Table of Contents

Tersine Mühendislik

Temel Kavramlar ve Mimari

- Tersine Mühendisliğe Giriş: Etik, Yasal Boyut ve Kullanım Alanları
- Bilgisayar Mimarisi: CPU, Bellek Yönetimi (RAM), Yığın (Stack) ve Yığınak (Heap)
- İşletim Sistemi Temelleri: Windows API (Win32), Linux Syscalls ve Süreç (Process) Yapısı
- Güvenli Laboratuvar Kurulumu: Sanal Makineler (VM), Snapshotlar ve Sandbox Ortamları

Assembly Dili ve Makine Kodu

- Yazmaçlar (Registers), Bellek Adresleme ve Bayraklar (Flags)
- x86 ve x64 Assembly Komutları (MOV, PUSH, POP, CALL, JMP)
- ARM Assembly Temelleri (Mobil, IoT ve Apple Silicon için)
- Çağrı Uzlaşımları (Calling Conventions): cdecl, stdcall, fastcall, x64 ABI
- Program Akışı Kontrolü: İf-Else ve Döngülerin Assembly Karşılıkları

Statik Analiz

- Çalıştırılabilir Dosya Formatları: PE (Windows), ELF (Linux), Mach-O (macOS)
- Temel Statik Analiz Araçları: Strings, Binwalk, Detect It Easy (DiE), CFF Explorer
- IDA Pro / IDA Free: Disassembly, Graph View, Cross-References (XREF)
- Ghidra: Proje Yönetimi, Decompiler Kullanımı ve Kod Yapılandırma
- Statik Analiz Otomasyonu: IDAPython ve Ghidra Scripting

Dinamik Analiz ve Debugging

- Dinamik Analize Giriş ve Davranışsal Analiz (Procmon, Wireshark, Regshot)
- Debugger Araçları: x64dbg, GDB, OllyDbg ve WinDbg Kullanımı
- Kesme Noktaları (Breakpoints): Software (INT3), Hardware ve Memory Breakpoints
- Adımlama (Stepping): Step In (F7), Step Over (F8) ve Call Stack İzleme
- Binary Patching: Bellekte Kodu Değiştirme (JMP, NOPing) ve Yamalama

Enjeksiyon, Hooking ve Instrumentation

- DLL Enjeksiyon Teknikleri (CreateRemoteThread, SetWindowsHookEx)
- API Hooking Mantığı: Detours ve IAT (Import Address Table) Hooking
- Frida: Dinamik Enstrümantasyon (Dynamic Instrumentation) ve Mobil Tersine Mühendislik
- Cheat Engine ile Bellek Tarama (Memory Scanning) ve Pointer Bulma

Zararlı Yazılım Analizi ve Korunma

- Kod Karmaşıklaştırma (Obfuscation) Teknikleri ve Okunabilirliği Artırma
- Paketleyiciler (Packers - UPX, Themida) ve Kriptografik Tanımlama
- Unpacking: OEP (Original Entry Point) Bulma ve Bellekten Dump Alma
- Anti-Debugging ve Anti-VM (Sanal Makine Algılama) Tekniklerini Atlatma
- IoC (Indicators of Compromise) Çıkarma ve Raporlama

UCH Viki'den alınmıştır.