CWL

CyberWarFare Labs

Certified Red Team – CredOps Infiltrator [CRT-COI]

@CyberWarFare Labs

Introduction

- Credentials and its significance
- Credentials Home (Memory, Files, Registry)
- Common Attacks on Credentials
- Credential Dumping

Tools & Techniques:

- Overview of Open-Source Tools
- In-depth exploration of modules
  - DPAPI decryption
  - Browsers credential extraction
  - WiFi password retrieval
  - Registry hive
  - Credential Manager
  - Wdigest
  - LSASS memory dumping
  - Offline credential extraction

CWL
CyberWarFare Labs

Evasion

- Obfuscation methods
  - Usage of packers
  - Code encryption
- Process injection for Evading Detection

Manual Dumping

- Hands-on manual extraction of credentials
- Real-world scenarios and case studies

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live