HACKSTRIX CERTIFIED MALWARE ANALYST (HCMA)

The **Hackstrix Certified Malware Analyst (HCMA)** program is an advanced, practical, and industry-focused cybersecurity training designed to equip learners with expertise in **malware analysis, reverse engineering, digital forensics, malware detection, threat hunting, exploit analysis, memory forensics, rootkit analysis, and malware intelligence**.

This program emphasizes **hands-on malware analysis in real-world environments**, enabling students to analyze modern malware families including:

- Trojans
- Ransomware
- Rootkits
- Spyware
- Banking Malware
- Credential Stealers
- Fileless Malware
- Mobile Malware
- Advanced Persistent Threats (APTs)

Students will develop skills in **static analysis, dynamic analysis, reverse engineering, malware behavior profiling, memory investigation, unpacking techniques, and malware reporting**.

MODULE 1: Introduction to Malware & Malware Analysis

Topics Covered

- Introduction to Malware
- History of Malware Evolution
- Goals of Malware Analysis
- Malware Lifecycle
- Malware Categories and Types
    - Virus
    - Worm
    - Trojan
    - Ransomware
    - Rootkits

    - Botnets
    - Spyware
    - Keyloggers
    - Banking Malware
    - Fileless Malware
- Malware Behavior and Capabilities
- Threat Landscape & Modern Malware Trends
- Malware-as-a-Service (MaaS)
- Supply Chain Attacks
- Malware Intelligence
- Threat Hunting Fundamentals
- MITRE ATT&CK Framework
- Malware Tactics, Techniques & Procedures (TTPs)
- Cyber Kill Chain Mapping

Practical Labs

- Malware Identification
- Threat Actor Profiling
- Malware Classification Exercises

MODULE 2: Malware Analysis Fundamentals

Static Analysis Basics

- Antivirus Scanning
- File Hashing (MD5, SHA1, SHA256)
- Finding Strings
- Metadata Analysis
- Entropy Analysis
- File Encoding
- Malware Signatures
- Linked Libraries and Functions
- Identifying Indicators of Compromise (IOCs)

Dynamic Analysis Basics

- Sandboxing
- Malware Execution Monitoring

- Process Monitoring
- Registry Monitoring
- File System Monitoring
- Runtime Behavioral Analysis
- Malware Persistence Observation

Practical Labs

- Runtime Malware Analysis
- Process Explorer Analysis
- Registry Snapshot Comparison
- Malware Sandbox Deployment

MODULE 3: Portable Executable (PE) & Windows Internals

Topics Covered

- Windows Architecture Fundamentals
- Executable File Structures
- Portable Executable (PE) Format
- PE Headers & Sections
- Import Address Table (IAT)
- Export Table
- Entry Point Analysis
- DLLs & Windows APIs
- Handles, Mutexes & Tokens
- COM Objects
- Networking APIs
- Data Encoding Techniques

Tools Covered

- PEView
- PEStudio
- Detect It Easy (DIE)
- CFF Explorer

Practical Labs

- PE File Dissection
- Executable Metadata Analysis

- Header Manipulation

MODULE 4: Reverse Engineering & Assembly

Topics Covered

- Introduction to Reverse Engineering
- Binary Analysis Concepts
- x86/x64 Assembly Language
- CPU Registers
- Memory Stack
- Functions & Offsets
- Arithmetic Operations
- Branching & Conditionals
- Loops
- Call Conventions
- Main Function Analysis
- Control Flow Analysis
- Graph-Based Analysis

Tools Covered

- IDA Pro
- Ghidra
- x64dbg
- OllyDbg
- GDB
- Objdump

MODULE 5: Advanced Dynamic Malware Analysis

Topics Covered

- Advanced Debugging
- Memory Inspection
- Runtime Decryption
- Malware Execution Tracing
- Process Hollowing
- DLL Injection

- Process Injection
- APC Injection
- Hook Injection
- Process Replacement
- API Hooking
- Detours Framework

Practical Labs

- Malware Memory Dumping
- Debugger-based Malware Analysis
- Process Injection Detection

MODULE 6: Malware Functionality Analysis

Topics Covered

- Downloaders & Launchers
- Droppers
- Backdoors
- Credential Stealers
- Information Stealers
- Keylogging Techniques
- Browser Credential Theft
- Privilege Escalation
- Persistence Mechanisms
- Scheduled Tasks
- Registry Persistence
- Service Abuse

Practical Labs

- Credential Stealer Investigation
- Persistence Hunting
- Malware Function Classification

MODULE 7: Malware Obfuscation, Packing & Evasion

Topics Covered

- Packers & Crypters
- Packing & Unpacking Malware
- Polymorphic Malware
- Metamorphic Malware
- Obfuscation Techniques
- Anti-Disassembly
- Anti-Debugging
- VM Detection
- Sandbox Evasion
- TLS Callbacks
- SEH-based Evasion
- Self-Defending Malware

Practical Labs

- Packed Malware Detection
- Manual Unpacking
- Anti-analysis Bypass

MODULE 8: Malicious Documents & Web-based Malware

Topics Covered

- PDF Malware Analysis
- Microsoft Office Malware
- Macro Malware
- Malicious RTF Documents
- JavaScript Obfuscation
- Browser Exploits
- Malicious Websites
- Web Exploit Chains

Practical Labs

- PDF Reverse Analysis
- Office Macro Investigation
- Malicious Script Deobfuscation

MODULE 9: Memory Forensics & Malware Investigation

Topics Covered

- Memory Forensics Fundamentals
- RAM Acquisition
- Malware in Memory
- Volatility Framework
- Memory Artifacts
- Live Memory Analysis
- Fileless Malware Detection

Practical Labs

- Memory Dump Investigation
- Hidden Malware Discovery

MODULE 10: Rootkits & Kernel Malware Analysis

Topics Covered

- Windows Kernel Basics
- Windows Kernel APIs
- Windows Drivers
- Kernel Debugging
- Rootkit Fundamentals
- Hooking Techniques
- SSDT Hooking
- DKOM (Direct Kernel Object Manipulation)
- Kernel Patching
- Rootkit Anti-Forensics
- Covert Channels

Practical Labs

- Rootkit Detection
- Kernel Malware Analysis

MODULE 11: Network & Malware Traffic Analysis

Topics Covered

- Malware Network Communication
- HTTP/HTTPS Analysis
- DNS Tunneling
- C2 (Command & Control) Traffic
- ICMP Attacks
- Malware Traffic Profiling
- Network Indicators of Compromise
- Email Malware & Phishing Analysis

Tools Covered

- Wireshark
- TCPDump
- NetworkMiner

Practical Labs

- Malware Traffic Investigation
- IOC Extraction

MODULE 12: Mobile Malware Analysis

Android Malware Analysis

- Android Architecture
- App Development Lifecycle
- APK Structure
- APKTool
- APKInspector
- Dex2Jar
- JD-GUI
- Android Static Analysis
- Android Dynamic Analysis

iOS Malware Overview

- iOS Architecture
- iOS Malware Fundamentals

- iOS Forensics Tools

Practical Labs

- APK Reverse Engineering
- Android Malware Investigation

MODULE 13: Malware Detection, Classification & AI

Topics Covered

- Static Malware Classification
- Dynamic Malware Classification
- Hybrid Malware Analysis
- Behavioral Malware Classification
- Machine Learning in Malware Detection
- AI-based Malware Detection
- Threat Intelligence Integration

Practical Labs

- Malware Classification Models
- IOC Mapping

MODULE 14: Malware Forensics & Incident Response

Topics Covered

- Windows Malware Forensics
- Linux Malware Forensics
- Android Malware Forensics
- Digital Evidence Collection
- Incident Investigation
- Threat Attribution
- Malware Containment
- Malware Mitigation Techniques

Case Studies

- Ransomware Investigation
- Data Stealer Malware

- Android Malware Case Study
- Real-world APT Malware Campaigns

MODULE 15: Malware Analysis Capstone Project

Hands-on Final Project

Students will perform:

- Static Malware Analysis
- Dynamic Malware Analysis
- Malware Classification
- Reverse Engineering
- Traffic Analysis
- Memory Analysis
- IOC Extraction
- Threat Intelligence Mapping
- Final Malware Report Documentation

Practical Experiments

- Malware Discovery
- Runtime Analysis
- PE File Analysis
- Executable Packers
- Obfuscation Analysis
- Malware Behavior Investigation
- Office/PDF Malware Analysis
- Rootkit Analysis
- Malware Traffic Analysis
- Android Malware Analysis
- Advanced Malware Reverse Engineering
- Antivirus Integration
- Malware Documentation & Reporting

Tools Covered

Analysis Tools

- IDA Pro
- Ghidra
- x64dbg
- OllyDbg
- GDB
- Objdump

Static Analysis Tools

- PEView
- PEStudio
- DIE
- CFF Explorer

Dynamic Analysis Tools

- Procmon
- Process Explorer
- Regshot
- Wireshark
- TCPDump

Malware Labs

- REMnux
- Cuckoo Sandbox
- Any.Run

Certification Outcome

Upon successful completion, participants will earn: **HACKSTRIX CERTIFIED MALWARE ANALYST (HCMA)**