Nama : Muhammad Ramdan
NIM : 1904637
Kelas : TE02 2019

UTS KEMANAN JARINGAN

1. Mengapa jaringan telekomunikasi harus diamankan? Apa yang menjadi kerentanan pada jaringan telekomunikasi?
2. Bagaimana caranya untuk mengatasi/ menindaklanjuti butir 1 tersebut?
3. Coba bandingkan 4 buah software/ algoritma keamanan data dalam hal kelebihan dan kekurangannya. Bebas memilih.
4. Apa yang anda ketahui esensi dan prinsip kerja dari:
    a. Firewall
    b. WEP
    c. Kriptografi
5. Suatu organisasi yang sarat penggunaan jaringan telekomunikasi, apa saja upaya-upaya pengamanan yang meyakinkan dan bijaknya?
6. Buatlah ikhtisar bagian tugas yang anda buat sebagai tugas mata kuliah yang telah dilalui?

JAWABAN

Soal 1

Jaringan telekomunikasi sangat rentan untuk disadap karena komunikasi data yang terjadi tidak terjadi secara langsung, melainkan adanya pihak ketiga sebagai server yang menjembatani komunikasi data. Hal ini memungkinkan data dapat diambil ataupun diubah dalam perjalanannya menuju penerima. Selayaknya paket yang diantarkan oleh kurir, paket tersebut bisa saja hilang di perjalanan ataupun dicuri. Oleh karena itu, pengamanan dalam telekomunikasi sangat penting.

Sering terjadi kebocoran data di banyak instansi pemerintahan ataupun non pemerintahan karena pengamanannya kurang kuat. Kebocoran data ini dapat berakibat fatal kepada keamanan warga negara bahkan negara sekalipun.

Soal 2

Untuk mengatasi masalah keamanan jaringan, diperlukan pengamanan ekstra untuk data yang penting. Dalam hal ini dibutuhkan orang orang yang handal untuk menangani keamanan jaringan. Dibutuhkan juga orang yang akan mencoba untuk menembus sistem pertahanan untuk mencoba seberapa kuat sistem pertahanan yang ada saat ini.

Selain itu, kebocoran data juga bisa disebabkan oleh algoritma yang kurang efektif. Sehingga dibutuhkan optimasi algoritma yang digunakan.

Soal 3

1. Smadav antivirus

Software ini kurang bagus untuk digunakan sebagai antivirus. Smadav dapat dengan mudah "digocek" oleh virus sehingga virus tersebut lolos dari pemindaian Smadav. Tak jarang pula, Smadav menganggap dirinya sendiri adalah virus.

2. Avira antivirus

Mirip dengan Smadav, software antivirus ini tidak begitu berguna untuk digunakan. Ada atau tidak adanya antivirus ini tidak terlalu berpengaruh terhadap keamanan data di sistem.

3. Avast antivirus

Daripada dua software di atas, Avast sedikit lebih berguna. Namun akan sama saja buruk jika Avast yang digunakan adalah hasil crack. Namun software ini agak memberatkan sistem karena optimasinya kurang baik.

4. Linux OS

Linux bukanlah software antivirus, melainkan sistem operasi. Mayoritas manusia menggunakan OS Windows sehingga memancing para pembuat virus untuk membuat virus demi kepentingan sendiri. Jumlah pengguna linux bahkan tidak samai 1% di dunia ini. Dengan ini, Linux bisa dikatakan bebas dari virus apa pun. Selain karena jumlah pengguna yang sedikit, Linux juga bersifat Open Source sehingga ada banyak orang di dunia ini yang akan memperbaiki OS ini untuk tetap aman.

Soal 4

a. Firewall

Firewall adalah sistem keamanan jaringan komputer yang mampu melindungi dari serangan virus, malware, spam, dan serangan jenis yang lainnya. Dapat dikatakan juga bahwa, firewall merupakan perangkat lunak untuk mencegah akses yang dianggap ilegal atau tidak sah dari jaringan pribadi (private network).

Sehingga, tugas utama dari adanya firewall sendiri adalah untuk melakukan monitoring dan mengontrol semua akses masuk atau keluar koneksi jaringan berdasarkan aturan keamanan yang telah ditetapkan.

Namun, masih terdapat beberapa orang atau user yang belum aware dengan adanya sistem ini dan cenderung mengabaikan dari sistem keamanan pada jaringan komputer. Selain itu, firewall juga mempunyai peranan penting dalam menjaga keamanan lalu lintas pada jaringan internet yang terhubung dengan perangkat komputer.

b. WEP

WEP (Wired Equivalent Privacy) atau Shared Key Authentication adalah security/metode keamanan untuk jaringan wireless yang agak lama. Jenis security ini mudah untuk dicrack atau di sadap orang luar. WEP menggunakan 64bit dan 128bit. Ada dua cara untuk memasukkan WEP key, sama seperti melakukan set sendiri atau generate menggunakan passphrase. Passphrase akan generate automatic WEP key untuk anda bila memasukkan abjad dan tekan generate. WEP hanyan menerima masukan 0-9 dan A-F(hexadecimal).

Kepanjangan key bergantung jenis securiy, jika 64bit, maka bisa masukkan 10key, dan untuk 128key bisa memasukkan 26key. Tak boleh kurang dan lebih. Intinya Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk autentikasi menuju access point.

c. Kriptografi

Kriptografi berasal dari kata bahasa Yunani, yang berarti kryptos dan graphein. Kryptos berarti rahasia atau tersembunyi, sedangkan graphein artinya menulis. Jadi, secara umum kriptografi merupakan proses menulis atau menyampaikan pesan secara rahasia dan tersembunyi.

Namun, jika kita kaitkan dengan penggunaan teknologi digital, maka kriptografi adalah disiplin ilmu yang mempelajari teknik enkripsi naskah asli (plaintext) yang tersusun acak, dengan memanfaatkan kunci enkripsi sehingga naskah tersebut berubah menjadi teks yang sulit terbaca (ciphertext) oleh user yang tidak memiliki kunci dekripsi.

Selanjutnya, ada istilah kriptografi klasik merupakan teknik cryptography yang pembuatannya tidak memerlukan bantuan komputer dan biasanya menggunakan alat bantu pena, batu, kertas, dan alat tradisional lainnya.

Soal 5

Dalam sebuah organisasi berskala besar dan memiliki sistem digital, pengamanan jaringan telekomunikasi sangat diperlukan. Organisasi tersebut harus memiliki SDM yang bisa diandalkan dalam bidang kemanan jaringan, seperti hacker, cracker, ataupun programmer.

Upaya yang bisa dilakukan adalah:

1. Membuat sistem pertahanan yang kuat
2. Mengoptimasi setiap algoritma yang berjalan
3. Menutup celah yang terbuka pada sistem
4. Pemeliharaan sistem secara rutin harus dilakukan
5. Menggunakan software keamanan jaringan yang baguis

Soal 6

Tugas yang pertama dibuat adalah artikel mengenai LAND Attack.

LAND Attack adalah jenis serangan semacam DoS yang menyerang server secara terus menerus hingga membuatnya down.

Tugas kedua adalah mereview beberapa software kemanan jaringan. Isinya kurang lebih sama dengan soal nomor 3.

Tugas ketiga adalah presentasi kelompok yang menjelaskan mengenai Steganografi.

Steganografi adalah teknik menyisipkan pesan dalam suatu file. Berbeda dengan kriptografi yang mengubah bentuk fisik file, teknik ini hampir tidak mengubah bentuk fisik sama sekali (berubah, namun tak kasat mata).