Table of Contents

Windows Credential Dumping Techniques – 0x12 Dark Development

00 Introduction

Overview of credential dumping evolution, Credential Guard, Remote Credential Guard, and modern bypass landscape

Theory

01 Credential Guard

How VBS-based isolation protects NT hashes and Kerberos tickets using LSAIso.exe

02 Local Security Authority Subsystem Service (LSASS)

Role of lsass.exe, comparison before/after Credential Guard, proxy behavior in VSM

03 Evolution of Credential Dumping

Historical timeline from WDigest plaintext to RCG abuse and chosen-challenge NTLMv1 attacks

Techniques

04 Classic LSASS Dumping

MiniDumpWriteDump to disk – the traditional (now often detected) method

05 In-Memory Dumping

Callback-based memory dump with memory mapping – avoids disk writes and improves stealth

06 Dumping Windows Credential Manager Vault

Enumerating stored credentials via CredEnumerateW – disk-resident secrets outside LSASS

07 Remote Credential Guard Abuse (SpecterOps 2025)

Abusing RCG protocol redirection to extract crackable NTLMv1 responses from guarded systems

08 Exercise – Mini Project

Build a modular credential access PoC suite combining multiple techniques with basic evasion

09 Conclusions

Key takeaways, defender recommendations, and suggested next topics in credential attacks & defenses

For educational and authorized security testing purposes only • 0x12 Dark Development • 2025–2026