Nama : Rahmi Aulia
NIM : 21110983019
Kelas : TRPL 3C

I. DEFINISI SECURITY PADA SISTEM TERDISTRIBUSI

Keamanan pada sistem terdistribusi adalah praktik dan upaya yang dilakukan untuk melindungi komputer-komputer yang terhubung dalam jaringan terdistribusi dari ancaman, risiko, serta upaya yang tidak sah atau merusak, dengan tujuan menjaga kerahasiaan, integritas, dan ketersediaan data serta sumber daya yang terdistribusi tersebut.

Security memuat hal-hal semacam :

1. **Proteksi Data :** Keamanan sistem terdistribusi berarti melindungi data yang disimpan dan dipertukarkan antar komputer agar tidak jatuh ke tangan yang salah.
2. **Identifikasi dan Otentikasi :** Mengenali siapa yang boleh mengakses sistem dan memastikan mereka adalah orang yang seharusnya dengan menggunakan kata sandi, kartu akses, atau metode otentikasi lainnya.
3. **Otorisasi :** Setelah identifikasi, keamanan juga mencakup memberikan hak akses yang tepat kepada pengguna atau komputer tertentu. Jadi, tidak semua orang punya akses penuh.
4. **Pemantauan :** Memantau aktivitas sistem secara terus-menerus untuk mendeteksi aktivitas mencurigakan atau aneh yang bisa menjadi tanda-tanda ancaman.
5. **Pencegahan dan Deteksi :** Mencegah serangan dengan firewall, antivirus, dan langkah-langkah keamanan lainnya, serta mendeteksi serangan jika terjadi.
6. **Enkripsi :** Menggunakan teknik enkripsi untuk menyandikan data sehingga hanya orang yang memiliki kunci yang tepat yang bisa membaca atau memahaminya.
7. **Manajemen Krisis** : Memiliki rencana darurat untuk mengatasi situasi darurat jika sistem terdistribusi mengalami masalah keamanan, seperti serangan.
8. **Pembaruan dan Pemeliharaan :** Melakukan pembaruan teratur pada perangkat lunak dan sistem agar mendapatkan perlindungan terbaru dari ancaman keamanan.
9. **Pemulihan Data :** Mempersiapkan langkah-langkah pemulihan jika data atau sistem mengalami kerusakan atau kehilangan.
10. **Pelatihan Pengguna :** Mengajarkan pengguna cara menggunakan sistem dengan aman dan menjaga keamanan mereka sendiri.

II. ANCAMAN DAN SERANGAN

Tujuan utama dari sebuah keamanan adalah untuk membatasi akses informasi & sumber hanya untuk user yang memiliki hak akses. Ancaman dan serangan pada sistem terdistribusi merujuk pada potensi bahaya dan tindakan yang dapat merusak atau mengganggu integritas, kerahasiaan, dan ketersediaan komputer-komputer dalam jaringan terdistribusi.

1. Ancaman

Ancaman adalah situasi atau kondisi yang memiliki potensi untuk mengakibatkan kerugian atau gangguan pada sistem terdistribusi. Ancaman bisa berupa ancaman fisik

seperti kebakaran atau banjir, atau ancaman siber seperti virus komputer, malware, atau peretas (hacker).

Ada tiga jenis acaman :

- **Leakage (kebocoran)**, mengacu pada tindakan atau insiden yang mengakibatkan informasi rahasia atau data sensitif keluar dari sistem terdistribusi tanpa izin. Ini bisa terjadi karena kesalahan konfigurasi, kerentanan keamanan, atau tindakan penyerangan. Kebocoran dapat menyebabkan pengungkapan informasi yang seharusnya tidak diketahui oleh pihak lain, seperti data pribadi pengguna atau informasi bisnis rahasia.

- **Tampering (Pencurian)**, adalah tindakan yang melibatkan perubahan atau manipulasi data atau sumber daya dalam sistem terdistribusi dengan cara yang tidak sah. Ini bisa mencakup pencurian atau perubahan data, konfigurasi, atau aplikasi. Tujuan dari tampering bisa beragam, termasuk pencurian informasi, penggantian data, atau merusak integritas sistem.

- **Vandalism (Vandalisme)**, merujuk pada tindakan merusak atau merusak sumber daya dalam sistem terdistribusi. Ini bisa mencakup penghapusan data, merusak perangkat keras, atau mengganggu operasi normal sistem dengan niat merusak. Vandalisme seringkali dilakukan tanpa tujuan finansial atau pencurian, tetapi dengan niat untuk mengacaukan atau merusak.

  Ancaman-ancaman yang termasuk dalam tiga jenis ancaman di atas (leakage, tampering, dan vandalism) dapat diklasifikasikan sebagai berikut:

  Ancaman Leakage (Kebocoran):

  1. Pencurian Data: Upaya untuk mencuri data rahasia atau informasi sensitif dari sistem terdistribusi, seperti informasi identitas pribadi atau data bisnis.
  2. Kebocoran Informasi: Penyusupan yang tidak sah ke dalam sistem untuk mengakses atau mengungkapkan informasi yang tidak boleh diketahui oleh pihak lain.
  3. Pelanggaran Privasi: Ancaman yang menargetkan privasi individu atau organisasi dengan mengungkapkan data pribadi atau rahasia.
  4. Pencurian Kredensial: Mencuri kata sandi atau informasi otentikasi pengguna untuk mengakses akun atau sistem.

  Ancaman Tampering (Pencurian):

  1. Manipulasi Data: Upaya untuk mengubah atau memanipulasi data dalam sistem terdistribusi, baik untuk merusak integritasnya atau untuk mendapatkan keuntungan tertentu.
  2. Pencurian Informasi Rahasia: Tindakan untuk mengakses atau mencuri informasi rahasia atau data yang sah tanpa izin.
  3. Penggantian Data: Merusak atau menggantikan data asli dengan data palsu atau yang telah dimodifikasi.

4. Pengendalian Sistem: Mencoba mengambil alih kendali sistem terdistribusi untuk tujuan yang tidak sah.

Ancaman Vandalism (Vandalisme):

1. Merusak Perangkat Keras: Upaya untuk merusak atau merusak perangkat keras fisik dalam sistem terdistribusi, seperti menghancurkan server atau router.
2. Pengganggguan Layanan: Tindakan yang bertujuan mengganggu operasi normal sistem dengan merusak aplikasi, proses, atau layanan yang berjalan.
3. Penghancuran Data: Menghapus atau merusak data yang ada dalam sistem, menyebabkan hilangnya informasi yang penting.
4. Pemblokiran Akses: Mencegah pengguna sah untuk mengakses sumber daya atau layanan dalam sistem terdistribusi.
5. Penyusupan Fisik: Ancaman yang melibatkan akses fisik yang tidak sah ke perangkat keras atau pusat data, yang dapat mengakibatkan kerusakan atau manipulasi perangkat fisik.

2. **Serangan**

Serangan adalah tindakan yang dilakukan oleh pihak yang tidak sah atau berpotensi merusak dengan tujuan mengambil alih atau merusak sistem terdistribusi. Contoh serangan termasuk peretasan (hacking), serangan DDoS (Distributed Denial of Service) yang membanjiri jaringan dengan lalu lintas palsu, serta pencurian data atau informasi penting.

Serangan dapat dibedakan menjadi dua kategori utama :

- **Serangan Pasif**

  Serangan pasif adalah serangan yang biasanya melibatkan pengamatan atau penyelidikan terhadap sistem tanpa mempengaruhi operasional sistem tersebut secara langsung. Tujuan utama serangan pasif adalah untuk mengumpulkan informasi tanpa melakukan perubahan atau kerusakan yang nyata.

  Beberapa contoh serangan pasif meliputi:

  1. Pengintipan (Eavesdropping): Penyerang mencoba untuk mendengarkan atau mengintersep komunikasi antara komputer-komputer dalam jaringan untuk mengakses informasi rahasia, seperti percakapan atau data yang dikirimkan secara tidak terenkripsi.
  2. Pencarian Informasi Publik: Penyerang mencari informasi yang tersedia secara publik untuk memahami lebih banyak tentang infrastruktur atau penggunaan sistem terdistribusi.
  3. Analisis Trafik: Penyerang menganalisis pola lalu lintas jaringan untuk mengidentifikasi celah atau titik masuk yang potensial.

- **Serangan Aktif**

  Serangan aktif adalah serangan yang secara aktif mencoba untuk mempengaruhi sistem atau data dalam sistem terdistribusi. Tujuannya adalah untuk merusak, mengubah, atau menghentikan operasi sistem. Beberapa contoh serangan aktif meliputi:

  1. Virus dan Malware: Penyerang mengirimkan perangkat lunak jahat ke dalam sistem terdistribusi dengan tujuan menginfeksi komputer dan merusak data atau mengendalikan sistem.
  2. Penginjeksian Paket (Packet Injection): Penyerang mengirimkan paket data palsu ke jaringan dengan niat untuk mengganggu atau memanipulasi komunikasi antar komputer.
  3. Serangan DDoS (Distributed Denial of Service): Penyerang menggunakan banyak komputer yang dikendalikan untuk membanjiri sistem terdistribusi dengan lalu lintas sehingga membuatnya tidak dapat diakses oleh pengguna yang sah.
  4. Pencurian Data (Data Theft): Penyerang mencoba mencuri data sensitif dari sistem, seperti informasi pengguna atau informasi bisnis, dengan tujuan eksploitasi.
  5. Manipulasi Konfigurasi: Penyerang mencoba mengubah konfigurasi sistem atau perangkat keras untuk mengganggu operasi normal atau memperoleh akses yang tidak sah.
  6. Penyusupan (Intrusion): Penyerang mencoba untuk masuk ke dalam sistem terdistribusi secara ilegal dengan tujuan merusak atau mencuri data.

III. METODE PENYERANGAN

Metode penyerangan pada sistem terdistribusi adalah cara-cara atau teknik yang digunakan oleh penyerang untuk mencoba mengakses, merusak, atau mengambil alih sistem terdistribusi. Metode-metode ini digunakan dengan niat merusak, mencuri data, atau mengganggu operasi normal dari jaringan atau komputer dalam sistem terdistribusi. Ada beberapa jenis metode penyerangan yang sering digunakan dalam konteks keamanan komunikasi dan sistem terdistribusi, yakni :

1. **Eavesdropping (Pengintipan)**

   Eavesdropping adalah metode di mana penyerang mencoba untuk mendengarkan atau mengintersep komunikasi antara dua entitas tanpa diketahui oleh pihak yang berkomunikasi.

   - Penyerang menguping atau memata-matai lalu lintas data atau pesan yang sedang dikirimkan antara pengirim dan penerima.
   - Tujuannya adalah untuk mengakses informasi rahasia atau data yang dikirimkan, yang dapat digunakan untuk kepentingan penyerang.
   - Contoh : Seorang penyerang mencoba mendengarkan percakapan telepon antara dua individu dengan menggunakan perangkat penyadap suara.

2. **Masquerading (Pemalsuan Identitas)**

Masquerading, juga dikenal sebagai spoofing, adalah metode di mana penyerang berpura-pura menjadi entitas atau pengguna yang sah untuk mendapatkan akses yang tidak sah.

- Penyerang mencoba untuk menyamar sebagai pengguna atau sistem terpercaya untuk mendapatkan izin atau hak akses tertentu.
- Ini bisa mencakup pemalsuan alamat IP, identitas pengguna, atau asal data.
- Contoh : Seorang penyerang mengirimkan email yang tampaknya berasal dari perusahaan bank terkemuka dengan tujuan meminta informasi login dan kata sandi pengguna.

3. Message Tampering (Pencurian Pesan)

Message tampering adalah metode di mana penyerang mencoba untuk mengubah atau memanipulasi pesan atau data yang dikirimkan antara dua entitas dalam komunikasi.

- Penyerang dapat memodifikasi data dalam pesan untuk mengirimkan informasi yang salah atau merusak integritas pesan.
- Tujuannya adalah untuk mempengaruhi hasil atau operasi yang sedang berlangsung.
- Contoh : Seorang penyerang mengecilkan jumlah uang dalam pesan transfer bank sebelum mengirimkannya, mengubah nominalnya dari $1.000 menjadi $100 sebelum pesan sampai ke bank penerima.

4. Replaying (Pemutaran Ulang)

Replaying adalah metode di mana penyerang merekam dan kemudian memutarkan ulang pesan atau tindakan yang sebelumnya telah dilakukan oleh entitas yang sah.

- Penyerang mencoba untuk mengirimkan kembali pesan yang telah direkam sebelumnya untuk mendapatkan manfaat tertentu.
- Ini dapat digunakan untuk mengulangi transaksi atau perintah yang telah dijalankan oleh pengguna sah.
- Contoh : Seorang penyerang merekam percakapan telepon antara dua individu yang mengandung kesepakatan bisnis dan kemudian memutar ulang rekaman tersebut untuk mengakali salah satu pihak.