Module Structure

WINDOWS PROTECTED PROCESS LIGHT — PART 1

ADVANCED | WINDOWS INTERNALS | 0X12 DARK DEV

THEORY

00 **Introduction**

Scope, ethical context, and PPL as a kernel-enforced Windows security boundary.

01 **What is PPL?**

PS_PROTECTION structure, signer levels, protection types & the _EPROCESS trust byte.

02 **PPL Attack Surface**

DKOM via kernel driver, handle access rules, PatchGuard & HVCI constraints.

TECHNIQUES

T1 **Discovering PPL**

Enumerating running processes and reading their PS_PROTECTION byte via NtQuerySystemInformation.

T2 **Disabling PPL Protection**

Kernel driver IOCTL to zero out the protection byte — stripping PPL from AV/EDR processes.

T3 **Setting PPL Protection**

Writing an arbitrary signer level into _EPROCESS to elevate any process to PPL.

T4 **PPL Reaper**

Bulk removal of PPL from all protected processes in a single driver sweep.

T5 **Demonstrating Windows Defender Evasion via PPL Manipulation**

Elevating attacker process to WinTcb-Light — operating at Defender's own trust level.

→ **Exercise**

Challenge 1: Dynamic offset resolution across Windows builds. Challenge 2: PPL elevation + persistence combo with watchdog thread.

■ **Conclusions**

PPL as a single byte of trust — how one kernel write flips a security feature into an offensive primitive.