Windows Internals for Malware Analysts & Reverse Engineers syllabus:

📝 Windows Internals – 2 Week Intensive

Focus: Malware Analysis, Reverse Engineering, and Security Research

Duration: 10 Days (Full-Day Sessions)

Format: Lectures + Hands-On Labs + Case Studies

Day 1 – Fundamentals & Tooling

Windows architecture: kernel vs. user mode

Core processes: SMSS, CSRSS, WINLOGON, LSASS, SERVICES.EXE

Subsystems: Win32, WoW64

Sysinternals Suite deep dive (ProcExp, ProcMon, Autoruns, VMMap)

Lab: Process monitoring & tracing with ProcMon

Day 2 – Processes & Threads

Process objects & job objects

Thread internals, scheduling, APCs

Handle tables & object manager

Lab: Inspecting threads, handles, and injections with WinDbg + x64dbg

---

Day 3 – Memory Management

Virtual memory, paging, working sets

DLL loading, PE format, injection methods

Malware injection techniques (CreateRemoteThread, hollowing, reflective DLLs)

Lab: Debugging a process hollowing malware sample

Day 4 – Security & Tokens

Windows security model: SIDs, ACLs, tokens, privileges

LSASS, authentication flows (NTLM, Kerberos)

Integrity levels, AppContainer, UAC bypasses

Lab: Analyzing Mimikatz credential dumping behavior

Day 5 – Mitigations & Defenses

DEP, ASLR, Control Flow Guard

Virtualization-Based Security (Credential Guard, Device Guard)

Code Integrity, PatchGuard, AMSI

Lab: Testing AMSI bypass techniques in a safe lab

Day 6 – I/O, File System & Registry

Windows I/O Manager & IRPs

NTFS internals: MFT, alternate data streams

Registry internals: hives, logs, volatile keys

Malware persistence via registry, services, drivers

Lab: Detect persistence with Autoruns & registry forensics tools

---

Day 7 – Event Logging & ETW

Windows Event Logs & ETW internals

Sysmon deep dive (event types, detection configs)

Event tracing for malware detection

Lab: Configure Sysmon to detect process injection & persistence

---

Day 8 – Kernel & Rootkits

Interrupts, SSDT, IDT

Kernel drivers & exploitation basics

DKOM (Direct Kernel Object Manipulation)

Rootkit detection & PatchGuard internals

Lab: Analyze a kernel rootkit sample (with WinDbg kernel debugging)

Day 9 – Forensics & Malware Case Studies

Memory forensics (Volatility)

Crash dump analysis

Registry carving

Case studies:

Ransomware NTFS operations & shadow copy deletion

Credential theft malware in LSASS

Day 10 – Capstone & ATT&CK Mapping

Mapping techniques to MITRE ATT&CK

Red vs. Blue exercise:

Inject, persist, exfiltrate (attacker role)

Detect, analyze, mitigate (defender role)

Final case study: Analyze and document a complete malware infection chain