K7 ACADEMY

Malware Analysis Course - Windows

Course Overview

The K7 Academy Malware Analysis Course is a comprehensive 4-month, 160-hour program designed for individuals seeking deep expertise in identifying, dissecting, and neutralising malicious software. Spanning dynamic analysis, static inspection, and advanced reverse engineering, the course is built around extensive hands-on labs using real malware samples — equipping you to be job-ready as a malware analyst, reverse engineer, or SOC Tier 2/3 specialist.

Mode	Duration	Level
Online/Offline Classes	4 Months | 160 Hours	Beginner to Intermediate

Who Should Enroll?

- Cybersecurity Students seeking a career in malware research or reverse engineering
- SOC Analysts looking to level up to Tier 2 / Tier 3 analysis
- Security Analysts wanting structured malware investigation skills
- Incident Responders who need to understand malware behaviour during IR
- Threat Hunters building IOC generation and detection engineering skills
- Ethical Hackers expanding into defensive malware tradecraft
- Digital Forensics Professionals adding malware analysis to their toolkit

Learning Outcomes

- Understand Windows internals, persistence mechanisms, and malware infection vectors
- Set up fully isolated lab environments for safe malware analysis
- Perform static analysis of PE files — headers, strings, hashing, and packer detection
- Reverse engineer packed malware using IDA Pro, OllyDbg, and x86 assembly
- Conduct dynamic analysis — observe file, registry, network, and process behaviour
- Analyse and classify malware behaviour using industry-standard monitoring tools
- Detect persistence mechanisms and evasion techniques (Anti-VM, Anti-Debug)
- Generate actionable Indicators of Compromise (IOCs) from malware samples
- Write professional malware analysis reports for SOC and threat intelligence teams
- Support SOC operations, threat hunting workflows, and incident response activities

Course Modules

Module 1 — Dynamic Windows Malware Analysis

- Introduction to Windows Malware
- Malware Terminology & Classification
- Windows Internals & Registry
- Windows Boot Process & Persistence
- Malware Infection Vectors
- Virtualization & Sandboxing
- Monitoring Tools (Process, File, Network)
- Behavioral Classification of Malware

Practical Labs

- Setting up isolated malware analysis lab
- Executing malware samples safely
- Observing file, registry, and network changes
- Behavior-based malware classification

Module 2 — Static Windows Malware Analysis

- Introduction to Static Malware Analysis
- Number Systems & Base Conversions
- Endianness and Byte Ordering
- File Attributes and Hashing
- Strings Analysis
- Windows PE File Format & Headers
- File Signatures & Magic Numbers
- Packed & Obfuscated Malware Detection

Practical Labs

- Manual hexadecimal analysis
- PE header inspection
- String and hash-based analysis
- Packer identification exercises

Module 3 — Reverse Engineering Malware Analysis *(80 Hours)*

- Fundamentals of Reverse Engineering
- Malware RE Use Cases
- Introduction to x86 Assembly Language
- Microprocessor Architecture
- Registers and Flags
- Stack Operations & Function Calls
- Control Flow & Branching Instructions
- Debugging Concepts & OllyDbg
- Disassemblers (IDA)
- Packed & Obfuscated Malware Analysis

Practical Labs

- Assembly code tracing
- Debugging malware samples
- Anti-VM and Anti-Debugging techniques
- API call analysis
- Packed malware reverse engineering

Tools & Technologies Covered

FlareVM
Windows malware analysis distro

MalwareBazaar
Malware sample repository

IDA Pro / Free
Industry-standard disassembler & decompiler

OllyDbg
x86 debugger for dynamic RE

x64dbg
Modern open-source debugger

Regshot
Registry snapshot diff for malware analysis

PE-bear / CFF Explorer
PE header inspection & editing

Detect-It-Easy (DIE)
Packer and compiler identification

FakeNet-NG
Network simulation for malware C2 analysis

Process Monitor
File, registry & network event monitoring

Process Hacker
Process and memory inspection

Wireshark
Network traffic capture and analysis

ANY.RUN / CAPE
Interactive & automated sandbox analysis

VirusTotal
Multi-engine file & hash reputation

Career Opportunities

Role

- Malware Analyst
- Reverse Engineer
- Threat Intelligence Analyst
- SOC Analyst – Tier 2 / Tier 3
- Incident Response Analyst
- Digital Forensics Investigator
- Detection Engineer

Certification & Assessment

- Module-wise Assessments
- Practical Lab Reports — written analysis submitted for each hands-on exercise
- Practical Malware Analysis Challenge — analyse an unknown malware sample end-to-end
- Final Certification Exam — Passing Score: 70%

K7 ACADEMY

www.k7academy.com