



## CYBERVIDYAPEETH FOUNDATION





















+91 971 114 7900 +91 893 973 2808 www.cybervidyapeeth.in

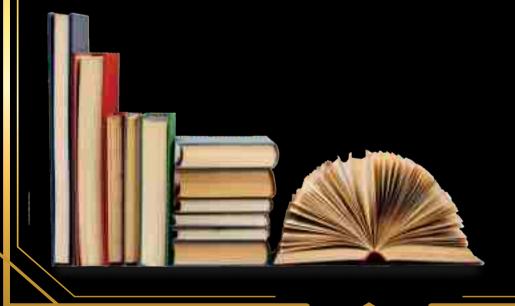
mentor@cybervidyapeeth.in

## THE **SYLLABUS**



нуль 2 автоматизированный

**Mastering Malware Reverse Engineering** 



## **Duration: 50 Days (400 Hours+)**

- Assembly Language: A Primer
- Machine Code and Human Code
- Sandbox making and Breaking
- Recommended system Hardening
- Algorithms: RC4 & More
- ntroduction to tooling: IDA PRO, GHIDRA, GDB,x32/64dbq
- Digging deep into IDA PRO
- Foothold
- Case Study: Analysis of ASUS SHADOW HAMMER

- Case Study: Analysis of IRC Botnet
- Persistence
- PrivEsc Techniques
- Injection and RigEK
- **POS**
- @ FIN7
- Hooking Engine
- @ Golang and Rust in Malware
- Yara: Introduction
- Stagers and droppers

- Evasion and deception
- Deep Malware Internals
- Case Study 3
- Developing and detecting wrappers
- **®** Obfuscation and Decoys
- Case Study 4
- Windows Internals: Part 1
- **@** Windows Internals: Part 2
- Playing with DLLs and LNK
- Case Study 5

- Yara: Advanced
- **@ AV/IDS/EDR/XDR Engines and Powerlessness**
- **@** Kernel Playground: BIOS/UEFI Malware
- Case Study 6
- Kernel debugging for Malware
- BsD and Linux
- Case Study 7
- Patching binaries and Plugin development
- Closing Remarks and Certification Test