MALWARE INCIDENT AND LOG FORENSICS

Malware Analysis and Threat Hunting Training Program

Dark Vortex LLP

Table of Contents

Day 1

Day 2

- Introduction to Windows API
- Hypothesis v/s Use-cases
- Threat Hunting Use Case Development
  - DNS Logs
  - Proxy Logs
  - Firewall Logs
  - Windows Event Logs
  - Sysmon Logs
  - Network Detection and Response (Zeek)
  - Anomaly Detection
- Raw log hunting with Linux toolkit
- Lab 1 – Hunting Network Artefacts
  - Zeek Scripting
  - Extracting Data from PCAPS
  - Hunting APTs from an Old Investigation

Day 3

- Hunting in a Simulated Active Directory Environment
- Threat Hunting Workflow
- Kill-Chain and Categorization
- Lab 2 – Hunting in Simulated Environment
    - Hunting Initial Foothold
    - Endpoint Analytics
        - Windows Logon Analytics
        - Scheduled Tasks
        - Services
        - Autoruns
        - Lateral Movement
        - Domain Privilege Escalation Artefacts
        - Parent and Child Process Anomalies
        - Malware Analysis and Debuggers
        - IMPHashing
        - Memory Forensics with Volatility
        - Windows API Hooking
    - Detection Weakness and Log Analysis Limitations
- Lab 3 –Hunting CTF

Target Audience

- Blue Teamers
- Threat Hunters
- SOC Analysts

This training program uses real-world attacks that help the L1/L2 threat hunters to enhance their detection and hunting capabilities. The training focuses on all log sources for hunting and eventually performing quick malware analysis and memory forensics found during hunts. The training program is a highly hands-on intermediate course for analysts and blue teamers who want to understand real-world threat actors. For a more advanced course on endpoint hunting, please refer our other course on ADVERSARY OPERATIONS & PROACTIVE HUNTING.

Requirements

- Strong will to learn and creative mindset
- Basic understanding of behavioral v/s signatured detections
- Basic programming concepts and Windows OS knowledge
- Basic understanding of Linux OS

What all do you get in the end

- 3 days of rigorous training program
- Course PDF and content materials

For any queries, contact paranoidninja@0xdarkvortex.dev