CWL
CyberWarFare Labs

The Silent Pivot: Member Server to Domain Controller

About CW Labs :

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats and client requirements. The company has these primary divisions:

1. Cyber Range Labs
2. Up-Skilling Platform
3. Infinity Learning Platform

CWL provides customized on-site training for organizations and accepts bulk orders for corporate upskilling. For inquiries or more details, feel free to reach out at **support@cyberwarfare.live.**

About Speaker

Ranjitha V

Security Engineer@CWL

Ranjitha V is a Blue Team Security Engineer at CyberWarfare Labs.Interested in Cloud and On-Premise Defense Operations.

AGENDA

1. Challenge Overview
2. Attack Flow
3. Key Concepts Behind The Attack
4. Investigation MindMap
5. Solving the Challenge

Challenge Overview :

The Silent Pivot: Member Server to Domain Controller

- Detect remote authentication → SYSTEM execution → credential access → lateral movement → Domain Takeover
- Analyze key Windows events: 4624, 7045, 4688, 4673/4674, 4672
- Trace attacker movement from member server to Domain Controller

Goal: Reconstruct a full Active Directory compromise path using SIEM logs.

Attack Flow :

1. Gains access to a member server
2. Executes commands using SYSTEM privileges
3. Attempts to access LSASS (credential dumping)
4. Reuses stolen credentials
5. Moves laterally to Domain Controller
6. Gains Domain Administrator privileges

Key Concepts Behind the Attack :

Active Directory (AD)

- Centralized system managing users, systems, and access

Member Server vs Domain Controller

- Member Server → Regular domain-joined system
- Domain Controller → Handles authentication & controls domain

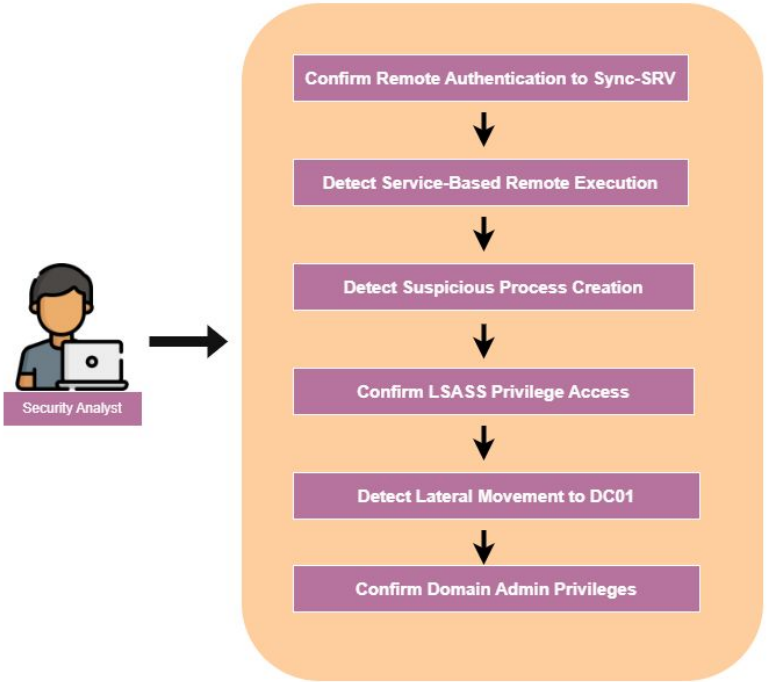
SYSTEM Privileges

- Highest privilege in Windows
- Full control over the system.

LSASS (Credential Storage)

- Local Security Authority Subsystem Service
- Stores passwords, hashes, and tickets in memory

Investigation MindMap :



CWL
CyberWarFare Labs

Thank You

For Professional Red Team / Blue Team / Purple Team / Cloud Cyber Range labs / Trainings

Please Contact :

support@cyberwarfare.live

To know more about our offerings, please visit: **https://cyberwarfare.live**