Windows Kernel Rootkit Development

From Architecture to Ethical Evasion Techniques

- Introduction
- Theory: Windows Kernel Architecture
- Theory: Windows Driver Model
- Theory: Basic Rootkit Skeleton
- **Techniques**
    1. Driver Installation as Service
    2. SSDT Hooking using a Kernel Driver
    3. Process Hiding using a Kernel Driver
    4. Network Port Manipulation Hide/Unhide
- Exercise
- Conclusions