Dasar Teknis Reverse Engineering

Istilah Penting dalam Reverse Engineering

1. Disassembler adalah program yang mengubah file biner (executable) mejadi file teks yang berisi kode Assembly
2. Kode Assembly merupakan representasi tekstual dari kode objek
3. Hasil disassembly bergantung pada jenis prosesor, tetapi beberapa disassembler mendukung banyak arsitektur CPU
4. Disassembler yang berkualitas tinggi merupakan alat esensial bagi seorang reverser
5. Decompiler adalah alat yang mengubah kode mesin menjadi representasi kode tingkat tinggi, biasanya menyerupai bahasa C
6. Membaca Assembly membutuhkan keahlian khusus, sementara hasil dekompilasi lebih mudah dipahami sehingga mempercepat proses analisis
7. Hasil dekompilasi tidak selalu identik dengan source code aslinya.
8. Debugger memungkinkan pengguna mengeksekusi program baris demi baris untuk mengamati, memodifikasi, dan memahami bagaimana program berjalan di CPU
9. Debugger memungkinkan developer atau reverser menghentikan eksekusi di titik tertentu (breakpoint) untuk memeriksa alur program, nilai variabel, isi memori, dan register CPU
10. Meskipun bekerja dengan kode mesin, debugger sering menampilkan program dalam bentuk yang lebih mudah dipahami, biasanya mirip source code
11. Debugger dan disassembly yang kuat bagi reverser untuk memahami perilaku program pada level assembly