Document Generated: 11/24/2026

Learning Style: On Demand

Technology:

Difficulty: Beginner

Course Duration: 1 Hour

Lab - Process Investigation



Analyze a Windows memory dump using Volatility. You'll identify suspicious processes, examine loaded DLLs, scan for network connections, detect code injection, and verify findings using VirusTotal.