jika komputer yang di milikinya terjangkit virus sampai salah satu data hilang atau program yang ada pada komputer tidak bisa di jalankan.
Virus komputer umumnya di buat untuk tujuan yang tidak baik , banyak Efek negatif yang di timbulkan oleh virus komputer seperti memperbanyak dirinya sendiri sehingga memori menjadi kecil, hal ini membuat komputer sering hang atau freeze, lalu mengubah ekstensi pada file dan program yang membuat program/file tersebut tidak bisa di gunakan, dan dapat juga mencuri data pribadi seseorang tanpa sepengetahuan orang tersebut. selain itu juga virus dapat merusak hardware pada komputer.

Faktanya hampir 95% virus menyerang pengguna sistem operasi windows. Sisanya menyerang Linux/GNU, Mac, FreeBSD, OS/2 IBM, dan Sun Operating System.

KRITERIA VIRUS

Suatu program yang disebut virus baru dapat dikatakan adalah benar benar
virus apabila minimal memiliki 5 kriteria :

1. Kemampuan suatu virus untuk mendapatkan informasi
2. Kemampuannya untuk memeriksa suatu program
3. Kemampuannya untuk menggandakan diri dan menularkan
4. Kemampuannya melakukan manipulasi
5. Kemampuannya untuk menyembunyikan diri.

Sekarang akan coba dijelaskan dengan singkat apa yang dimaksud dari tiap
-tiap kemampuan itu dan mengapa ini sangat diperlukan.

1.Kemampuan untuk mendapatkan informasi

Pada umumnya suatu virus memerlukan daftar nama-nama file yang ada dalam
suatu directory, untuk apa? agar dia dapat mengenali program program apa

saja yang akan dia tulari,semisal virus makro yang akan menginfeksi semua
file berekstensi *.doc setelah virus itu menemukannya, disinilah kemampuan
mengumpulkan informasi itu diperlukan agar virus dapat membuat daftar/
data semua file, terus memilahnya dengan mencari file-file yang bisa
ditulari.Biasanya data ini tercipta saat program yang tertular/terinfeksi
atau bahkan program virus ini dieksekusi. Sang virus akan segera melakukan
pengumpulan data dan menaruhnya di RAM (biasanya :P) , sehingga apabila
komputer dimatikan semua data hilang tetapi akan tercipta setiap program
bervirus dijalankan dan biasanya dibuat sebagai hidden file oleh virus .

2.Kemampuan memeriksa suat program

Suatu virus juga harus bias untuk memeriksa suatu program yang akan
ditulari, misalnya ia bertugas menulari program berekstensi *.doc, dia
harus memeriksa apakah file dokumen ini telah terinfeksi ataupun belum,
karena jika sudah maka dia akan percuma menularinya 2 kali. Ini sangat
berguna untuk meningkatkan kemampuan suatu virus dalam hal kecepatan
menginfeksi suatu file/program.Yang umum dilakukan oleh virus adalah
memiliki/ memberi tanda pada file/program yang telah terinfeksi
sehingga mudah untuk dikenali oleh virus tersebut . Contoh penandaan
adalah misalnya memberikan suatu byte yang unik disetiap file yang
telah terinfeksi.

3.Kemampuan untuk menggandakan diri

Kalo ini emang virus "bang-get", maksudnya tanpa ini tak adalah virus.
Inti dari virus adalah kemampuan mengandakan diri dengan cara menulari
program lainnya. Suatu virus apabila telah menemukan calon korbannya
(baik file atau program) maka ia akan mengenalinya dengan memeriksanya,

jika belum terinfeksi maka sang virus akan memulai aksinya untuk menulari
dengan cara menuliskan byte pengenal pada program/ file tersebut,dan
seterusnya mengcopikan/menulis kode objek virus diatas file/program
yang diinfeksi. Beberapa cara umum yang dilakukan oleh virus untuk
menulari/ menggandakan dirinya adalah:

a.File/Program yang akan ditulari dihapus atau diubah namanya. kemudian
diciptakan suatu file menggunakan nama itu dengan menggunakan virus
tersebut (maksudnya virus mengganti namanya dengan nama file yang dihapus)
b.Program virus yang sudah di eksekusi/load ke memori akan langsung
menulari file-file lain dengan cara menumpangi seluruh file/program
yang ada.

4.Kemampuan mengadakan manipulasi

Rutin (routine) yang dimiliki suatu virus akan dijalankan setelah virus
menulari suatu file/program. isi dari suatu rutin ini dapat beragam
mulai dari yang teringan sampai pengrusakan. rutin ini umumnya digunakan
untuk memanipulasi program ataupun mempopulerkan pembuatnya! Rutin ini
memanfaatkan kemampuan dari suatu sistem operasi (Operating System) ,
sehingga memiliki kemampuan yang sama dengan yang dimiliki sistem
operasi. misal:

a.Membuat gambar atau pesan pada monitor
b.Mengganti/mengubah ubah label dari tiap file,direktori,atau label dari
drive di pc
c.Memanipulasi program/file yang ditulari
d.Merusak program/file
e.Mengacaukan kerja printer , dsb

5.Kemampuan Menyembunyikan diri

Kemampuan Menyembunyikan diri ini harus dimiliki oleh suatu virus agar semua

pekerjaan baik dari awal sampai berhasilnya penularan dapat terlaksana.
langkah langkah yang biasa dilakukan adalah:

-Program asli/virus disimpan dalam bentuk kode mesin dan digabung dengan
 program lain yang dianggap berguna oleh pemakai.
-Program virus diletakkan pada Boot Record atau track yang jarang
 diperhatikan oleh komputer itu sendiri
-Program virus dibuat sependek mungkin, dan hasil file yang diinfeksi tidak
 berubah ukurannya
-Virus tidak mengubah keterangan waktu suatu file
-dll

SIKLUS HIDUP VIRUS

Siklus hidup virus secara umum, melalui 4 tahap:

o Dormant phase (Fase Istirahat/Tidur)
Pada fase ini virus tidaklah aktif. Virus akan diaktifkan oleh suatu kondisi
tertentu, semisal:tanggal yang ditentukan,kehadiran program lain/dieksekusinya
program lain, dsb. Tidak semua virus melalui fase ini

o Propagation phase (Fase Penyebaran)
Pada fase ini virus akan mengkopikan dirinya kepada suatu program atau
ke suatu tempat dari media storage (baik hardisk, ram dsb). Setiap
program yang terinfeksi akan menjadi hasil "klonning" virus tersebut
(tergantung cara virus tersebut menginfeksinya)

o Trigerring phase (Fase Aktif)
Di fase ini virus tersebut akan aktif dan hal ini juga di picu oleh beberapa
kondisi seperti pada Dormant phase

o Execution phase (Fase Eksekusi)
Pada Fase inilah virus yang telah aktif tadi akan melakukan fungsinya.
Seperti menghapus file, menampilkan pesan-pesan, dsb

JENIS – JENIS VIRUS

Untuk lebih mempertajam pengetahuan kita tentang virus, Aku akan coba

memberikan penjelasan tentang jenis-jenis virus yang sering berkeliaran
di dunia cyber.

1.Virus Makro
Jenis Virus ini pasti sudah sangat sering kita dengar.Virus ini ditulis
dengan bahasa pemrograman dari suatu aplikasi bukan dengan bahasa
pemrograman dari suatu Operating System. Virus ini dapat berjalan apabila
aplikasi pembentuknya dapat berjalan dengan baik, maksudnya jika pada
komputer mac dapat menjalankan aplikasi word maka virus ini bekerja pada
komputer bersistem operasi Mac.
contoh virus:

-variant W97M, misal W97M.Panther
 panjang 1234 bytes,
 akanmenginfeksi NORMAL.DOT dan menginfeksi dokumen apabila dibuka.
-WM.Twno.A;TW
 panjang 41984 bytes,
 akan menginfeksi Dokumen Ms.Word yang menggunakan bahasa makro, biasanya
 berekstensi *.DOT dan *.DOC
-dll

2.Virus Boot Sector
Virus Boot sector ini sudah umum sekali menyebar.Virus ini dalam menggandakan
dirinya akan memindahkan atau menggantikan boot sector asli dengan program
booting virus. Sehingga saat terjadi booting maka virus akan di load kememori
dan selanjutnya virus akan mempunyai kemampuan mengendalikan hardware standar
(ex::monitor, printer dsb) dan dari memori ini pula virus akan menyebar
eseluruh drive yang ada dan terhubung kekomputer (ex: floopy, drive lain
selain drive c).
contoh virus :

-varian virus wyx
 ex: wyx.C(B) menginfeksi boot record dan floopy ;
 panjang :520 bytes;
 karakteristik :   memory resident dan terenkripsi)
-varian V-sign :
 menginfeksi : Master boot record ;

panjang 520 bytes;
karakteristik: menetap di memori (memory resident),terenkripsi, dan polymorphic)
-Stoned.june 4th/ bloody!:
menginfeksi : Master boot record dan floopy;
panjang 520 bytes;
karakteristik: menetap di memori (memory resident), terenkripsi dan menampilkan
pesan"Bloody!june 4th 1989" setelah komputer melakukan booting sebanyak 128 kali

3.Stealth Virus
Virus ini akan menguasai tabel tabel interupt pada DOS yang sering kita kenal
dengan "Interrupt interceptor" . virus ini berkemampuan untuk mengendalikan
instruksi instruksi level DOS dan biasanya mereka tersembunyi sesuai namanya
baik secara penuh ataupun ukurannya .
contoh virus:
-Yankee.XPEH.4928,
menginfeksi file *.COM dan *.EXE ;
panjang 4298 bytes;
karakteristik: menetap di memori, ukurantersembunyi, memiliki pemicu
-WXYC (yang termasuk kategori boot record pun karena masuk kategri stealth
dimasukkan pula disini), menginfeksi floopy an motherboot record;
panjang 520 bytes;
menetap di memori; ukuran dan virus tersembunyi.
-Vmem(s):
menginfeksi file file *.EXE, *.SYS, dan *.COM ;
panjang fie 3275 bytes;
karakteristik:menetap di memori, ukuran tersembunyi, di enkripsi.
-dll

4.Polymorphic Virus
Virus ini Dirancang buat mengecoh program antivirus,artinya virus ini selalu
berusaha agar tidak dikenali oleh antivirus dengan cara selalu merubah rubah
strukturnya setiap kali selesai menginfeksi file/program lain.

contoh virus:

-Necropolis A/B,
menginfeksi file *.EXE dan *.COM;
panjang file 1963 bytes;

karakteristik: menetap di memori, ukuran dan virus tesembunyi,terenkripsi dan
dapat berubah ubah struktur
-Nightfall,
menginfeksi file *.EXE;
panjang file 4554 bytes;
karakteristik : menetap di memori, ukuran dan virus tesembunyi,memiliki pemicu,
terenkripsidan dapat berubah-ubah struktur
-dll

5.Virus File/Program
Virus ini menginfeksi file file yang dapat dieksekusi langsung dari sistem operasi,
baik itu file application (*.EXE), maupun *.COm biasanya juga hasil infeksi
dari virus ini dapat diketahui dengan berubahnya ukuran file yang diserangnya.

6.Multi Partition Virus
Virus ini merupakan gabungan dariVirus Boot sector dan Virus file: artinya
pekerjaan yang dilakukan berakibat dua, yaitu dia dapat menginfeksi file-
file *.EXE dan juga menginfeksi Boot Sector.

Jenis-jenis virus pada komputer

1. **Worm** - Menduplikatkan dirinya sendiri pada harddisk. Ini membuat sumber daya komputer (Harddisk) menjadi penuh akan worm itu.
2. **Trojan** - Mengambil data pada komputer yang telah terinfeksi dan mengirimkannya pada pembuat trojan itu sendiri.
3. **Backdoor** - Hampir sama dengan trojan. Namun, Backdoor bisanya menyerupai file yang baik-baik saja. Misalnya game.
4. **Spyware -** Virus yang memantau komputer yang terinfeksi.
5. **Rogue** - merupakan program yang meniru program antivirus dan menampilkan aktivitas layaknya antivirus normal, dan memberikan peringatan-peringatan palsu tentang adanya virus. Tujuannya adalah agar pengguna membeli dan mengaktivasi program antivirus palsu itu dan mendatangkan uang bagi pembuat virus rogue tersebut. Juga rogue dapat membuka celah keamanan dalam komputer guna mendatangkan virus lain.

6. **Rootkit** - Virus yang bekerja menyerupai kerja sistem komputer yang biasa saja.
7. **Polymorphic virus** - Virus yang gemar beubah-ubah agar tidak dapat terdeteksi.
8. **Metamorphic virus** - Virus yang mengubah pengkodeannya sendiri agar lebih sulit dideteksi.
9. **Virus ponsel** - Virus yang berjalan di telepon seluler, dan dapat menimbulkan berbagai macam efek, mulai dari merusak telepon seluler, mencuri data-data di dalam telepon seluler, sampai membuat panggilan-panggilan diam-diam dan menghabiskan pulsa pengguna telepon seluler.

Banyak sekali virus yang sudah menyebar dan sangat sulit di hentikan penyebarannya namun kita dapat melakukan beberapa cara untuk menghindari terjangkitnya virus pada komputer ,
dapat menggunakan antivirus yang dapat mendeteksi keberadaan virus pada komputer.sehingga data dan program menjadi aman.

Contoh virus komputer yang sering menyerang para pengguna komputer :

- **Virus Shortcut.exe**
  virus yang merubah ekstensi program atau file menjadi shortcut. hal ini menyebabkan tidak dapat di aksesnya dokumen atau program yang ingin kita gunakan.
- **Virus: Trojan.Lodear**Trojan Horse menyerang apabila kita mendownload data dari internet.
- **Virus: W32.Beagle.CO@mm**
  Adalah virus yang mengirimkan email massal terhadap situs yang mempunyai tingkat keamanan rendah.
- **Virus: Backdoor.Zagaban**

Virus trojan yang satu ini menginjeksi komputer tertentu untuk digunakan sebagai tempat berlindung untuk merusak network atau jaringan terkait.

- **Virus: W32/Netsky-P**
  Virus ini mampu menyebarkan email massal dengan sendirinya kepada alamat email yang diproduksi oleh suatu file pada PC / local drive.
- **Virus: W32/Mytob-GH**
  Virus penyebar email massal dan merupakan Trojan untuk IRC pada komputer berbasis Windows.
- **Virus: W32/Mytob-EX**
  Virus yang menyebarkan email massal dan Trojan IRC yang mirip dengam W32-mytob-gh.
- **Virus: W32/Mytob-AS, Mytob-BE, Mytob-C, and Mytob-ER**
  Keluarga virus ini mempunyai karasteristik yang sama atas apa yang mereka lakukan.
- **Virus: Zafi-D**
  Meupakan virus pengirim email massal dan peer-to-peer yang membuat salinan sendiri kepada folder sistem windows dengan nama file nortonupdate. exe.
- **Virus: W32/Netsky-D**
  Virus ini juga mengirimkan serangan melalui IRC backdoor yang berfungsi juga menginfeksi komputer yang lemah.
- **Virus: W32/Zafi-B**
  Virus ini menyerang peer-to-peer (P2P) dan email virus akan dicopy dengan sendirinya pada sistem folder windows yang akan diberi nama otomastis secara acak.
- **Virus Bagle.BC**
  Virus Bagle BC ini termasuk salah satu jenis virus yang berbahaya dan telah masuk peringkat atas jenis virus yang paling cepat mempengaruhi komputer kita.

BEBERAPA CARA PENYEBARAN VIRUS

Virus layaknya virus biologi harus memiliki media untuk dapat menyebar,virus
computer dapat menyebar keberbagai komputer/mesin lainnya juga melalui berbagai
cara, diantaranya:

1.Disket, media storage R/W
Media penyimpanan eksternal dapat menjadi sasaran empuk bagi virus untuk
dijadikan media. Baik sebagai tempat menetap ataupun sebagai media penyebarannya.

Media yang bias melakukan operasi R/W (read dan Write) sangat memungkinkan untuk
ditumpangi virus dan dijadikan sebagai media penyebaran.

2.Jaringan (LAN, WAN,dsb)
Hubungan antara beberapa computer secara langsung sangat memungkinkan suatu
virus ikut berpindah saat terjadi pertukaran/pengeksekusian file/program
yang mengandung virus.

3.WWW (internet)
Sangat mungkin suatu situs sengaja di tanamkan suatu 'virus' yang akan
menginfeksi komputer-komputer yang mengaksesnya.

4.Software yang Freeware, Shareware atau bahkan Bajakan
Banyak sekali virus yang sengaja di tanamkan dalam suatu program yang di
sebarluaskan baik secara gratis, atau trial version yang tentunya sudah
tertanam virus didalamnya.

5.Attachment pada Email, transferring file
Hampir semua jenis penyebaran virus akhir-akhir ini menggunakan email attachment
dikarenakan semua pemakai jasa internet pastilah menggunakan email untuk
berkomunikasi, file-file ini sengaja dibuat mencolok/menarik perhatian, bahkan
seringkali memiliki ekstensi ganda pada penamaan filenya.

PENANGULANGANNYA

1.Langkah-Langkah untuk Pencegahan
Untuk pencegahan anda dapat melakukan beberapa langkah-langkah berikut :
o Gunakan Antivirus yang anda percayai dengan updatean terbaru, tdak
  perduli appun merknya asalkan selalu di update, dan nyalakan Auto protect
o Selalu men-scan semua media penyimpanan eksternal yang akan di gunakan,
  mungkin hal ini agak merepotkan tetapi jika Autoprotect anti virus anda
  bekerja maka prosedur ini dapat dilewatkan.
o Jika Anda terhubung langsung ke Internet cobalah untuk mengkombinasikan
  Antivirus anda dengan Firewall, Anti spamming, dsb

2.Langkah-Lagkah Apabila telah Terinfeksi

o Deteksi dan tentukan dimanakah kira-kira sumber virus tersebut apakah disket,
  jaringan, email dsb, jika anda terhubung ke jaringan maka ada baiknya anda
  mengisolasi computer anda dulu (baik dengan melepas kabel atau mendisable
  dari control panel)
o Identifikasi dan klasifikasikan jenis virus apa yang menyerang pc anda,
  dengan cara:
  - Gejala yang timbul, misal : pesan, file yang corrupt atau hilang dsb
  - Scan dengan antivirus anda, jika anda terkena saat Autoprotect berjalan
    berarti vius definition di computer anda tidak memiliki data virus ini,
    cobalah update secara manual atau mendownload virus definitionnya untuk
    anda install. Jika virus tersebut memblok usaha anda untuk mengupdatenya
    maka ,upayakan untuk menggunakan media lain (komputer) dengan antivirus
    updatean terbaru.
o Bersihkan, setelah anda berhasil mendeteksi dan mengenalinya maka usahakan
  segera untuk mencari removal atau cara-cara untuk memusnahkannya di situs
  -situs yang memberikan informasi perkembangan virus. Hal ini jika antivirus
  update-an terbaru anda tidak berhasil memusnahkannya.
o Langkah terburuk, jika semua hal diatas tidak berhasil adalah memformat
  ulang komputer anda .

FIREWALL

Firewall adalah sistem keamanan jaringan komputer yang digunakan untuk melindungi komputer dari beberapa jenis serangan dari komputer luar.

Yang dimaksudkan diatas adalah sistem atau perangkat yang memberi otorisasi pada lalu lintas jaringan komputer yang dianggapnya aman untuk melaluinya dan melakukan pencegahan terhadap jaringan yang dianggap tidak aman. Firewall dapat berupa perangkat keras dan perangkat lunak, perangkat yang menyaring lalu lintas jaringan antara jaringan.

Secara umum firewall digunakan untuk mengontrol akses terhadap siapapun yang memiliki akses terhadap jaringan privat dari pihak luar.

Fungsi Firewall

1. Mengontrol dan mengawasi paket data yang mengalir di jaringan Firewall harus dapat mengatur, memfilter dan mengontrol lalu lintas data yang diizin untuk mengakses jaringan privat yang dilindungi firewall. Firewall harus dapat melakukan pemeriksaan terhadap paket data yang akan melawati jaringan privat. Beberapa kriteria yang dilakukan firewall apakah memperbolehkan paket data lewati atau tidak, antara lain :
    a. Alamat IP dari komputer sumber.
    b. Port TCP/UDP sumber dari sumber.
    c. Alamat IP dari komputer tujuan.
    d. Port TCP/UDP tujuan data pada komputer tujuan
    e. Informasi dari header yang disimpan dalam paket data.
2. Melakukan autentifikasi terhadap akses.
3. Aplikasi proxy Firewall mampu memeriksa lebih dari sekedar header dari paket data, kemampuan ini menuntut firewall untuk mampu mendeteksi protokol aplikasi tertentu yang spesifikasi.
4. Mencatat setiap transaksi kejadian yang terjadi di firewall. Ini Memungkinkan membantu sebagai pendeteksian dini akan penjebolan jaringan.

Beberapa karakteristik dari firewall

- Firewall harus lebih kuat dan kebal terhadap serangan luar. Hal ini berarti bahwa Sistem Operasi akan relatif lebih aman dan penggunaan sistemnya dapat dipercaya.
- Hanya aktivitas atau kegiatan yang dikenal/terdaftar saja yang dapat melewati atau melakukan hubungan. Hal ini dilakukan dengan menyetting policy pada konfigurasi keamanan lokal.
- Semua aktivitas atau kegiatan dari dalam ke luar harus melewati firewall. Hal ini dilakukan dengan membatasi atau memblok semua akses terhadap jaringan lokal, kecuali jika melewati firewall terlebih dahulu.
  Firewall ini berjalan pada satu host atau lebih, dan firewall ini terdiri dari beberapa komponen software. Firewall sendiri mempunyai empat tipe, yaitu Screened Subnet Firewall, Screened Host Firewall, Dual-homed Gateway Firewall, dan Packet-filtering Firewall. Berikut penjelasannya :

a. Screened Subnet Firewall ini menyediakan keamanan yang sangat baik dan sangat tinggi daripada tipe firewall lainnya, karena membuat Demilitarized Zone (DMZ) diantara jaringan internal dan jaringan eksternal.
b. Screened Host Firewall ini terdiri dari sebuah bastion host (host yang berupa application level gateway) dan dua router packet filtering.
c. Dual-homed Gateway Firewall ini sedikitnya memiliki dua IP address dan dua interface jaringan dan apabila ada serangan dari luar dan tidak dikenal maka akan diblok.
d. Packet-filtering Firewall ini terdiri dari router diantara jaringan internal dan eksternal yang aman. Tipe ini untuk menolak dan mengijinkan trafik.

MANFAAT FIREWALL

Manfaat dari Firewall yaitu sebagai berkut:

- ✓ Mengatur lalu intas/trafik data antar jaringan
- ✓ Dapat mengatur *port* atau paket data yang diperbolehkan atau ditolak.
- ✓ Autentikasi terhadap akses
- ✓ Memonitoring atau mencatat lalu lintas jaringan

CARA KERJA FIREWALL

Firewall pada dasarnya merupakan penghalang antara komputer Anda (atau jaringan) dan Internet (luar dunia). Firewall bisa hanya dibandingkan dengan seorang penjaga keamanan yang berdiri di pintu masuk rumah Anda dan menyaring pengunjung yang datang ke tempat AndaDia mungkin mengizinkan beberapa pengunjung untuk masuk sementara menyangkal orang lain yang ia tersangka penyusup yang. Demikian pula firewall adalah sebuah program perangkat lunak atau perangkat keras yang menyaring informasi (paket) yang datang melalui internet ke komputer pribadi Anda atau jaringan

komputer.

Firewall dapat memutuskan untuk mengizinkan atau memblokir lalu lintas jaringan antara perangkat berdasarkan aturan yang pra-dikonfigurasi atau ditentukan oleh administrator firewall. Kebanyakan personal firewall seperti firewall Windows beroperasi pada seperangkat aturan pra-konfigurasi yang paling cocok dalam keadaan normal sehingga pengguna tidak perlu khawatir banyak tentang konfigurasi firewall.

firewall pribadi adalah mudah untuk menginstal dan menggunakan dan karenanya disukai oleh pengguna-akhir untuk digunakan pada komputer pribadi mereka. Namun jaringan besar dan perusahaan-perusahaan lebih memilih orang-orang firewall yang memiliki banyak pilihan untuk mengkonfigurasi sehingga untuk memenuhi kebutuhan khusus mereka. Sebagai contoh, perusahaan mungkin

membuat aturan firewall yang berbeda untuk server FTP, Telnet server dan server Web. Selain itu perusahaan bahkan dapat mengontrol bagaimana karyawan dapat terhubung ke Internet dengan memblokir akses ke situs web tertentu atau membatasi transfer file ke jaringan lain. Jadi selain keamanan, firewall dapat memberikan perusahaan kontrol luar biasa atas bagaimana orang menggunakan jaringan.

Firewall menggunakan satu atau lebih metode berikut untuk mengatur lalu lintas masuk dan keluar dalam sebuah jaringan:

1. 1.. Packet Filtering: Pada metode ini paket (potongan kecil data) dianalisa dan dibandingkan dengan**filter.** filter paket memiliki seperangkat aturan yang datang dengan tindakan menerima dan menolak yang pra-dikonfigurasi atau dapat dikonfigurasi secara manual oleh administrator firewall.. Jika paket berhasil membuatnya melalui filter ini maka itu diperbolehkan untuk mencapai tujuan, kalau tidak akan dibuang.

2. 2. Stateful Inspeksi: Ini adalah metode baru yang tidak menganalisa isi dari paket. Sebaliknya ia membandingkan aspek kunci tertentu setiap paket database sumber terpercaya.. Kedua paket yang masuk dan keluar dibandingkan terhadap database ini dan jika perbandingan menghasilkan pertandingan yang wajar, maka paket yang diizinkan untuk melakukan perjalanan lebih lanjut. Jika tidak, mereka akan dibuang.

KONFIGURASI FIREWALL

Firewall dapat dikonfigurasi dengan menambahkan satu atau lebih filter berdasarkan beberapa kondisi seperti tersebut di bawah ini:

1. 1. Alamat IP: Dalam kasus apapun jika sebuah alamat IP di luar jaringan dikatakan kurang baik, maka dimungkinkan untuk mengatur filter untuk memblokir semua lalu lintas ke dan dari alamat IP. Misalnya, jika alamat IP cetain ditemukan akan membuat terlalu banyak koneksi ke server, administrator dapat memutuskan untuk memblokir lalu lintas dari IP ini menggunakan firewall.

2. 2. Nama Domain: Karena sulit untuk mengingat alamat IP, itu adalah cara yang lebih mudah dan lebih cerdas untuk mengkonfigurasi firewall dengan menambahkan filter berdasarkan nama domain. Dengan mendirikan domain filter, perusahaan dapat memutuskan untuk memblokir semua akses ke nama domain tertentu, atau mungkin menyediakan akses hanya untuk daftar nama domain yang dipilih.

3. 3. Port / Protokol: Setiap layanan yang berjalan pada server dibuat tersedia ke Internet menggunakan nomor port, satu untuk setiap layananDengan kata sederhana, port bisa dibandingkan dengan pintu virtual dari server melalui layanan yang tersedia. Sebagai contoh, jika server adalah menjalankan Web (HTTP) layanan maka akan biasanya tersedia pada port 80. Untuk memanfaatkan layanan ini, klien ingin terhubung ke server

melalui port 80. Demikian pula berbagai layanan seperti Telnet (Port 23), FTP (port 21) dan SMTP (port 25) Layanan dapat berjalan pada server. Jika layanan ini ditujukan untuk publik, mereka biasanya tetap terbuka. Jika tidak, mereka yang diblok menggunakan firewall sehingga mencegah penyusup menggunakan port terbuka untuk membuat sambungan tidak sah.

4. 4. Firewall dapat dikonfigurasi untuk menyaring satu atau lebih kata atau frase spesifik sehingga, baik dan keluar paket yang datang dipindai untuk kata-kata dalam saringan. Misalnya, Anda mungkin mengatur aturan firewall untuk menyaring setiap paket yang berisi istilah ofensif atau frase yang mungkin Anda memutuskan untuk memblokir dari memasuki atau meninggalkan jaringan Anda.

HARDWARE VS SOFTWARE FIREWALL

Hardware firewall menyediakan tingkat keamanan yang lebih tinggi dan karenanya lebih disukai untuk server mana keamanan memiliki prioritas paling atas sedangkan, firewall perangkat lunak yang lebih murah dan paling disukai di komputer rumah dan laptop. Hardware firewall biasanya datang sebagai unit built-in router dan memberikan keamanan maksimum karena filter masing-masing paket di tingkat hardware itu sendiri bahkan sebelum itu berhasil memasuki komputer AndaSebuah contoh yang baik adalah Linksys Cable / DSL router.

Mengapa Firewall?

Firewall memberikan keamanan di sejumlah ancaman online seperti login Remote, backdoors Trojan, pembajakan Sesi, serangan DOS & DDOS, virus, cookie mencuri dan banyak lagi. Efektivitas keamanan tergantung pada cara Anda mengkonfigurasi firewall dan bagaimana Anda mengatur aturan filter. Namun ancaman utama seperti DOS dan serangan DDOS kadang-kadang dapat mengelola untuk melewati firewall dan melakukan kerusakan server. Meskipun firewall bukanlah jawaban yang lengkap terhadap ancaman online, dapat paling efektif menangani serangan dan memberikan keamanan untuk komputer sampai batas maksimal.

Arsitektur Dasar Firewall

1. **Arsitektur dengan dual-homed host (*dual homed gateway/DHG*)**

Menggunakan sebuah komputer dengan (minimal) dua NIC. Interface pertama dihubungkan ke jaringan internal dan yang lainnya dengan internet. *Dual homed host*-nya sendiri berfungsi sebagai *bastion host* (Suatu sistem komputer yang harus memiliki keamanan yang tinggi, karena biasanya peka terhadap serangan jaringan,

2. **Screened-host (screened host gateway/SHG)**

fungsi firewall dilakukan oleh sebuah screening-router dan bastian host. Router ini akan menolak semua trafik kecuali yang

ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan.

3. **Screened subnet (*screened subnet gateway* (SSG)**
   Firewall dengan arsitektur ini menggunakan dua Screened-router dan jaringan tengah (*perimeter network)* antara kedua router tersebut, dimana ditempatkan bastion host.

Daftar Pustaka

http://www.it-jurnal.com/2014/03/Pengertian.dan.Jenis-jenis.Virus.pada.Komputer.html

http://ezine.echo.or.id/ezine4/ez-r04-y3dips-viruskomputer.txt

[Stallings, William],"CRYPTOGRAPHY AND NETWORK SECURITY,principle and practice: second edition " ,Prentice-Hall,Inc., New Jersey ,1999

[Salim, IR.Hartojo],"Virus Komputer, teknik pembuatan & langkah-langkah penaggulangannya ,Andi OFFSET,Yogyakarta , 1989.

[Amperiyanto, Tri],"Bermain-main dengan Virus Macro",Elex Media Komputindo, Jakarta,2002

[Jayakumar], " Viruspaperw.pdf ", EBOOK version

[y3dips],"pernak pernik Virus",http://ezine.echo.or.id,Jakarta,2003

Virus Definition dari salah satu Antivirus "

http://www.jaringankomputer.org/firewall-pengertian-fungsi-manfaat-dan-cara-kerja-firewall/

http://fajarypnet.blogspot.com/2014/02/perngertian-fungsi-manfaat-dan-cara.html

staff site: fitria_okta