

JAWABAN SOAL MID SEMESTER **KEAMANAN SISTEM KOMPUTER**

Dosen:
Abdullah A. Koro, M.Kom



Disusun oleh:

Nama : Mawan Agus Nugroho.
NIM: 1011.600.184
Kelas: X.A

Program PascaSarjana Magister Ilmu Komputer
Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Jakarta Selatan 12260

Soal Mid Test 16 April 2011

Keamanan Sistem Komputer

Case Study:

Disuatu Non Government Organization (LSM) anda ditunjuk menjadi Kepala Perencanaan Teknologi Informasi dan Komunikasi. Total Staff ada 50 orang. Lingkungan sistem operasi yang digunakan ada beragam baik itu laptop dan desktop.

Sistem operasi desktop yang digunakan yaitu

1. Mac OS X 10.6
2. Ubuntu Linux 10.10
3. Windows 7, Windows XP dan Vista

Untuk Server, OS nya yaitu

1. FreeBSD + Samba (untuk Windows networking)

Pertanyaan:

1. Jelaskan langkah-langkah anda dalam mengamankan aset teknologi informasi baik dari segi sistem operasi, aplikasi organisasi, perilaku pengguna, jaringan lokal dan internet. Buat gambar jika perlu
2. Perlukah antivirus digunakan jika sistem operasi desktop dan laptop beragam? Bagaimana dengan server yang menggunakan FreeBSD yang merupakan varian UNIX apakah perlu dipasang antivirus? Perlukah anda menggunakan firewall dan sejenisnya? Bagaimana anda menangani bila bujet NGO terbatas?

Jawaban di kirim via email ke koro@bentala.co.id

Paling lambat hari Rabu, 20 April 2011, Pukul 21.00

Jawaban yang sudah diterima, akan di reply: OK (mohon cek email anda)

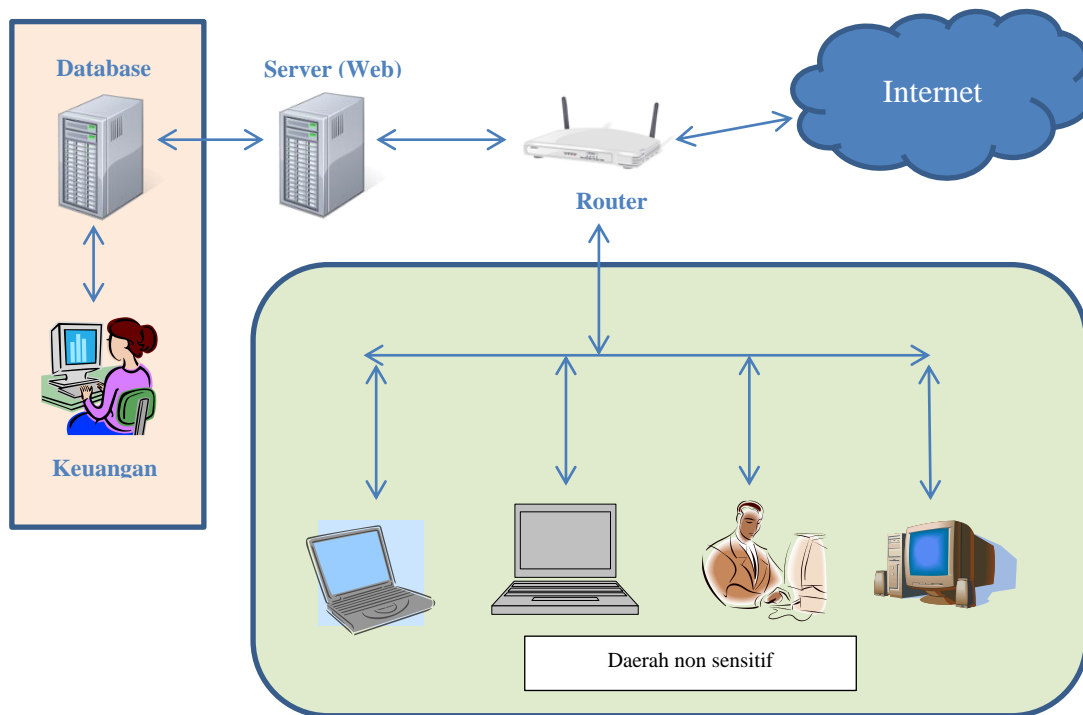
Tuliskan NIM dan Nama pada jawaban anda, juga di email.

Format file: PDF, RTF, DOC, ODT

(Jangan dalam bentuk DOCX)

Jawaban soal nomor 1.

Langkah yang pertama kali saya lakukan adalah merancang struktur jaringan komputer.



STRUKTUR JARINGAN KOMPUTER (INTERNET DAN INTRANET).

- Pada router dipasang basic firewall. Namun demikian, di tiap komputer juga dipasang firewall.
- Pada server dipasang web server dan ftp server. Sistem operasi yang digunakan adalah Free BSD dan Samba.
- Data yang sensitif (keuangan dsb) tidak dihubungkan secara langsung ke internet. Hal ini untuk mencegah agar hacker dari luar tidak mudah menyentuhnya. Bagian keuangan dengan demikian terisolasi dari luar.

Satu-satunya penghubung antara data sensitif dengan karyawan dari departemen lain adalah web server yang secara fisik berbeda komputer dengan komputer yang digunakan untuk menyimpan data. Pada komputer database diinstall MySQL.

- Komputer-komputer yang lain (yang berada di daerah non sensitif) terhubung dengan internet. Untuk mengakses data sensitif yang tersimpan di database, satu-satunya cara adalah melalui web browser.

- Untuk komunikasi antar pegawai, karena sistem operasi yang digunakan beragam, maka yang paling efektif adalah Yahoo Messenger.

APLIKASI YANG DIGUNAKAN.

- Database
 - Sistem operasi: Linux Debian.
 - Database: MySQL.
- Server web
 - Sistem operasi: Free BSD.
 - Web Server: Apache, PHP.
- Bagian keuangan
Microsoft Windows 7, web browser FireFox, Microsoft Office 2010, dan program aplikasi keuangan MYOB versi 18.
- Kepala Bagian / Eksekutif: Mac OS X.10.6.
- Karyawan lain cukup Ubuntu Linux 10.10.

PERILAKU PENGGUNA.

Perlu dibuat peraturan agar karyawan dilarang menggunakan internet pada jam kerja untuk melakukan kegiatan yang tidak ada hubungannya dengan pekerjaan kantor. Namun demikian, tidak perlu dipasang program spyware untuk mengawasi aktivitas bawahan karena hal ini dapat membuat karyawan tidak nyaman dan melanggar hak privacy mereka.

Jawaban soal nomor 2.

Virus tidak hanya ada di sistem operasi Windows. Menurut Wikipedia, setidaknya ada 30 virus yang berjalan di sistem operasi Linux.

Viruses

- 42^{[23][24]}
- Arches^[25]
- Alaeda - Virus.Linux.Alaeda^[26]
- Bad Bunny - Perl.Badbunny^{[6][27]}
- Binom - Linux/Binom^[28]
- Bliss - requires root privileges
- Brundla^[29]
- Bukowski^[30]
- Caveat^{[31][32]}
- Coin^{[33][34]}
- Diesel - Virus.Linux.Diesel.962^[35]
- Hasher^{[36][37]}
- Kagob a - Virus.Linux.Kagob.a^[38]
- Kagob b - Virus.Linux.Kagob.b^[39]
- Lacrimae (aka Crimea)^{[40][41]}
- MetaPHOR (also known as Simile)^[42]
- Nuxbee - Virus.Linux.Nuxbee.1403^[43]
- OSF.8759
- PiLoT^{[44][45]}
- Podloso - Linux.Podloso (The iPod virus)^{[46][47]}
- RELx^[48]
- Rike - Virus.Linux.Rike.1627^[49]
- RST - Virus.Linux.RST.a^[50] (known for infecting Korean release of Mozilla Suite 1.7.6 and Thunderbird 1.0.2 in September 2005^[51])
- Satyr - Virus.Linux.Satyr.a^[52]
- Staog - obsoleted by updates
- Vit - Virus.Linux.Vit.4096^[53]
- Winter - Virus.Linux.Winter.341^[54]
- Winux (also known as Lindose and PEEIt)^[55]
- Wit virus^[56]
- ZipWorm - Virus.Linux.ZipWorm^[57]

Worms

- Adm - Net-Worm.Linux.Adm^[58]
- Adore^[59]
- Cheese - Net-Worm.Linux.Cheese^[60]
- Devnull
- Kork^[61]
- Linux/Lion
- Linux/Lupper.worm^[62]
- Mighty - Net-Worm.Linux.Mighty^[63]
- Millen - Linux.Millen.Worm^[64]
- Ramen worm - targeted only Red Hat Linux distributions versions 6.2 and 7.0
- Slapper^[65]
- SSH Bruteforce^[66]

Sumber: http://en.wikipedia.org/wiki/Linux_malware

Mengapa masyarakat umum hanya mendengar virus di Windows? Jawabannya adalah: 90% pengguna komputer di dunia menginstall sistem operasi keluarga Windows (Windows XP, Vista, 7, dsb).

OS Platform Statistics

Windows XP is the most popular operating system. The Windows family counts for almost 90%:

2011	Win7	Vista	Win2003	WinXP	W2000	Linux	Mac
March	34.1%	7.9%	0.9%	42.9%	0.2%	5.1%	8.0%
February	32.2%	8.3%	1.0%	44.2%	0.2%	5.1%	8.1%
January	31.1%	8.6%	1.0%	45.3%	0.2%	5.0%	7.8%

Sumber: http://www.w3schools.com/browsers/browsers_os.asp

Programmer virus lebih tertarik membuat virus untuk lingkungan Windows karena efeknya dapat secara cepat dinikmati. Jika membuat virus untuk Linux, daya sebarannya kurang meluas dan tidak cepat populer. Lagi pula pengguna Linux umumnya lebih mengetahui tentang keamanan komputer dibandingkan pengguna Windows yang banyak terdiri dari orang awam.

Penyebaran virus bukan melulu salah sistem operasi, tapi juga kerap kali karena perilaku pengguna yang sembrono.

Dengan demikian, setiap komputer **wajib diinstall anti virus** dan firewall. Berikut ini anti virus yang berjalan di sistem operasi Linux:

1. Avast! (freeware dan commercial)
2. AVG (freeware dan commercial)
3. Avira (freeware dan commercial)
4. Bitdefender (freeware dan commercial)
5. ClamAV (free open source software)
6. Dr.Web (commercial)
7. Eset (commercial)
8. F-Secure Linux (commercial)
9. Kaspersky Linux Security (commercial)
10. Linux Malware Detect (free open source)
11. McAfee VirusScan Enterprise for Linux (commercial)
12. Panda Security for Linux (commercial)
13. rkhunter
14. Sophos (commercial)
15. Symantec AntiVirus for Linux (commercial)
16. Trend Micro ServerProtect for Linux (commercial)

Jika budget NGO terbatas, dapat digunakan anti virus gratis, misalnya Avast! Dan AVG.