Malware Investigation with Memory Forensic and Threat Hunting

-Prepared by: Amrit Chhetri

Contents

DAY 1 Outlines:

1. **Malware Analysis with Memory Forensics**
    a. Sample Investigation-Scenario & Analysis
    b. Malware Analysis Sandbox & Tools
    c. Malware Analysis Tools Reviews
    d. Enriching Evidences With VI, CTI & TH
    e. Post-Memory Forensics Analysis
    f. Context, Scenario & Evidences
    g. Malware Analysis with Memory Forensics
2. **Post-Memory Forensics Analysis**
    a. Vulnerability Intelligence and Reverse Engineering
3. **Movies on Malware Attacks and Investigations**
    a. Malware Infection : Algorithm , ultimate scene of Malware Infection for Free Internet
    b. Photo Forensics : Forensic (Hindi Movie)
    c. Malware Attack : Forensics Files , Episode 38

4. **Malware Analysis with Memory Forensics**
    a. Malware Analysis using Volatility
    b. Practical Analysis using Yara and Volatity
    c. Vulnerability Intelligence and RE Labs
5. **Industrial Courses & Certifications**
    a. Industrial Courses and Certifications
6. **Q&A And Assessment**

DAY 2 Outlines: