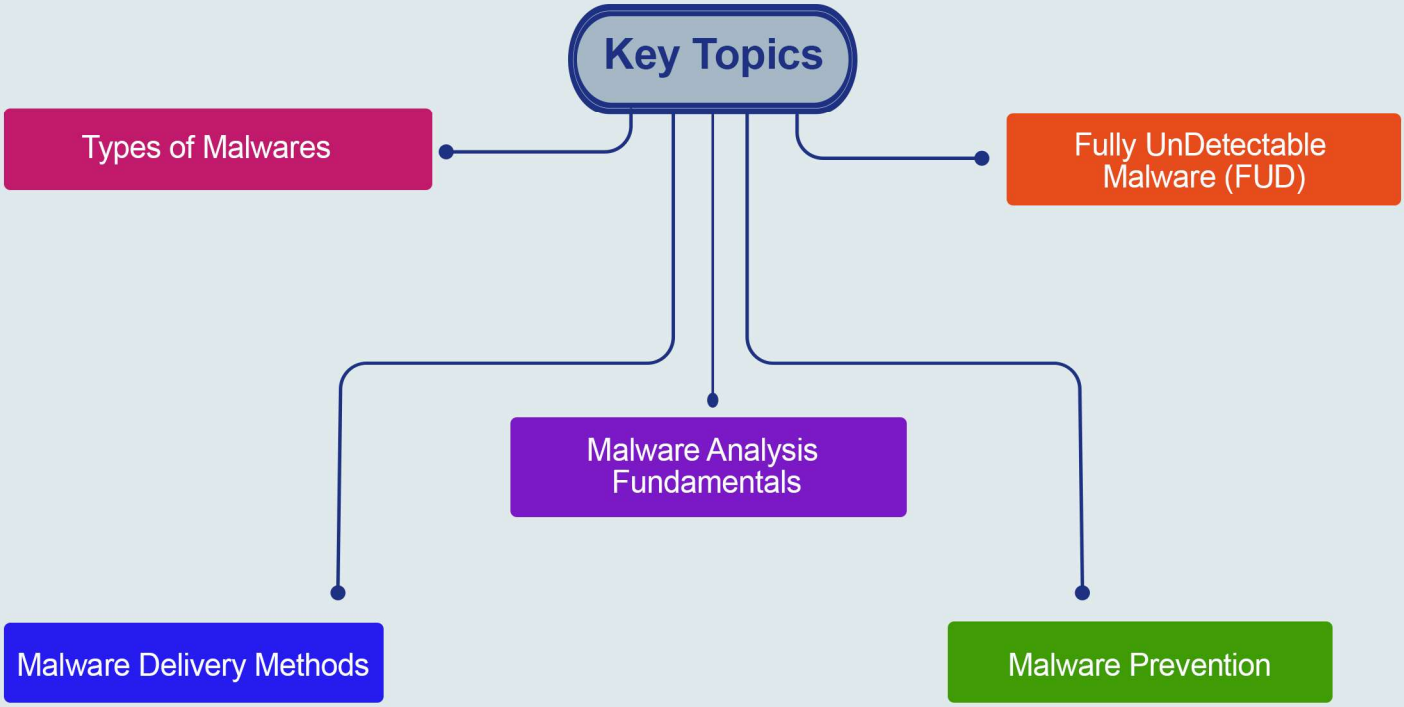
## About the Course

In this course, you will be introduced to the key concepts associated with performing malware analysis. You will learn how malicious actors attack organizations, users and endpoints and how you can begin to analyze the artifacts associated with these attacks. Finally, you will apply everything you have learned to begin to develop a workflow for performing malware analysis, identifying key indicators of compromise and the ability to create a narrative around an incident.

## Learning Objectives

1. How Malicious Actors Attack
2. Analyze the Artifacts Associated with Malware Attacks
3. Develop a Workflow for Performing Malware Analysis
4. Identify Key Indicators of Compromise
5. Familiarity with Types of Malwares
6. How to Prevent Malware

## Key Topics




## Pre Requisites

- Information Security Incident Management Course
- Cyber Security Forensics Course

Terminus System

## What You Will Receive

- Course Presentation File
- Complementary Files
- Malware Identification & Reverse Engineering eBook

## Who Should Attend

- Threat & Vulnerability Analysts
- Information Security Specialists
- Incident Responders
- Cyber Forensics Analysts

# Syllabus

## An Introduction to Malware

- Various types of malwares
- History of malware
- Malware trends

## Malware Delivery Methods

- Instant Messenger applications
- IRC
- Removable devices
- Attachment
- Legitimate “shrink-wrapped” software
- Browser and email software bugs
- NetBIOS
- Fake programs
- Untrusted sites and freeware software
- Downloading files

## Malware Analysis Fundamentals

- Reversing Malicious Code
- In-Depth Malware Analysis
- Examining Self-Defending Malware
- Malware Analysis Tournament

## Malware Prevention

- Email attachments
- Web (including URLs in emails)
- Remote Desktop Protocol (RDP)
- Abusing Microsoft Office

## Syllabus

### Fully UnDetectable Malware (FUD)

- Fully Undetectable Malware Creation

### Ransomware

- What is Ransomware
- How to Reduce Ransomware Risk

### Malware Threats

- Introduction to Malware
- Trojan Concepts
- Virus & Worm Concepts
- Malware Reverse engineering
- Malware Detection
- Countermeasures

## Hands-on Training

- Lab 1: Creating s Server using the ProRat Tool
- Lab 2: Wrapping a Trojan Using One File Exe Maker
- Lab 3: Proxy Server Trojan
- Lab 4: HTTP Trojan
- Lab 5: Creating a Virus
- Lab 6: Virus Analyzing