Vskills CERTIFIED

www.vskills.in

# Certified Malware Analysis Professional

# Certified Malware Analysis Professional

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

## Why should one take this certification?

This Course is intended for professionals and graduates wanting to excel in their chosen areas. It is also well suited for those who are already working and would like to take certification for further career progression.

Earning Vskills Certified Malware Analysis Professional Certification can help candidate differentiate in today's competitive job market, broaden their employment opportunities by displaying their advanced skills, and result in higher earning potential.

## Who will benefit from taking this certification?

Job seekers looking to find employment in IT security, or IT departments of various companies, students generally wanting to improve their skill set and make their CV stronger and existing employees looking for a better role can prove their employers the value of their skills through this certification.

## Test Details

- **Duration:** 60 minutes
- **No. of questions:** 50
- **Maximum marks:** 50, Passing marks: 25 (50%)

There is no negative marking in this module.

## Fee Structure

Rs. 3,499/- (Excludes taxes)*

*Fees may change without prior notice, please refer http://www.vskills.in for updated fees

# Table of Contents


## 1. Malware Analysis Basics and Lab Setup

1.1 What Is Malware and the Need for Malware Analysis

1.2 Types of Malware

1.3 Malware Analysis Methodology

1.4 How to Set Up Your Lab?

1.5 Why a Snapshot Is Useful?

1.6 Some Warnings

## 2. Dynamic Malware Analysis

2.1 Why Dynamic Analysis?

2.2 Monitoring System Processes

2.3 Analyzing Network Traffic

2.4 Detecting Local Changes

2.5 What Is a Debugger?

2.6 Basic Features of OllyDbg

2.7 Malware Analysis Using OllyDbg

## 3. Static Malware Analysis

3.1 Why Static Analysis?

3.2 x86 Instruction Set

3.3 Introduction to File Formats

3.4 Extracting Useful Information from Malware Binary

3.5 Finding Imports and Linked Files

3.6 How a Disassembler Can Help Us?

3.7 Basic Features of IDA Pro

3.8 Malware Analysis Using IDA Pro

## 4. Malware Evasion Techniques

4.1 Anti-Debugging

4.2 Anti-Disassembly

4.3 Anti-Virtual Machines

4.4 Data Encoding

4.5 Polymorphism

4.6 More Evasion Techniques

## 5. Malware Functionalities

5.1 Backdoors

5.2 Keyloggers and Information Stealers

5.3 Downloaders

5.4 Ransomware

5.5 Rootkits

## 6. Malware Advanced Techniques

6.1 Privilege Escalation

6.2 Persistence Methods

6.3 Data Encoding

6.4 Covert Launching Techniques

## 7. Advanced Dynamic Malware Analysis

7.1 Using a Debugger

7.2 An Overview of the Windows Environment

7.3 User Mode Debugging

7.4 Malware Analysis Using OllyDbg

7.5 Features of OllyDbg

7.6 Kernel Mode Debugging

7.7 Malware Analysis Using WINDBG

7.8 Features of WINDBG

## 8. Advanced Static Malware Analysis

8.1 Advanced Notes on the x86 Architecture

8.2 How a Disassembler Can Help Us

8.3 Loading and Navigating Using IDA Pro

8.4 Functions in IDA

8.5 IDA Pro Graphic Features

8.6 Analysing Malware Using IDA Pro

## 9. Malware Detection and Defence

9.1 Malware Detection Techniques

9.2 Steps to Clean a Compromised Network

9.3 How Intrusion Detection Systems Work

9.4 An Introduction to Snort

9.5 How to Setup Snort?

## 10. Evasive Malware

10.1 How Do Packers Work?

10.2 How to Detect Packed Malware?

10.3 How to Unpack a Malware Program?

10.4 Examples of Unpacking a Malware Program

# Certifications

**Accounting, Banking & Finance**
- Certified GST Professional
- Certified AML-KYC Compliance Officer
- Certified Business Accountant
- Certified BASEL III Professional
- Certified GAAP Accounting Standards Professional
- Certified Treasury Markets Professional

**Big Data**
- Certified Hadoop and Mapreduce Professional

**Cloud Computing**
- Certified Cloud Computing Professional

**Design**
- Certified Interior Designer

**Digital Media**
- Certified Social Media Marketing Professional
- Certified Inbound Marketing Professional
- Certified Digital Marketing Professional

**Foreign Trade**
- Certified Export Import (Foreign Trade) Professional

**Health, Nutrition and Well Being**
- Certified Fitness Instructor

**Hospitality**
- Certified Restaurant Team Member (Hospitality)

**Human Resources**
- Certified HR Compensation Manager
- Certified HR Staffing Manager
- Certified Human Resources Manager
- Certified Performance Appraisal Manager

**Office Skills**
- Certified Data Entry Operator
- Certified Office Administrator

**Project Management**
- Certified Master in Project Management
- Certified Scrum Specialist

**Real Estate**
- Certified Real Estate Consultant

**Marketing**
- Certified Marketing Manager

**Quality**
- Certified Six Sigma Green Belt Professional
- Certified Six Sigma Black Belt Professional
- Certified TQM Professional

**Logistics & Supply Chain Management**
- Certified International Logistics Professional
- Certified Logistics & SCM Professional
- Certified Supply Chain Management Professional

**Legal**
- Certified IPR & Legal Manager
- Certified Labour Law Analyst
- Certified Business Law Analyst
- Certified Corporate Law Analyst

**Information Technology**
- Certified Angular JS Professional
- Certified Basic Network Support Professional
- Certified Business Intelligence Professional
- Certified Core Java Developer
- Certified E-commerce Professional
- Certified IT Support Professional
- Certified PHP Professional
- Certified Selenium Professional

**Mobile Application Development**
- Certified Android Apps Developer
- Certified iPhone Apps Developer

**Security**
- Certified Ethical Hacking and Security Professional
- Certified Network Security Professional

**Management**
- Certified Corporate Governance Professional
- Certified Corporate Social Responsibility Professional
- Certified Leadership Skills Professional

**Life Skills**
- Certified Business Communication Specialist
- Certified Public Relations Officer

**Media**
- Certified Advertising Manager
- Certified Advertising Sales Professional

**Sales, BPO**
- Certified Sales Manager
- Certified Telesales Executive

**& many more job related certifications**

**Contact us at:**
**V-Skills**
**011-473 44 723 or info@vskills.in**
**www.vskills.in**