Pengantar Reverse Engineering

Konsep Forward Engineering

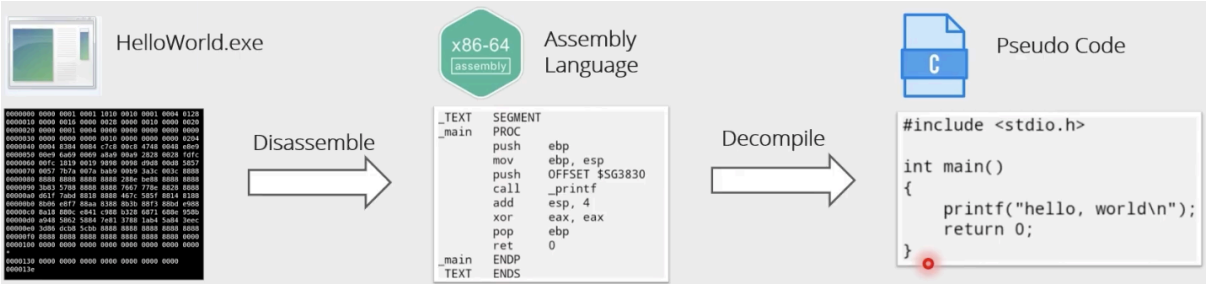
Forward Engineering adalah proses membangun software dari tahap perancangan hingga implementasi, di mana kode sumber ditulis, dikompilasi menjadi program biner, lalu dieksekusi menjadi proses yang dapat dijalankan oleh komputer.

Contoh :
Program C dicompile menjadi program.exe lalu dieksekusi dan dijalankan di komputer.

Konsep Reverse Engineering

Reverse Engineering atau Backwards Engineerig adalah proses di mana suatu objek buatan manusia dibongkar untuk mengungkap desain, kode, logic, atau untuk mengekstrak pengetahuan dari objek tersebut.

Contoh :
Dari file .exe di disassemble menjadi bahasa Assembly lalu dicompile menjadi pseudo code atau bahasa mirip program asli seperti C.



3 Tahapan Dasar Reverse Engineering

Dalam proses Reverse Engineering ada 3 tahap utama meliputi :

1. Information Extracting : Mengambil binary atau aplikasi target (misalnya malware) lalu mengekstrak informasi awal seperti strings, API calls, struktur file, dan perilaku dasar file.
2. Modeling/Analysis : Mengubah informasi yang diperoleh menjadi pemahaman konseptual tentang cara kerja malware, alur eksekusi, serta teknik proteksi yang digunakan

3. Review/Validation : Menguji pemahaman melalui debugging, sandboxing, atau pembuatan PoC exploit/patch untuk memastikan analisis benar dan dapat digunakan

Tujuan Reverse Engineering

1. Untuk memahami dan meningkatkan sistem
2. Menemukan kelemahan dan kerentanan
3. Analisis malware
4. Pemeliharaan dan pembaruan software