Nama:dapa imanuel simanjuntak

Nim2281044

Denial of Service (DoS)

Serangan DoS adalah serangan yang dilakukan untuk membanjiri sumber daya jaringan, sehingga membuat layanan yang tersedia menjadi tidak dapat diakses atau menjadi sangat lambat. Serangan ini dilakukan dengan cara membanjiri jaringan dengan banyak permintaan atau trafik yang tidak perlu atau palsu. Cara mengatasi serangan DoS adalah dengan memperkuat infrastruktur jaringan, memblokir alamat IP yang mencurigakan, dan menggunakan teknologi seperti firewall dan IDS (Intrusion Detection System) untuk mendeteksi dan mencegah serangan DoS.

Man in the Middle (MitM)

Serangan MitM adalah serangan di mana penyerang dapat mengakses data yang dikirimkan antara dua pihak yang sedang berkomunikasi di internet. Dalam serangan ini, penyerang memposisikan dirinya di antara kedua pihak dan mengambil alih komunikasi tersebut. Cara mengatasi serangan MitM adalah dengan menggunakan teknologi enkripsi seperti SSL/TLS, menjaga keamanan sertifikat SSL/TLS, dan memperbarui perangkat lunak dengan patch keamanan terbaru.

Phishing

Serangan phishing adalah serangan yang dilakukan dengan cara menipu pengguna internet agar memberikan informasi pribadi seperti kata sandi dan informasi kartu kredit. Serangan ini umumnya dilakukan dengan cara mengirimkan email palsu atau membuat situs web palsu yang terlihat seperti situs web asli. Cara mengatasi serangan phishing adalah dengan memberikan pelatihan pada pengguna internet untuk mengenali email dan situs web palsu, menggunakan perangkat lunak anti-phishing, dan menambahkan fitur verifikasi pada situs web yang sensitif.

Malware

Serangan malware adalah serangan yang dilakukan dengan cara menginfeksi perangkat komputer dengan program jahat seperti virus, worm, dan Trojan. Serangan ini dapat menyebabkan kerusakan pada perangkat dan mencuri informasi pribadi pengguna. Cara mengatasi serangan malware adalah dengan memperbarui perangkat lunak dengan patch keamanan terbaru, menggunakan perangkat lunak antivirus dan antimalware, dan tidak membuka lampiran email dari pengirim yang tidak dikenal.

Password Attack

Serangan password adalah serangan yang dilakukan dengan cara menebak atau mencuri kata sandi pengguna. Serangan ini dapat menyebabkan akses yang tidak sah ke akun pengguna dan mengakibatkan pencurian data pribadi. Cara mengatasi serangan password adalah dengan menggunakan kata sandi yang kuat dan berbeda untuk setiap akun, tidak menggunakan kata sandi yang mudah ditebak, dan menggunakan teknologi autentikasi multi-faktor.

APA ITU TATAKELOLA KEAMANAN INFORMASI ATAU JARINGAN?

Tatakelola Keamanan Informasi/Jaringan (Information/Network Security Management) adalah praktik untuk memastikan kerahasiaan, integritas, dan ketersediaan informasi dan sistem jaringan yang digunakan oleh suatu organisasi. Ini mencakup pengidentifikasian risiko keamanan, pengembangan dan penerapan kebijakan keamanan, pemantauan keamanan secara terus-menerus, serta penanganan insiden keamanan jika terjadi pelanggaran. Tujuannya adalah untuk melindungi informasi penting dari ancaman seperti peretasan, virus, malware, atau serangan siber lainnya yang dapat merugikan organisasi atau pelanggannya.