Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Dynamic Analysis with Sysinternals



This lab provides a comprehensive hands-on experience with Sysinternals tools to analyze a suspicious file. You will identify malware, analyze its properties, investigate persistence mechanisms, monitor registry and file activities, and explore its network behavior. Using tools like Process Explorer, Process Monitor, and Autoruns, you'll isolate Indicators of Compromise (IOCs) and mitigate threats. You'll also interact directly with malware via PuTTY, learning how to investigate and deactivate its behavior.