Muhammad Firdaus Sukma Adi
A11.2021.13396
A11.4304

SISTEM INFORMASI - TUGAS 3
UPAYA MENGAMANKAN JARINGAN KOMPUTER

Serangan terhadap keamanan sistem informasi (security attack) dewasa ini seringkali terjadi. Kejahatan computer (cyber crime) pada dunia maya seringkali dilakukan oleh sekelompok orang yang ingin menembus suatu keamanan sebuah sistem. Aktivitas ini bertujuan untuk mencari, mendapatkan, mengubah, dan bahkan menghapus informasi yang ada pada sistem tersebut jika memang benar-benar dibutuhkan. Ada beberapa kemungkinan tipe dari serangan yang dilakukan oleh penyerang yaitu :

1. Interception yaitu pihak yang tidak mempunyai wewenang telah berhasil mendapatkan hak akses informasi.
2. Interruption yaitu penyerang telah dapat menguasai sistem, tetapi tidak keseluruhan. Admin asli masih bisa login.
3. Fabrication yaitu penyerang telah menyisipkan objek palsu ke dalam sistem target.
4. Modification yaitu penyerang telah merusak sistem dan telah mengubah secara keseluruhan.

Menurut David Icove, dilihat dari lubang keamanan yang ada pada suatu sistem, keamanan dapat diklasifikasikan menjadi empat macam :

1) Keamanan Fisik (Physical Security)

Suatu keamanan yang meliputi seluruh sistem beserta peralatan, peripheral, dan media yang digunakan. Biasanya seorang penyerang akan melakukan wiretapping (proses pengawasan dan penyadapan untuk mendapatkan password agar bisa memiliki hak akses). Dan jika gagal, maka DOS (Denial Of Service) akan menjadi pilihan sehingga semua service yang digunakan oleh komputer tidak dapat bekerja. Sedangkan cara kerja DOS biasanya mematikan service apa saja yang sedang aktif atau membanjiri jaringan tersebut dengan pesan-pesan yang sangat banyak jumlahnya. Secara sederhana, DOS memanfaatkan celah lubang keamanan pada protokol TCP/IP yang dikenal dengan Syn Flood, yaitu sistem target yang dituju akan dibanjiri oleh permintaan yang sangat banyak jumlahnya (flooding), sehingga akses menjadi sangat sibuk.

2) Keamanan Data dan Media

Pada keamanan ini penyerang akan memanfaatkan kelemahan yang ada pada software yang digunakan untuk mengolah data. Biasanya penyerang akan menyisipkan virus pada komputer target melalui attachment pada e-mail. Cara lainnya adalah dengan memasang backdoor atau trojan horse pada sistem target. Tujuannya untuk mendapatkan dan mengumpulkan informasi berupa password administrator. Password tersebut nantinya digunakan untuk masuk pada account administrator.

3) Keamanan Dari Pihak Luar

Memanfaatkan faktor kelemahan atau kecerobohan dari orang yang berpengaruh (memiliki hak akses) merupakan salah satu tindakan yang diambli oleh seorang hacker maupun cracker untuk dapat masuk pada sistem yang menjadi targetnya. Hal ini biasa disebut social engineering. Social engineering merupakan tingkatan tertinggi dalam dunia hacking maupun cracking. Biasanya orang yang melakukan social engineering akan menyamar sebagai orang yang memakai sistem dan lupa password, sehingga akan meminta kepada orang yang memiliki hak akses pada sistem untuk mengubah atau mengganti password yang akan digunakan untuk memasuki sistem tersebut.

4) Keamanan dalam Operasi

Merupakan salah satu prosedur untuk mengatur segala sesuatu yang berhubungan dengan sistem keamanan pasca serangan. Dengan demikian, sistem tersebut dapat berjalan baik atau menjadi normal kembali. Biasanya para penyerang akan menghapus seluruh log-log yang tertinggal pada sistem target (log cleaning) setelah melakukan serangan.

Firewall merupakan suatu cara atau mekanisme yang diterapkan baik terhadap hardware, software ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN). Penggunaan firewall secara umum di peruntukkan untuk melayani :

1. Mesin/computer setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
2. Jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang di miliki oleh perusahaan, organisasi dsb.

Firewall adalah sebuah pembatas antara suatu jaringan lokal dengan jaringan lainnya yang sifatnya publik sehingga setiap data yang masuk dapat diidentifikasi untuk dilakukan penyaringan sehingga aliran data dapat dikendalikan untuk mencegah bahaya/ancaman yang datang dari jaringan public.

Firewall juga dapat memantau informasi keadaan koneksi untuk menentukan apakah ia hendak mengizinkan lalu lintas jaringan. Umumnya hal ini dilakukan dengan memelihara sebuah tabel keadaan koneksi (dalam istilah firewall: state table) yang memantau keadaan semua komunikasi yang melewati firewall. Secara umum Fungsi Firewall adalah untuk:

1. Mengatur dan mengontrol lalu lintas.
2. Melakukan autentikasi terhadap akses.
3. Melindungi sumber daya dalam jaringan privat.
4. Mencatat semua kejadian, dan melaporkan kepada administrator