NAMA : ODE ANDI ALAMSYAH

NPM : 714230032

KELAS : 2A

Network sniffing merupakan ancaman keamanan jaringan yang secara langsung berkorelasi dengan seluruh kerangka threat modelling pada Modul 3, karena serangan ini berfokus pada pencurian informasi melalui jalur komunikasi. Dalam STRIDE, network sniffing secara jelas termasuk dalam kategori Information Disclosure, sebab penyerang berupaya memperoleh data yang seharusnya bersifat rahasia, seperti kredensial, token, dan informasi pengguna. Ancaman ini muncul ketika aliran data melewati trust boundary tanpa perlindungan yang memadai, misalnya tidak menggunakan TLS atau enkripsi end-to-end.

Risiko network sniffing dapat dianalisis lebih lanjut menggunakan DREAD, dengan nilai Damage dan Discoverability yang tinggi karena dampaknya besar dan metode serangannya mudah dilakukan pada jaringan yang lemah. Kemudian, dalam metodologi PASTA, serangan ini ditempatkan pada tahap Threat Analysis dan Weakness Analysis untuk menunjukkan bagaimana serangan dapat terjadi akibat celah dalam desain komunikasi.

Selain itu, CVSS dapat memberikan penilaian kuantitatif terhadap kerentanan yang memungkinkan sniffing, seperti penggunaan protokol tanpa enkripsi dengan Attack Vector berbasis jaringan dan dampak Confidentiality tinggi. Dalam pendekatan OCTAVE, network sniffing dipandang sebagai risiko organisasi yang memengaruhi aset informasi kritis dan memerlukan kebijakan jaringan yang kuat. Dengan demikian, serangan ini menunjukkan hubungan erat antara analisis ancaman teknis dan manajemen risiko menyeluruh.