Rootkits & Stealth Malware
Medium-granularity class topics covered
Xeno Kovah
CC BY AT licensed
hosted at OpenSecurityTraining.info

Overview

Detection Tools
- WinDbg
- GMER
- VirusBlokA
- da
- Tuluka

Persistence Techniques
- Volatility w/ Malware Plugin

- Inline Hooking
- IAT/EAT Hooking
- IDT
- System Service Descriptor Table (SSDT)
- Direct Kernel Object Manipulation (DKOM)
- OS Callbacks
- Kernel Object Hooking (KOH)
- Master Boot Record (MBR)
- Trusted Boot
- Trusted Boot
- Master Boot Record (MBR)